Estratégia Concursos

Aula 10

PRF (Policial) Informática - 2023

(Pré-Edital)

Autor:

Diego Carvalho, Renato da Costa,

Equipe Informática e TI

25 de Fevereiro de 2023

Índice

1) Segurança da Informação - Antimalwares 3

2) Questões Comentadas - Segurança da Informação - Antimalwares - Multibancas 17

3) Lista de Questões - Segurança da Informação - Antimalwares - Multibancas 53

4) Segurança da Informação - Firewall 74

5) Questões Comentadas - Segurança da Informação - Firewall - Multibancas 94

6) Lista de Questões - Segurança da Informação - Firewall - Multibancas 146

7) Segurança da Informação - Mecanismos de Segurança 174

8) Questões Comentadas - Segurança da Informação - Mecanismos de Segurança - Multibancas 194

9) Lista de Questões - Segurança da Informação - Mecanismos de Segurança - Multibancas 225

APRESENTAÇÃO DA AULA

Pessoal, o tema da nossa aula é: **Ferramentas de Proteção e Segurança**. Nós já conhecemos os softwares maliciosos mais comuns e sabemos como são seus processos de infecção e propagação – além disso, nós já sabemos quais são suas ações maliciosas mais comuns. Agora chegou o momento de entender como proteger um computador e uma rede de ações maliciosas. Vem comigo que a aula é tranquilaaaaaaça...

PROFESSOR DIEGO CARVALHO - WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO

Galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. *Diego, se cai pouco para que colocar em aula?* Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: BAIXÍSSIMA
INCIDÊNCIA EM PROVA: BAIXA
INCIDÊNCIA EM PROVA: MÉDIA
INCIDÊNCIA EM PROVA: ALTA
INCIDÊNCIA EM PROVA: ALTÍSSIMA

Além disso, essas faixas não são por banca – é baseado tanto na quantidade de vezes que caiu em prova independentemente da banca e também em minhas avaliações sobre cada assunto...

#ATENÇÃO

Avisos Importantes

O curso abrange todos os níveis de conhecimento...

Esse curso foi desenvolvido para ser acessível a **alunos com diversos níveis de conhecimento diferentes.** Temos alunos mais avançados que têm conhecimento prévio ou têm facilidade com o assunto. Por outro lado, temos alunos iniciantes, que nunca tiveram contato com a matéria ou até mesmo que têm trauma dessa disciplina. A ideia aqui é tentar atingir ambos os públicos - iniciantes e avançados - da melhor maneira possível..

Por que estou enfatizando isso?

O **material completo** é composto de muitas histórias, exemplos, metáforas, piadas, memes, questões, desafios, esquemas, diagramas, imagens, entre outros. Já o **material simplificado** possui exatamente o mesmo núcleo do material completo, mas ele é menor e bem mais objetivo. *Professor, eu devo estudar por qual material?* Se você quiser se aprofundar nos assuntos ou tem dificuldade com a matéria, necessitando de um material mais passo-a-passo, utilize o material completo. Se você não quer se aprofundar nos assuntos ou tem facilidade com a matéria, necessitando de um material mais direto ao ponto, utilize o material simplificado.

Por fim...

O curso contém diversas questões espalhadas em meio à teoria. Essas questões possuem um comentário mais simplificado porque **têm o único objetivo de apresentar ao aluno como bancas de concurso cobram o assunto previamente administrado**. A imensa maioria das questões para que o aluno avalie seus conhecimentos sobre a matéria estão dispostas ao final da aula na lista de exercícios e **possuem comentários bem mais completos, abrangentes e direcionados.**

FERRAMENTAS ANTIMALWARE

Conceitos Básicos

INCIDÊNCIA EM PROVA: ALTA

Ferramentas Antimalware são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador (Ex: Antivírus, Antispyware, Antirootkit e Antitrojan). Ainda que existam ferramentas específicas para os diferentes tipos de códigos maliciosos, muitas vezes é difícil delimitar a área de atuação de cada uma delas, pois a definição do tipo de código depende de cada fabricante e muitos códigos mesclam as características dos demais tipos.

Entre as diferentes ferramentas existentes, a que engloba a maior quantidade de funcionalidades é o antivírus. **Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso.** Há diversos tipos de programas *antimalware* que diferem entre si das seguintes formas:

- **Método de detecção:** assinatura (uma lista de assinaturas é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características do código) e comportamento (baseia-se no comportamento apresentado) são alguns dos métodos mais comuns.

- **Forma de obtenção**: podem ser gratuitos, experimentais ou pagos. Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras e suporte.

- **Execução**: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.

- **Funcionalidades apresentadas**: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e *firewall* pessoal.

Para escolher o *antimalware* que melhor se adapta à necessidade de um usuário, é importante levar em conta o uso que você faz e as características de cada versão. **Observe que não há relação entre o custo e a eficiência de um programa, pois há versões gratuitas que apresentam mais funcionalidades que versões pagas de outros fabricantes.** Cuidados a serem tomados com o *antimalware* escolhido:

CUIDADOS NA ESCOLHA DE ANTIMALWARE
Tenha um *antimalware* instalado em seu computador – há programas online úteis, mas em geral possuem funcionalidades reduzidas;

Utilize programas online quando suspeitar que o *antimalware* local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião;
Configure o *antimalware* para verificar toda extensão de arquivo e para verificar automaticamente arquivos anexados aos e-mails e obtidos pela Internet;
Configure o *antimalware* para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos);
Mantenha o arquivo de assinaturas sempre atualizado (configure o *antimalware* para atualizá-lo automaticamente pela rede, de preferência diariamente);
Mantenha o *antimalware* sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas;
Evite executar simultaneamente diferentes programas *antimalware* – eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção;
Crie um disco de emergência e o utilize-o quando desconfiar que o *antimalware* instalado está desabilitado/comprometido ou que o comportamento do computador está estranho.

(TRT/RS - 2015) Ferramentas antimalware, como os antivírus, procuram detectar, anular ou remover os códigos maliciosos de um computador. Para que estas ferramentas possam atuar preventivamente, diversos cuidados devem ser tomados, por exemplo:

a) utilizar sempre um antimalware online, que é mais atualizado e mais completo que os locais.

b) configurar o antimalware para verificar apenas arquivos que tenham a extensão .EXE.

c) não configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives e discos externos), pois podem ser uma fonte de contaminação que o usuário não percebe.

d) atualizar o antimalware somente quando o sistema operacional for atualizado, para evitar que o antimalware entre em conflito com a versão atual do sistema instalado.

e) evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

Comentários: (a) Errado, um antimalware online só funciona se estiver conectado à internet, logo o ideal é ter um antimalware que esteja ativo independente de estar online ou não; (b) Errado, há outras extensões que também podem causar problemas – inclusive outras extensões executáveis; (c) Errado, é ideal que ele seja configurado para fazer verificações automaticamente discos rígidos e outras mídias; (d) Errado, sugere-se atualizar o antimalware sempre que possível – quanto mais atualizado melhor; (e) Correto, é recomendável evitar a execução simultânea de antimalwares para que eles não entrem em conflito (Letra E).

Antivírus

INCIDÊNCIA EM PROVA: ALTA

Como o próprio nome sugere, o antivírus é uma ferramenta para remover vírus existentes em um computador e combater a infecção por novos vírus. A solução ideal para a ameaça de vírus é a prevenção: em primeiro lugar, não permitir que um vírus entre no sistema. Esse objetivo, em geral, é impossível de se conseguir, embora a prevenção possa reduzir o número de ataques virais bem-sucedidos. Caso não seja possível, recomenda-se seguir os seguintes passos:

FASES	DESCRIÇÃO
DETECÇÃO	Uma vez que a infecção do vírus tenha ocorrido em algum programa de computador, localize o vírus.
IDENTIFICAÇÃO	Uma vez que o vírus tenha sido detectado, identifique qual vírus específico que infectou um programa.
REMOÇÃO	Uma vez o vírus tenha sido identificado, remova todos os traços do vírus do programa infectado e restaure-o ao seu estado original.

Algumas vezes, quando o antivírus encontra um arquivo que considera maligno, ele também oferece a opção colocá-lo em quarentena. *O que é isso, professor?* **A quarentena é uma área virtual onde o antivírus armazena arquivos identificados como possíveis vírus enquanto ele aguarda uma confirmação de identificação**. As assinaturas nem sempre são totalmente confiáveis e podem detectar vírus em arquivos inofensivos – falsos-positivos.

Trata-se de uma opção à remoção, uma vez que eventualmente determinados arquivos não podem ser eliminados por possuírem grande valor para o usuário ou por serem considerados importantes para o bom funcionamento de um sistema. Nesse caso, a quarentena permite que o arquivo fique isolado por um período até que desenvolvedores do antivírus possam lançar alguma atualização. *Bacana?*

Ao deixar os arquivos suspeitos em um local isolado e seguro, o antivírus permite que eles eventualmente sejam recuperados mais tarde e também impede que eventuais pragas virtuais realizem qualquer atividade maliciosa. Idealmente, os arquivos na situação de quarentena são

criptografados ou alterados de alguma forma para que ele não possa ser executado e outros antivírus não os identifiquem como um potencial vírus.

(CBTU - 2014) Ao realizar a verificação por meio de um antivírus, um usuário detectou a presença de um vírus no seu computador. Foi orientado por um amigo a não excluir o arquivo infectado de imediato, mas, sim, isolá-lo em uma área sem a execução de suas funções por um determinado período de tempo. Tal recurso é conhecido como:

a) vacina b) maturação c) isolamento d) quarentena

Comentários: o recurso que isola um malware em uma área por um período de tempo é a quarentena (Letra D).

Os principais antivírus do mercado são: Avast, McAfee, Bitdefender, Kaspersky, AVG, ESET, Symantec, Norton, Avira, Comodo, PSafe, entre outros. *Professor, isso cai em prova?* Infelizmente, saber o nome dos principais antivírus do mercado cai em prova. **Agora um ponto que despeeeeeeeeeeenca em prova: é recomendável evitar a execução simultânea de mais de um antimalware (antivírus) em um mesmo computador.**

POR QUE NÃO UTILIZAR MAIS DE UM ANTIMALWARE SIMULTANEAMENTE?

Galera, existem diversos motivos para não utilizar mais de um antimalware simultaneamente. Dentre eles, podemos mencionar: podem ocasionar problemas de desempenho no computador escaneado; podem interferir na capacidade de detecção um do outro; um pode detectar o outro como um possível malware; entre outros. **Dessa forma, recomenda-se evitar a utilização de mais de um antimalware. *Fechado?* ;)**

Vamos falar agora sobre as gerações de antivírus. Os avanços na tecnologia de vírus e antivírus seguem lado a lado. Pesquisas mostram que todos os dias surgem cerca de 220.000 novos tipos de vírus. Os softwares utilitários de antivírus têm evoluído e se tornando mais complexos e sofisticados como os próprios vírus – inclusive antivírus modernos podem detectar até worms, se sua assinatura for conhecida. **Hoje em dia, identificam-se quatro gerações de software antivírus...**

1ª Geração: Detecção baseada em Assinatura

INCIDÊNCIA EM PROVA: ALTA

A assinatura é uma informação usada para detectar pragas. Assim como a assinatura do nome identifica a identidade da pessoa, a assinatura de um vírus é o que o antivírus usa para identificar que uma praga digital está presente em um arquivo. **A assinatura é geralmente um trecho único do código do vírus – estrutura ou padrão de bits**. Procurando por esse trecho, o antivírus pode detectar o vírus sem precisar analisar o arquivo inteiro.

É realizada uma engenharia reversa no software malicioso para entendê-lo. Então é desenvolvida uma maneira de detectá-lo, depois ele é catalogado em uma base de dados e distribuído para todos os clientes do antivírus. Dessa forma, **há um tempo razoável da identificação à atualização da base da dados e esse tempo varia de acordo com fatores como**: complexidade do vírus, tempo para receber a amostra, entre outros.

Por outro lado, as assinaturas permitem detectar códigos maliciosos de um modo muito mais específico, sendo mais eficientes para remover ameaças complexas anteriormente mapeadas. **Além disso, devido a inúmeras técnicas utilizadas pelos atacantes para ofuscar o malware e burlar métodos heurísticos, é necessário – em alguns casos – contar com assinaturas específicas**. *Fechado?*

> **(TCE/ES – 2012)** Em geral, softwares antivírus trabalham com assinaturas de vírus; assim, para um novo vírus ser detectado pelo software, este precisa conhecer a assinatura desse novo vírus.
>
> _____
>
> **Comentários:** é verdade... como ele funciona baseado em uma assinatura conhecida, ele precisa conhecê-la (Correto).

2ª Geração: Detecção baseada em Heurística

INCIDÊNCIA EM PROVA: MÉDIA

A heurística é um conjunto de técnicas para identificar vírus desconhecidos de forma proativa – sem depender de assinatura. Nesta linha, a solução de segurança analisa trechos de código e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça. Para cada ação executada pelo arquivo é atribuída uma pontuação e assim – se esse número for superior a um determinado valor – será classificado como um provável *malware*.

Para tal, ele pode – por exemplo – procurar o início de um loop de criptografia usado em um vírus polimórfico ou verificar a integridade do software, utilizando funções de *hash*. Agora uma informação interessante: a palavra *Heurística* vem de "*Eureka*" – a exclamação atribuída ao matemático Arquimedes ao descobrir uma solução para um problema complexo envolvendo densidade e volume de um corpo. *Eureka* significa *encontrar*, *descobrir, deduzir*!

Em um sentido mais genérico, a palavra *heurística* trata de regras e métodos que conduzem à dedução de uma solução aproximada ou satisfatória para um problema. *E não é a mesma coisa com o antivírus?* Ele busca comparar algumas estruturas e comportamentos com padrões predefinidos com o intuito de indicar a provável presença de um malware. **Eventualmente pode haver alguns falsos-positivos, mas se trata de uma aproximação razoável**.

Em suma, nós podemos afirmar que a detecção baseada em heurística é capaz de identificar possíveis vírus utilizando dados genéricos sobre seus comportamentos. Assim sendo, esta técnica é capaz de detectar vírus genéricos, sem assinatura conhecida, através da comparação com um código conhecido de vírus e, assim, determinar se aquele arquivo ou programa pode ou não ser um vírus. *Compreendido, galera?*

Essa é uma estratégia eficaz, uma vez que a maioria dos códigos maliciosos da Internet são cópias de outros códigos. Ao descobrir um código malicioso, podem ser descobertos muitos outros similares, sem que eles sejam conhecidos. **O principal benefício é a capacidade de detectar novos vírus, antes mesmo que o antivírus conheça e tenha capacidade de evitá-los**. Em outras palavras, é capaz de detectar um novo vírus antes que ele faça algum mal.

> **(TCE/ES - 2014)** Para tentar prevenir uma infecção por vírus ou malware, algumas ferramentas de antivírus procedem à detecção por heurística, técnica de detecção de vírus baseada no comportamento anômalo ou malicioso de um software.
>
> _____
>
> **Comentários:** perfeito... a detecção por heurística permite identificar vírus desconhecidos de forma proativa – sem depender de assinatura – baseado no comportamento anômalo ou malicioso (Correto).

3ª Geração: Interceptação de Atividade

INCIDÊNCIA EM PROVA: BAIXA

Trata-se de uma tecnologia que identifica um vírus por suas ações, em vez de sua estrutura em um programa infectado. Esses programas têm a vantagem de não ser necessário desenvolver assinaturas e heurísticas para uma ampla variedade de vírus. **É diferente da heurística porque só funciona com programas em execução, enquanto a heurística analisa o próprio arquivo sem a necessidade de executá-lo**.

Funciona como um policial à procura de ações estranhas em um suspeito. **Ele observa o sistema operacional, procurando por eventos suspeitos**. Se o programa antivírus testemunhar uma tentativa de alterar ou modificar um arquivo ou se comunicar pela web, ele poderá agir e avisá-lo da ameaça ou poderá bloqueá-la, dependendo de como você ajusta suas configurações de segurança. Também há uma chance considerável de encontrar falsos-positivos.

Em suma: o antivírus monitora continuamente todos os programas em execução no computador. Cada atividade dos softwares é considerada maliciosa ou inofensiva. Se várias tarefas suspeitas forem realizadas por um mesmo aplicativo, o antivírus irá considerá-lo malicioso. **Caso o vírus se**

comporte de forma semelhante a pragas conhecidas, ele será reconhecido como malicioso sem a necessidade de uma vacina específica.

4ª Geração: Proteção Completa

INCIDÊNCIA EM PROVA: BAIXA

São pacotes compostos por uma série de técnicas antivírus utilizadas em conjunto. Estas incluem componentes de varredura e de interceptação de atividades. Ademais, esse tipo de pacote inclui recurso de controle de acesso, que limita a capacidade dos vírus de penetrar em um sistema e, por consequência, limita a capacidade de um vírus de atualizar arquivos a fim de passar a infecção adiante. Trata-se da geração da maioria dos antivírus atuais.

Next Generation Antivirus (NGAV)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Por fim, vamos falar rapidamente sobre o Next Generation Antivirus (NGAV). Para entender o que são e como funcionam os antivírus da nova geração, é preciso focar na sua principal diferença em relação aos antivírus convencionais. Essas soluções que conhecemos há décadas não são "inteligentes"; tudo o que fazem é varrer o sistema em busca de ameaças conhecidas, que constam em listas atualizadas várias vezes ao dia.

O problema é que o tempo entre uma atualização e outra é suficiente para milhares de ataques agirem com sucesso. São ineficazes também contra alguns ataques, nos quais a falha é descoberta e explorada no mesmo dia em que foi identificada sua existência. **Já o NGAV vai além de assinaturas de malwares conhecidas – eles usam análises preditivas, conduzidas por aprendizado de máquina e inteligência artificial para detectar e prevenir ataques de malware.**

Eles podem também identificar comportamentos maliciosos, bem como coletar e analisar dados para determinar as causas raiz de uma vulnerabilidade. **Dessa forma, são capazes de responder a ameaças novas e emergentes que anteriormente não eram detectadas.** Em suma, eles agem com base no comportamento do usuário, verificando em tempo real se cada atividade sua representa – ou não – um risco real.

E faz isso com análises constantes sobre tudo que é feito no dispositivo, usando inteligência artificial e aprendizado de máquina, para determinar o que é seguro ou não. Eles utilizam o conceito de *sandbox*, monitorando e respondendo às táticas, técnicas e procedimentos de invasão. Essa nova tecnologia e arquitetura de software foi criada para preencher a lacuna deixada pelo antivírus comum, levando a proteção a um nível totalmente novo.

O NGAV possui tecnologias de: Anti-Ransomware; Anti-Exploit Prevention; ATP - Advanced Threat Protection; DLP - Data Loss Prevention; Mitigação; Proteção preventiva com Deep Learning; Resposta a Incidentes instantânea; e EDR - Endpoint Detection and Response. **A habilidade em reconhecer e lidar com ameaças de segurança por conta própria é muito mais eficaz em vez de depender de um banco de dados de assinaturas.**

Antispam

INCIDÊNCIA EM PROVA: BAIXA

Os Filtros Antispam já vêm integrados à maioria dos programas de e-mails e permite separar os desejados dos indesejados – os famosos *spams*. A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas *spam* e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens. Ao detectá-las, essas ferramentas alertam para que ele tome as atitudes adequadas para si.

Existem também algumas técnicas de bloqueio de spam (no sentido de classificá-lo como spam e, não, de impedir o seu recebimento) que se baseiam na análise do conteúdo da mensagem. Em geral, são filtros baseados no reconhecimento de padrões do conteúdo que buscam identificar se o *e-mail* pode conter um vírus ou se tem características comuns aos spams. Os filtros de conteúdo mais comuns são os antivírus e os identificadores Bayesianos de spam.

Antispyware

INCIDÊNCIA EM PROVA: BAIXA

Antispyware é um tipo de software projetado para detectar e remover programas de *spyware* indesejados. Spyware é um tipo de *malware* instalado em um computador sem o conhecimento do usuário para coletar informações sobre ele. Isso pode representar um risco de segurança para o usuário, além de degradar o desempenho do sistema, absorvendo o poder de processamento, instalando *software* adicional ou redirecionando a atividade do navegador dos usuários.

(DPE/MT – 2015) Antispyware é um software de segurança que tem o objetivo de detectar e remover spywares, sendo ineficaz contra os adwares.

_____

Comentários: *adwares* são tipos de *spywares*, logo é eficaz também (Errado).

RESUMO

FERRAMENTAS ANTIMALWARE

Ferramentas Antimalware são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador (Ex: Antivírus, Antispyware, Antirootkit e Antitrojan). Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso. Há diversos tipos de programas antimalware que diferem entre si sob diversos critérios.

- **Método de detecção:** assinatura (uma lista de assinaturas é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características do código) e comportamento (baseia-se no comportamento apresentado) são alguns dos métodos mais comuns.

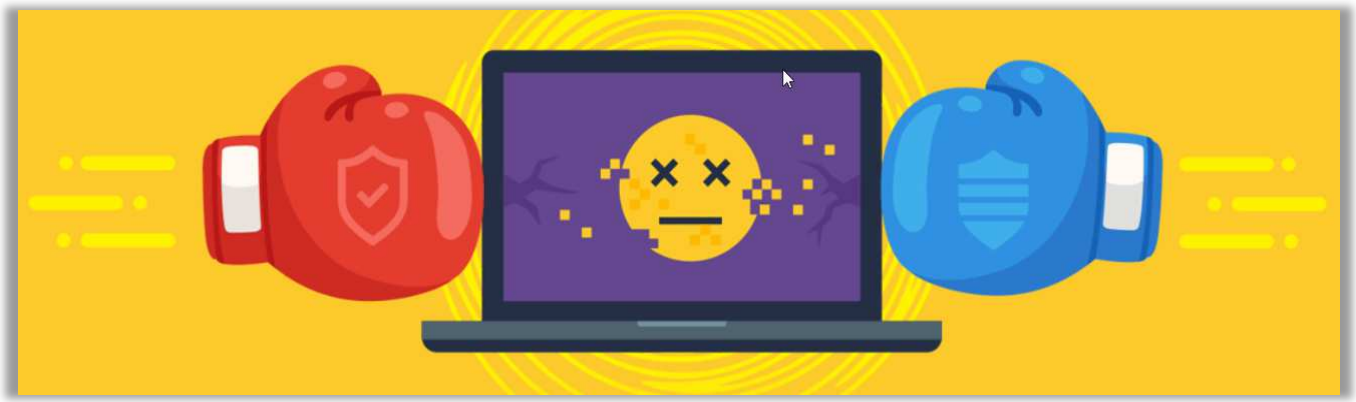
- **Forma de obtenção**: podem ser gratuitos, experimentais ou pagos. Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras e suporte.

- **Execução**: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.

- **Funcionalidades apresentadas**: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e *firewall* pessoal.

FASES	DESCRIÇÃO
DETECÇÃO	Uma vez que a infecção do vírus tenha ocorrido em algum programa de computador, localize o vírus.
IDENTIFICAÇÃO	Uma vez que o vírus tenha sido detectado, identifique qual vírus específico que infectou um programa.
REMOÇÃO	Uma vez o vírus tenha sido identificado, remova todos os traços do vírus do programa infectado e restaure-o ao seu estado original.

NÃO É RECOMENDÁVEL UTILIZAR MAIS DE UM ANTIMALWARE SIMULTANEAMENTE



POSSÍVEIS CUIDADOS
Tenha um antimalware instalado em seu computador (programas online, apesar de bastante úteis, exigem que seu computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas).
Utilize programas online quando suspeitar que o antimalware local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião (quiser confirmar o estado de um arquivo que já foi verificado pelo antimalware local).
Configure o antimalware para verificar toda e qualquer extensão de arquivo.
Configure o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos).
Mantenha o arquivo de assinaturas sempre atualizado (configure o antimalware para atualizá-lo automaticamente pela rede, de preferência diariamente).
Mantenha o antimalware sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.
Evite executar simultaneamente diferentes programas antimalware (eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro).
Crie um disco de emergência e o utilize-o quando desconfiar que o antimalware instalado está desabilitado/comprometido ou que o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc).

TIPOS DE ANTIVÍRUS	DESCRIÇÃO
1º GERAÇÃO	Também chamada de Detecção Baseada em Assinatura, ele busca por um trecho único do código do vírus (estrutura ou padrão de bits) chamado de assinatura. Procurando por esse trecho, o antivírus pode detectar o vírus sem precisar analisar o arquivo inteiro. É realizada uma engenharia reversa no software malicioso para entendê-lo. Então é desenvolvida uma maneira de detectá-lo, depois ele é catalogado em uma base de dados e distribuído para todos os clientes do antivírus.

2º GERAÇÃO	Também chamada de Detecção Baseada em Heurística, ele utiliza um conjunto de técnicas para identificar vírus desconhecidos de forma proativa chamada heurística – sem depender de assinatura. Nesta linha, a solução de segurança analisa a estrutura de um arquivo e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça.
3º GERAÇÃO	Também chamada de Interceptação de Atividade, ele utiliza uma tecnologia que identifica um vírus por suas ações, em vez de sua estrutura em um programa infectado. Esses programas têm a vantagem de não ser necessário desenvolver assinaturas e heurísticas para uma ampla variedade de vírus. É diferente da heurística porque só funciona com programas em execução, enquanto a heurística analisa o próprio arquivo sem a necessidade de executá-lo.
4º GERAÇÃO	Também chamado de Proteção Completa, São pacotes compostos por uma série de técnicas antivírus utilizadas em conjunto. Estas incluem componentes de varredura e de interceptação de atividades. Ademais, esse tipo de pacote inclui recurso de controle de acesso, que limita a capacidade dos vírus de penetrar em um sistema e, por consequência, limita a capacidade de um vírus de atualizar arquivos a fim de passar a infecção adiante. Trata-se da geração da maioria dos antivírus atuais.

ANTISPYWARE

- **Antispyware** é um tipo de software projetado para detectar e remover programas de spyware indesejados. Spyware é um tipo de malware instalado em um computador sem o conhecimento do usuário para coletar informações sobre ele. Isso pode representar um risco de segurança para o usuário, além de degradar o desempenho do sistema, absorvendo o poder de processamento, instalando software adicional ou redirecionando a atividade do navegador dos usuários.

ANTISPAM

- **Filtros Antispam** já vêm integrados à maioria dos programas de e-mails e permite separar os desejados dos indesejados – os famosos spams. A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens. Ao detectá-las, essas ferramentas alertam para que ele tome as atitudes adequadas para si.

MAPA MENTAL

Ferramentas Antimalware

Antivírus

- CRIADO INICIALMENTE PARA REMOVER VÍRUS EXISTENTES NO COMPUTADOR E COMBATER A INFECÇÃO POR NOVOS VÍRUS.
- HOJE, ENGLOBA AS FUNCIONALIDADES DE OUTROS PROGRAMAS, COMO ANTISPYWARES.
- CUIDADOS IMPORTANTES:
  - MANTER O ANTIVÍRUS SEMPRE ATUALIZADO.
  - MANTER O ARQUIVO DE ASSINATURAS SEMPRE ATUALIZADO.
  - CONFIGURAR O ANTIVÍRUS P/ VERIFICAR AUTOMATICAMENTE OS DISCOS RÍGIDOS E AS UNIDADES REMOVÍVEIS (EX: PENDRIVES).
  - EVITAR A EXECUÇÃO SIMULTANEAMENTE DE DIFERENTES ANTIVÍRUS.

GERAÇÕES DE ANTIVÍRUS

1ª GERAÇÃO: DETECÇÃO BASEADA EM ASSINATURA

- A ASSINATURA É UM TRECHO ÚNICO DO CÓDIGO DO VÍRUS (ESTRUTURA OU PADRÃO DE BITS) QUE O ANTIVÍRUS USA PARA IDENTIFICAR QUE UMA PRAGA VIRTUAL ESTÁ PRESENTE EM UM ARQUIVO.
- DESVANTAGEM: LEVA UM CERTO TEMPO PARA QUE O MALWARE SEJA IDENTIFICADO E A BASE DE DADOS SEJA ATUALIZADA COM SUA ASSINATURA.
- VANTAGEM: É MAIS EFICIENTE NA REMOÇÃO DE AMEAÇAS COMPLEXAS ANTERIORMENTE MAPEADAS OU DE MALWARES QUE BURLAM OS MÉTODOS HEURÍSTICOS.

2ª GERAÇÃO DETECÇÃO BASEADA EM HEURÍSTICA

- A HEURÍSTICA É UM CONJUNTO DE TÉCNICAS P/ IDENTIFICAR VÍRUS DESCONHECIDOS DE FORMA PROATIVA – SEM DEPENDER DE ASSINATURA.
- ANALISA O COMPORTAMENTO DE UM TRECHO DE CÓDIGO P/ DESCOBRIR PADRÕES SUSPEITOS EM SUA ATIVIDADE MALICIOSA.
- É UMA ESTRATÉGIA EFICAZ PORQUE A MAIORIA DOS CÓDIGOS MALICIOSOS DA INTERNET SÃO CÓPIAS DE OUTROS CÓDIGOS.
- DESVANTAGEM: PODE GERAR MAIS FALSOS-POSITIVOS.
- VANTAGEM: É CAPAZ DE IDENTIFICAR VÍRUS NOVOS ANTES QUE ELES GEREM DANOS.

3ª GERAÇÃO: INTERCEPTAÇÃO DE ATIVIDADE

- IDENTIFICA O VÍRUS POR SUAS AÇÕES, EM VEZ DE SUA ESTRUTURA EM UM PROGRAMA INFECTADO.
- DESVANTAGEM: SÓ FUNCIONA COM PROGRAMAS EM EXECUÇÃO, ENQUANTO A HEURÍSTICA ANALISA O ARQUIVO EM SI, SEM NECESSIDADE DE EXECUTÁ-LO.
- VANTAGEM: NÃO É NECESSÁRIO DESENVOLVER ASSINATURAS E HEURÍSTICAS P/ UMA AMPLA VARIEDADE DE VÍRUS.

4ª GERAÇÃO: PROTEÇÃO COMPLETA

- É A GERAÇÃO DA MAIORIA DOS ANTIVÍRUS ATUAIS.
- SÃO PACOTES COMPOSTOS POR UM CONJUNTO DE TÉCNICAS ANTIVÍRUS.
- INCLUEM RECURSO DE CONTROLE DE ACESSO, QUE LIMITA A CAPACIDADE DOS VÍRUS DE PENETRAR EM UM SISTEMA, LIMITANDO SUA CAPACIDADE DE ATUALIZAR ARQUIVOS E, CONSEQUENTEMENTE, DE SE PROPAGAR.

QUARENTENA:

- ÁREA VIRTUAL ONDE O ANTIVÍRUS ARMAZENA ARQUIVOS IDENTIFICADOS COMO POSSÍVEIS VÍRUS ENQUANTO ELE AGUARDA CONFIRMAÇÃO.
- É UMA ALTERNATIVA À REMOÇÃO.
- ENQUANTO ESTIVEREM ISOLADAS NA QUARENTENA, EVENTUAIS PRAGAS VIRTUAIS FICAM IMPEDIDAS DE REALIZAR QUALQUER ATIVIDADE MALICIOSA.

Antispyware

- SOFTWARE PROJETADO PARA DETECTAR E REMOVER PROGRAMAS DE SPYWARE INDESEJADOS.
  - PODEM SER:
    - SCREENLOGGERS
    - KEYLOGGERS
    - ADWARES

Antispam

- PERMITE SEPARAR OS E-MAILS DESEJADOS DOS INDESEJADOS (SPAMS).
- JÁ VEM INTEGRADO À MAIORIA DOS PROGRAMAS DE E-MAILS.
- GERALMENTE PASSA POR UM PERÍODO DE "TREINAMENTO", EM QUE O USUÁRIO SELECIONA MANUALMENTE E-MAILS QUE CONSIDERA SPAM PARA QUE O FILTRO POSSA APRENDER A DISTINGUI-LOS.

@mapasdathai

QUESTÕES COMENTADAS – CESPE

1. **(CESPE / TRT8 – 2022)** Certo TRT deseja implementar uma solução de segurança cibernética que combine inteligência artificial, detecção comportamental e algoritmos de aprendizado de máquina para antecipar e prevenir ameaças conhecidas e desconhecidas.

   Com base nessa situação hipotética, assinale a opção que indica a solução requerida.

   a) NGAV.
   b) IPS
   c) IDS
   d) NIST
   e) WebProxy

Comentários:

O NGAV (Next Generation Antivirus) é a ferramenta utilizada para combinar inteligência artificial, detecção comportamental e algoritmos de aprendizado de máquina para antecipar e prevenir ameaças conhecidas e desconhecidas. Para entender o que são e como funcionam os antivírus da nova geração, é preciso focar na sua principal diferença em relação aos antivírus convencionais. Essas soluções que conhecemos há décadas não são "inteligentes"; tudo o que fazem é varrer o sistema em busca de ameaças conhecidas, que constam em listas atualizadas várias vezes ao dia.

O problema é que o tempo entre uma atualização e outra é suficiente para milhares de ataques agirem com sucesso. Logo, as ferramentas tradicionais acabam sendo vulneráveis a diversas ameaças. O NGAV atua além de assinaturas de malware conhecidas – eles usam análises preditivas, conduzidas por aprendizado de máquina e inteligência artificial, combinando com inteligência de ameaças para detectar e prevenir ataques de malware.

Podem também identificar comportamentos maliciosos de fontes desconhecidas, bem como coletar e analisar dados para determinar as causas raiz de uma vulnerabilidade. Assim, são capazes de responder a ameaças novas e emergentes que anteriormente não eram detectadas. Em suma, um NGAV age com base no comportamento do usuário, verificando em tempo real se cada atividade sua representa – ou não – um risco.

E faz isso com análises constantes sobre tudo que é feito no dispositivo, usando inteligência artificial e aprendizado de máquina, para determinar o que é seguro ou não.

Gabarito: Letra A

2. **(CESPE / PC-AL – 2021)** A heurística é um dos métodos de detecção das ferramentas antimalware – como antivírus, antirootkit e antispyware – que se baseiam nas estruturas, instruções e características que o código malicioso possui para identificá-lo.

Comentários:

Perfeito! A heurística é um conjunto de técnicas para identificar vírus desconhecidos de forma proativa – sem depender de assinatura. Nesta linha, a solução de segurança analisa trechos de código e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça. Para cada ação executada pelo arquivo é atribuída uma pontuação e assim – se esse número for superior a um determinado valor – será classificado como um provável malware.

Gabarito: Correto

---

3. **(CESPE / BNB– 2018)** Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes.

Comentários:

Na verdade, scareware é um software malicioso que faz com que os usuários de computadores acessem sites infestados por malware – não se trata de um antivírus!

Gabarito: Errado

---

4. **(CESPE / Polícia Federal – 2018)** Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

Comentários:

A heurística é um conjunto de técnicas para identificar vírus desconhecidos de forma proativa – sem depender de assinatura. Nesta linha, a solução de segurança analisa trechos de código e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça. Para cada ação executada pelo arquivo é atribuída uma pontuação e assim – se esse número for superior a um determinado valor – será classificado como um provável malware. Antivírus de 2ª Geração realmente utilizam heurísticas para identificar códigos maliciosos.

Gabarito: Correto

---

5. **(CESPE / CRBM – 2018)** O antispyware é conhecido como uma ferramenta complementar ao antivírus que deve ser executada frequentemente para checagem de possíveis ameaças que possam ter contaminado o sistema.

Comentários:

Perfeito... realmente é complementar aos antivírus – atualmente um antimalware integra todas essas ferramentas.

Gabarito: Correto

---

6. **(CESPE / CFO/DF – 2017)** Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

Comentários:

Elas conseguem - sim - realizar a verificação no conteúdo dos e-mails.

Gabarito: Errado

---

7. **(CESPE / TRE-PI – 2016)** A remoção de códigos maliciosos de um computador pode ser feita por meio de:

a) anti-spyware.
b) detecção de intrusão.
c) anti-spam.
d) anti-phishing.
e) filtro de aplicações.

Comentários:

(a) Correto, forçand a barra, anti-spywares podem remover spywares – que são malwares; (b) Errado, essas são ferramentas de monitoramento e detecção de intrusos em uma rede; (c) Errado, essas ferramentas protegem contra e-mails indesejados; (d) Errado, essas ferramentas protegem contra golpes ou fraudes de para obtenção de dados pessoais ou financeiros; (e) Errado, essas ferramentas permitem controlar acesso e analisar conteúdo de pacotes.

Gabarito: Letra A

---

8. **(CESPE / TRE-MT – 2015)** A função principal de uma ferramenta de segurança do tipo antivírus é:

a) monitorar o tráfego da rede e identificar possíveis ataques de invasão.
b) verificar arquivos que contenham códigos maliciosos.
c) fazer becape de segurança dos arquivos considerados críticos para o funcionamento do computador.
d) bloquear sítios de propagandas na Internet.

e) evitar o recebimento de mensagens indesejadas de email, tais como mensagens do tipo spams.

Comentários:

(a) Errado, essa é a função principal de um firewall; (b) Correto, a função principal de um antivírus realmente é verificar arquivos que contenham códigos maliciosos; (c) Errado, antivírus não realizam becapes; (d) Errado, essa é a função principal de um bloqueador de pop-ups; (e) Errado, essa é a função principal de um antispam – alguns antivírus podem exercer essa função, mas não é a sua função principal.

Gabarito: Letra B

---

9. **(CESPE / Telebras – 2015)** Como os antivírus agem a partir da verificação da assinatura de vírus, eles são incapazes de agir contra vírus cuja assinatura seja desconhecida.

Comentários:

Primeiro, é sempre possível agir isolando o vírus. Segundo, há tipos de antivírus que não necessitam conhecer a assinatura do vírus, eles podem também analisar seu comportamento.

Gabarito: Errado

---

10. **(CESPE / TRT-10 Região – 2013)** Um computador em uso na Internet é vulnerável ao ataque de vírus, razão por que a instalação e a constante atualização de antivírus são de fundamental importância para se evitar contaminações.

Comentários:

Perfeito, perfeito, perfeito! Recomenda-se manter o antivírus sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.

Gabarito: Correto

---

11. **(CESPE / SESA-ES – 2013 – Letra C)** O anti-spyware, ao contrário do antivírus, propaga a proteção contra os vírus existentes de maneira semelhante a um antídoto, o que evita a contaminação de outros computadores da rede.

Comentários:

Que viagem é essa? Antispyware protege contra spyware e, não, contra vírus.

Gabarito: Errado

---

12. (CESPE / Banco da Amazônia – 2012) Antispywares são softwares que monitoram as máquinas de possíveis invasores e analisam se, nessas máquinas, há informações armazenadas indevidamente e que sejam de propriedade do usuário de máquina eventualmente invadida.

Comentários:

Na verdade, antispywares são softwares que monitoram as máquinas de possíveis usuários e, não, invasores. Além disso, eles não procuram informações armazenadas e, sim, o programa malicioso que rouba informações do usuário.

Gabarito: Errado

---

13. (CESPE / Polícia Federal – 2012) A fim de se proteger do ataque de um spyware — um tipo de vírus (malware) que se multiplica de forma independente nos programas instalados em um computador infectado e recolhe informações pessoais dos usuários —, o usuário deve instalar softwares antivírus e antispywares, mais eficientes que os firewalls no combate a esse tipo de ataque.

Comentários:

Na verdade, spyware não é um tipo de vírus e também não se multiplica de forma independente.

Gabarito: Errado

---

14. (CESPE / PEFOCE – 2012) O antivírus, para identificar um vírus, faz uma varredura no código do arquivo que chegou e compara o seu tamanho com o tamanho existente na tabela de alocação de arquivo do sistema operacional. Caso encontre algum problema no código ou divergência de tamanho, a ameaça é bloqueada.

Comentários:

Einh? Como é? A comparação é realizada com o tamanho registrado em um banco de dados criado e mantido pelo próprio antivírus. Não há nenhuma relação com a tabela de alocação de arquivo do sistema operacional. O FAT (File Allocation Table) é uma tabela de utilização do disco rígido que permite ao sistema operacional saber exatamente onde um arquivo está armazenado.

Gabarito: Errado

---

15. (CESPE / TCE-RO – 2012) A manutenção da atualização dos antivírus auxilia no combate às pragas virtuais, como os vírus, que são mutantes.

Comentários:

Perfeito! Recomenda-se manter o antimalware/antivírus sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.

Gabarito: Correto

---

16. (CESPE / TRE/RJ – 2012) Recomenda-se utilizar antivírus para evitar phishing-scam, um tipo de golpe no qual se tenta obter dados pessoais e financeiros de um usuário.

Comentários:

Os navegadores podem ajudar a evitar phishing-scam – antivírus não são capazes, por padrão, de realizar essa função.

Gabarito: Errado

---

17. (CESPE / Banco da Amazônia – 2012) As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.

Comentários:

A verificação heurística é a capacidade que um antivírus possui de detectar um malware, sem possuir uma vacina específica para ele, isto é, a ideia da heurística é a de antecipar a descoberta de um malware. A questão trata da verificação de assinaturas, que determina as características que levam um arquivo a ser ou não considerado um malware.

Gabarito: Errado

---

18. (CESPE / TJ/AC – 2012) O antispyware é um software que se destina especificamente a detectar e remover spywares, enquanto o antivírus é uma ferramenta que permite detectar e remover alguns programas maliciosos, o que inclui certos tipos de spywares.

Comentários:

Perfeito... antivírus modernos – apesar do nome – permitem detectar e remover diversos tipos de software maliciosos, incluindo spywares.

Gabarito: Correto

---

19. (CESPE / TJ/AC – 2012) As ferramentas antispam permitem combater o recebimento de mensagens consideradas spam e, em geral, baseiam-se na análise do conteúdo das mensagens.

Comentários:

Sendo rigoroso, elas não combatem o recebimento em si – as mensagens indesejadas continuam sendo recebidas, mas elas são classificadas como spam. Em geral, baseiam-se na análise do conteúdo das mensagens. Enfim... caberia recurso!

Gabarito: Correto

---

20. (CESPE / IFB – 2011) Ferramentas como firewall e antivírus para estação de trabalho não ajudam a reduzir riscos de segurança da informação.

Comentários:

Como assim? Eles ajudam muito a reduzir riscos de segurança da informação.

Gabarito: Errado

---

21. (CESPE / FUB – 2009) O aplicativo antivírus original dessa versão do Windows é o Symantec Norton 2003.

Comentários:

Nem precisa saber à qual versão do Windows a questão se refere! Norton é um software antivírus proprietário, que não é nativo de nenhuma versão do MS-Windows.

Gabarito: Errado

QUESTÕES COMENTADAS – FCC

22. (FCC / TRF/4ª Região – 2019) Caso uma praga virtual seja muito forte e sua remoção por meio do processo de deleção de arquivos ou programas infectados possa afetar todo o funcionamento do computador, os antivírus devem executar um processo:

a) para isolar completamente o sistema operacional do sistema de arquivos.
b) para criptografar o arquivo ou programa infectado inteiro, antes renomeando-o em uma cópia com os caracteres $~ na frente de seu nome.
c) que visa manter o sistema operacional suspenso.
d) que visa manter o arquivo ou programa infectado em quarentena.
e) que se incumbe apenas de renomear o arquivo ou programa infectado com os caracteres $~ na frente de seu nome.

Comentários:

(a) Errado. Isso deixaria o sistema operacional inutilizável, logo não ajudaria a resolver o problema;
(b) Errado. Isso tornaria o arquivo ou programa inutilizável, logo não ajudaria a resolver o problema;
(c) Errado. Isso deixaria o sistema operacional inutilizável, logo não ajudaria a resolver o problema;
(d) Correto. Essa é uma maneira de deixar o arquivo isolado em uma área protegida do disco rígido por um período, logo é a ação mais adequada para o problema; (e) Errado. Isso não teria qualquer efeito prático.

Gabarito: Letra D

---

23. (FCC / SEMEF/Manaus – 2019) Um técnico tentou instalar uma aplicação no seu computador, mas o antivírus o impediu mostrando uma mensagem que o programa era legítimo, mas que poderia ser usado por criminosos para danificar o computador ou furtar dados pessoais. Analisando que as perdas que poderiam ser causadas pela execução do software seriam menores do que as perdas causadas pela não execução, o técnico pensou nas seguintes possibilidades para instalar e executar o software:

I. Incluir o software na lista de exclusão do antivírus, ou seja, na lista de programas que o antivírus não deverá verificar.

II. Mudar o nome do software para um nome amigável parecido com o nome recursos legítimos do sistema operacional, a fim de enganar o antivírus no momento da instalação e execução.

III. Desativar/Pausar o antivírus por um tempo determinado, ou seja, pelo tempo necessário para instalar e usar o software para o que necessita.

IV. Colocar o antivírus no modo de verificação apenas de disco rígido, de forma que ele não seja ativado quando perceber um possível malware carregado na memória.

Considerando que o técnico estava utilizando um dos principais antivírus do mercado, permitirá a instalação e execução do software APENAS o que consta em:

a) III.
b) I e III.
c) I e IV.
d) III e IV.
e) I e II.

Comentários:

(I) Correto. Caso ele esteja seguro, poderá incluir o software na lista de exclusão do antivírus de forma que o antivírus não o verifique; (II) Errado. Isso não teria qualquer efeito prático em termos de detecção pelo antivírus, uma vez que ele não verifica o nome do programa; (III) Correto. Caso ele esteja seguro, poderá pausar o antivírus enquanto instala o programa, de modo que o antivírus não impeça a instalação; (IV) Errado. Ao verificar apenas o disco rígido, ele poderá ser detectado normalmente pelo antivírus.

Gabarito: Letra B

---

24. (FCC / TRT/4ª Região – 2015) Ferramentas antimalware, como os antivírus, procuram detectar, anular ou remover os códigos maliciosos de um computador. Para que estas ferramentas possam atuar preventivamente, diversos cuidados devem ser tomados, por exemplo:

a) utilizar sempre um antimalware online, que é mais atualizado e mais completo que os locais.

b) configurar o antimalware para verificar apenas arquivos que tenham a extensão .EXE.

c) não configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives e discos externos), pois podem ser uma fonte de contaminação que o usuário não percebe.

d) atualizar o antimalware somente quando o sistema operacional for atualizado, para evitar que o antimalware entre em conflito com a versão atual do sistema instalado.

e) evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

Comentários:

(a) Errado, o ideal é que haja um antimalware instalado localmente na máquina do usuário – lembrem-se que um malware pode realizar ações maliciosas em um computador mesmo sem acesso à internet; (b) Errado, há diversos outros formatos de arquivos que podem causar danos além dos arquivos executáveis; (c) Errado, ambos devem ser sempre verificados – unidades removíveis, por exemplo, são fontes típicas de contaminação por malwares; (d) Errado, recomenda-se atualizar o antimalware sempre que houver novas atualizações independentemente da atualização do sistema operacional; (e) Correto, recomenda-se utilizar um único programa antimalware, uma vez que eles realmente podem entrar em conflito e afetar o desempenho do computador.

Gabarito: Letra E

---

25. (FCC / MPE/AM – 2013) Com relação à utilização correta de ferramentas antimalware, considere:

I. É aconselhável utilizar programas antimalware on-line quando se suspeitar que o antimalware local esteja desabilitado ou comprometido ou quando se necessitar de uma segunda verificação.

II. Devem ser configuradas para verificar apenas arquivos executáveis, pois são os únicos que podem conter vírus e outros tipos de malware.

III. Deve-se evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

IV. Não é recomendável ter um antimalware instalado no computador, pois os programas on-line além de serem mais eficientes, são suficientes para proteger o computador.

Está correto o que se afirma APENAS em:

a) I, II e III.
b) III e IV.
c) I e III.
d) II e IV.
e) I.

Comentários:

(I) Correto. Recomenda-se utilizar programas online quando suspeitar que o antimalware local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião (quiser confirmar o estado de um arquivo que já foi verificado pelo antimalware local); (II) Errado. Recomenda-se configurar o *antimalware* para verificar toda e qualquer extensão de arquivo; (III) Correto. Recomenda-se evitar a execução simultânea de diferentes programas antimalware, uma vez que eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de

detecção um do outro; (IV) Errado. Recomenda-se ter um antimalware instalado em seu computador (programas *online*, apesar de bastante úteis, exigem que seu computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas).

Gabarito: Letra C

QUESTÕES COMENTADAS – FGV

26.(FGV / CGU – 2022) Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

a) redução de custos e facilidade de atualização;
b) configuração simplificada e fácil instalação de API;
c) monitoramento completo e antivírus atualizado;
d) administração descentralizada e facilidade de integração com novas tecnologias;
e) bloqueio de ações indesejadas e controle no lado do usuário.

Comentários:

Endpoint é qualquer dispositivo, seja ele móvel ou não, desde uma estação de trabalho até notebooks, tablets e celulares, que podem ser conectados a uma rede. Logo, a segurança de endpoint visa assegurar que todos os serviços conectados a uma rede estejam protegidos contra vários tipos de ataques cibernéticos como worms, cavalos de troia, spywares, adwares, etc. Ué, professor... isso não é simplesmente um antivírus? Não...

Enquanto o antivírus é um software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e worms em PCs – único ou muitos -, a segurança de endpoint cobre toda a infraestrutura. Ele contém não apenas anti-malware, comum entre os antivírus, mas muitas ferramentas de segurança contra diferentes tipos de ameaças. Com ele, é possível manter a integridade dos dispositivos, a autenticação/autorização do usuário, para assim, preservar os endpoints seguros, o que não está incluído no pacote do antivírus.

Entre os benefícios da segurança de endpoint, temos:

- **Redução de Custos:** ao invés de investir em componentes separados para garantir a proteção de cada dispositivo conectado na rede, o sistema de endpoint reúne os componentes necessários em um só conjunto, o que é muito mais vantajoso financeiramente (Letra A);

- **Fácil Instalação:** basta instalar e configurar o servidor central que fará a segurança da rede. Assim, os dispositivos só conseguirão acessar a rede a partir da instalação do cliente em seus dispositivos;

- **Administração Centralizada:** é possível centralizar a rede a partir do sistema gerenciador de segurança, no caso, o endpoint. Assim, o gerente de infraestrutura de TI da empresa ou o parceiro

terceirizado passa a ser o administrador do servidor de endpoint, sendo responsável pelo controle para revogar e conceder permissões de uso, auditar a segurança, obter relatórios, monitorar a rede, entre outros aspectos. Essas ações ocorrem por meio de um orquestrador ou portal de gerenciamento remoto;

- Bloqueio de Ações Indesejadas: apesar de muitas vezes não ser intencional, invasões indesejadas podem ser frequentes no ambiente organizacional. Por exemplo, se um funcionário de uma empresa coloca um pendrive infectado no computador de trabalho, pode causar uma vulnerabilidade no sistema. Por esse motivo, algumas empresas possuem políticas de segurança que impedem que funcionários pluguem dispositivos internos em estações de trabalho. Assim, softwares de segurança de endpoint ajudam a bloquear esse tipo de atividade;

- Fácil integração com novas tecnologias: como o sistema de segurança é apenas um composto, torna-se mais fácil que novas soluções sejam adicionadas ao sistema de forma simples. Assim, as empresas têm acesso às atualizações de forma segura e unificada, de uma vez só, para todos os dispositivos.

Gabarito: Letra A

---

27. (FGV / PC-MA – 2012) Um funcionário em uma viagem de negócios teve de levar em seu notebook arquivos classificados para uma reunião com clientes. Ele foi então aconselhado pelo pessoal de suporte da empresa a instalar um antivírus em sua máquina. Resistindo à orientação recebida, o funcionário argumentou que:

I. O software antivírus deixa minha máquina muito lenta.
II. Eu não preciso de um software antivírus porque eu nunca abro arquivos anexados em e-mails de pessoas que eu não conheço.
III. Tantas pessoas usam a Internet, eu sou apenas um na multidão. Ninguém vai me achar.

São motivos válidos para a não instalação de um programa antivírus:

a) somente a opção I
b) somente a opção II
c) somente a opção III
d) somente as opções I e II
e) nenhuma das opções.

Comentários:

(I) Errado, esse não é um motivo válido porque a máquina não fica muito lenta – ele consome recursos computacionais, mas não deixam a máquina muito lenta; (II) Errado, abrir anexos de e-mail de pessoas conhecidas também pode ocasionar infecções, além disso existem outras formas de contaminação por vírus; (III) Errado, a infecção por malwares pode ocorrer mesmo sem acesso à internet como, por exemplo, através de mídias removíveis.

Gabarito: Letra E

QUESTÕES COMENTADAS – VUNESP

28.(VUNESP / PC-SP – 2022) Visando aumentar a proteção e a segurança dos computadores, diversas ferramentas *antimalware* podem ser utilizadas, como as *antirootkit*, que visam impedir que:

a) sejam capturadas e armazenadas posições do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o *mouse* é clicado.

b) sejam capturadas e armazenadas as teclas digitadas pelo usuário no teclado do computador.

c) um programa se instale para permitir o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

d) um conjunto de programas e técnicas escondam e assegurem a presença de um invasor ou de outro código malicioso em um computador comprometido.

e) um programa execute, além das funções para as quais foi aparentemente projetado, outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Comentários:

(a) Errado, ele não impede a ação de screenloggers; (b) Errado, ele não impede a ação de keyloggers; (c) Errado, ele não impede a ação de backdoors; (d) Correto, antirootkits impedem a ação de rootkits; (e) Errado, ele não impede a ação de trojans.

Gabarito: Letra D

29.(VUNESP / Câmara de Sertãozinho-SP – 2019) Programas antivírus representam uma importante ferramenta aos usuários de computadores, sendo que tais programas:

a) não atuam sobre arquivos presentes em mídias removíveis, como é o caso de pen drives.

b) não atuam sobre programas com determinadas extensões, como .pdf ou .docx.

c) não atuam sobre programas com tamanho de até 50 KB.

d) devem ser executados somente em dois momentos: quando o computador é ligado e quando é desligado.

e) devem ser mantidos atualizados, assim como as definições de vírus presentes nesses programas.

Comentários:

(a) Errado, eles atuam com ênfase em arquivos presentes em mídias removíveis, uma vez que essa é uma típica fonte de malwares; (b) Errado, eles podem atuar em programas com essas extensões; (c) Errado, não existe essa limitação de tamanho; (d) Errado, o ideal é que sejam executados em tempo real a todo momento; (e) Correto, o ideal é que sejam mantidos atualizados frequentemente assim como as suas definições de vírus.

Gabarito: Letra E

---

30. **(VUNESP / Câmara de Monte Alto - SP – 2019)** Um usuário necessita instalar, em seu computador, um programa antivírus. Duas das possíveis opções que ele pode selecionar para tal finalidade são os programas

a) McAfee e TrueCript.
b) Norton e Predator.
c) Bitdefender e 7-Zip.
d) AVG e Avast.
e) Kaspersky e WinRAR.

Comentários:

(a) Errado, Truecript é um software de criptografia de disco rígido; (b) Errado, desconheço antivírus chamado Predator; (c) Errado, 7-Zip é um software de compactação/descompactação de arquivos; (d) Correto; (e) Errado, WinRAR é um software de compactação/descompactação de arquivos.

Gabarito: Letra D

---

31. **(VUNESP / Prefeitura de Ribeirão Preto-SP – 2018)** A respeito da execução de um programa antivírus em um computador, é correto afirmar que:

a) somente pode ser feita em intervalos iguais ou maiores do que uma semana.
b) não pode ser feita quando não há Internet de banda larga disponível no computador.
c) só pode ser feita quando ocorre uma atualização do sistema operacional do computador.
d) pode ser programada para ocorrer, por exemplo, uma vez por dia.
e) não pode ser feita em sistemas operacionais instalados há mais de dois anos no computador.

Comentários:

(a) Errado, não só pode como é recomendável que seja feito com alta frequência; (b) Errado, pode ser feito inclusive sem acesso à internet; (c) Errado, pode ser feita independentemente da

atualização do sistema operacional; (d) Correto, pode ser programada para ocorrer com qualquer frequência desejada; (e) Errado, não existe essa limitação.

Gabarito: Letra D

QUESTÕES COMENTADAS – CESGRANRIO

32. **(CESGRANRIO / Petrobrás – 2011)** Dentre as ferramentas que auxiliam a proteção de um computador, inclui-se o:

a) HTTP.
b) driver do HD.
c) FTP.
d) RSS.
e) antivirus.

Comentários:

(a) Errado, isso é um protocolo de comunicação; (b) Errado, isso é uma mídia de armazenamento; (c) Errado, isso é um protocolo de comunicação; (d) Errado, isso é um formato de distribuição de informações em tempo real; (e) Correto, eles realmente auxiliam na proteção de um computador.

Gabarito: Letra E

QUESTÕES COMENTADAS – DIVERSAS BANCAS

33. **(FUNDATEC / IPE SAÚDE – 2022)** Em segurança da informação, utiliza-se o antivírus para proteção do computador contra vírus, que são códigos maliciosos e podem comprometer o funcionamento da máquina, bem como a integridade dos dados nela armazenados. Quando a remoção de um vírus pode comprometer o funcionamento do computador, o antivírus adota o seguinte procedimento:

a) Coloca o vírus em quarentena durante um tempo, enquanto busca por mais problemas relacionados a ele.
b) Apaga o vírus imediatamente e conserta os danos causados pela sua remoção.
c) Solicita que o usuário repare todos os arquivos comprometidos pelo vírus utilizando outra ferramenta.
d) Não toma providência alguma, pois, ao remover o vírus, o computador pode ficar instável.
e) Desliga imediatamente o computador para que o vírus não contamine outros programas.

Comentários:

Em regra, quando um antivírus detecta uma ameaça, há a opção de remoção ou envio para a quarentena. Como a questão afirmou que a remoção pode afetar o funcionamento do computador, o item não pode ser removido, então ele deve ser movido para a quarentena. Lembrando que a quarentena é uma área virtual onde o antivírus armazena arquivos identificados como possíveis vírus enquanto aguarda uma confirmação de identificação.

Gabarito: Letra A

---

34. **(IDIB / Ministério da Economia – 2021)** São softwares que detectam e removem programas maliciosos, como vírus e worms, protegendo os sistemas de computador contra essas ameaças. Assinale a alternativa que apresenta um desses programas:

a) Pipefy
b) Asana
c) Comodo
d) Avant
e) Acrobat

Comentários:

(a) Errado, esse é um software para gerenciamento de fluxos de trabalho; (b) Errado, esse é um software para gerenciamento de equipes e projetos; (c) Correto; (d) Errado, desconheço software com esse nome – acredito que a banca quis confundir com Avast; (e) Errado, esse é um software para leitura de PDF.

Gabarito: Letra C

---

35. **(QUADRIX / CONRERP/2ª Região – 2019)** O software antivírus, após sua instalação e configuração, não necessita de ser atualizado pelo fabricante, pois já contém uma lista de assinaturas válidas e consegue eliminar todas as formas de vírus.

Comentários:

Ele precisa – sim – ser atualizado pelo fabricante! Aliás, essa atualização deve ocorrer com alta frequência, uma vez que novas ameaça surgem diariamente no mundo inteiro. Dessa forma, a lista de assinaturas válidas deve ser constantemente revisitada.

Gabarito: Errado

---

36. **(OBJETIVA / Prefeitura de Tupanci do Sul - RS – 2019)** Atenção! Para responder às questões de Informática, a menos que seja explicitamente informado o contrário, considerar que os programas mencionados encontram-se na versão Português-BR e em sua configuração padrão de instalação, possuem licença de uso, o mouse está configurado para destros, um clique ou duplo clique correspondem ao botão esquerdo do mouse, e teclar corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Dessa forma, as teclas de atalho, os menus, os submenus, as barras, os ícones e os demais itens que compõem os programas abordados nesta prova encontram-se na configuração padrão.

    Em conformidade com a Cartilha de Segurança para Internet, sobre mecanismos de segurança, assinalar a alternativa que preenche a lacuna abaixo CORRETAMENTE:

    Ferramentas _____ são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

    a) pop-up's
    b) backups
    c) antispam
    d) antimalware

Comentários:

As ferramentas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador são as ferramentas antimalware.

Gabarito: Letra D

---

37. (IBADE / SAAE de Vilhena - RO – 2019) Qual dos softwares abaixo é um Anti-Virus?

a) Avast
b) Excel
c) Squirrel
d) WinRAR
e) WinZip

Comentários:

(a) Correto, é um antivírus; (b) Errado, é uma ferramenta de planilha eletrônica; (c) Errado, esse é um recurso de webmail do Linux; (d) Errado, essa é uma ferramenta de compactação de arquivos; (e) Errado, essa é uma ferramenta de compactação de arquivos.

Gabarito: Letra A

---

38. (IADES / CAU-MT – 2019) O antivírus tem como responsabilidade proteger o computador de potenciais arquivos maliciosos:

a) A capacidade de detecção de novas ameaças de um antivírus independe de ele estar atualizado.
b) O antivírus tem como principal responsabilidade proteger a navegação do usuário na internet.
c) São tão importantes para o funcionamento de um computador que todas essas máquinas já vêm com um antivírus previamente instalado.
d) Quando um antivírus está ativado, o computador está seguro contra qualquer tipo de ataque.
e) Uma das capacidades do antivírus é inspecionar os anexos do correio eletrônico, procurando por possíveis ameaças.

Comentários:

(a) Errado, novos vírus surgem todos os dias, logo suas assinaturas precisam ser identificadas para atualizar a base de dados dos antivírus de modo que ele fique atualizado e consiga detectar novas ameaças; (b) Errado, sua principal responsabilidade é proteger computadores de malwares e, não, a navegação na internet; (c) Errado, não é obrigatório ter um antivírus para o funcionamento de um computador, logo eles não são necessariamente pré-instalados; (d) Errado, ele não é infalível; (e) Correto, ele realmente é capaz de inspecionar os anexos do correio eletrônico, procurando por possíveis ameaças.

Gabarito: Letra E

---

39. (UECE-CEV / DETRAN/CE – 2018) Um software antivírus é um programa responsável por:

a) dividir os recursos da máquina entre os processos em execução.

b) prevenir, procurar, detectar e remover programas maliciosos.
c) arranjar em espaço contíguo os arquivos contidos em disco.
d) realizar a atualização do sistema operacional.

Comentários:

(a) Errado, essa não é uma função de antivírus; (b) Correto, essa é uma função típica de antivírus; (c) Errado, essa não é uma função de antivírus; (d) Errado, essa não é uma função de antivírus;

Gabarito: Letra B

---

40. (FAPEC / UFMS – 2018) A prevenção, detecção e a eliminação de vírus são feitos por aplicativos denominados antivírus. É um exemplo de antivírus:

a) AVG.
b) FTP.
c) Keylogger.
d) Spam.
e) Malware.

Comentários:

(a) Correto, esse é um exemplo de software antivírus; (b) Errado, isso é um exemplo protocolo de comunicação; (c) Errado, isso é um exemplo de software malicioso; (d) Errado, esse é uma mensagem eletrônica indesejável; (e) Errado, isso é um software malicioso.

Gabarito: Letra A

---

41. (CPCON / Prefeitura de São José dos Pinhais-PB – 2018) Alguns softwares de antivírus têm se popularizado bastante e construído marcas sólidas e facilmente reconhecíveis por seus usuários. NÃO é um exemplo de software antivírus:

a) McAfee.
b) NetBeans.
c) Avast.
d) Kaspersky.
e) Norton.

Comentários:

(a) Correto, trata-se de um exemplo de software antivírus; (b) Errado, trata-se de uma ferramenta de programação; (c) Correto, trata-se de um exemplo de software antivírus; (d) Correto, trata-se de um exemplo de software antivírus; (e) Correto, trata-se de um exemplo de software antivírus.

Gabarito: Letra B

---

42. (IF-CE / IF-CE – 2017) São ações desejáveis em um programa de antivírus:

a) proteção contra arquivos infectados de e-mail e varredura à procura de vírus em tempo real.
b) verificação contínua de defeitos de discos rígidos e varredura à procura de vírus em tempo real.
c) alerta de instalação de aplicativos infectados e impedimento de formatação de disco rígido.
d) proteção contra arquivos infectados de e-mail e atualização de softwares aplicativos.
e) atualização automática do programa de antivírus e criptografia de mensagens de e-mail.

Comentários:

(a) Correto, é altamente desejável que ele seja capaz de verificar e-mails, uma vez que essa é uma fonte típica de contaminação por malwares – de preferência, em tempo real; (b) Errado. Ele não é utilizado para detectar defeitos de discos rígidos; (c) Errado. Ele não deve impedir a formatação de disco rígido; (d) Errado. Ele não deve ser utilizado para atualizar softwares aplicativos; (e) Errado. Ele não deve criptografar mensagens de e-mail.

Gabarito: Letra A

---

43. (IESES / Prefeitura de São José do Cerrito – 2017) O software que utilizaríamos para protegermos nossos arquivos de programas maliciosos que desejassem controlar nosso computador são da categoria de softwares de:

a) Gerenciamento de Banco de Dados.
b) Antivírus.
c) Backup.
d) Processamento de Textos.

Comentários:

O software que utilizaríamos para protegermos nossos arquivos de programas maliciosos que desejassem controlar nosso computador são da categoria de softwares de... antivírus.

Gabarito: Letra B

---

44. (QUADRIX / CRB 6ª Região – 2017) Em um ambiente público, com um microcomputador e um sistema operacional para desktop com acesso à internet, as diversas vulnerabilidades e falhas de segurança são uma constante preocupação ao usuário, seja navegando na internet ou acessando o microcomputador. Qual das seguintes alternativas auxilia um usuário padrão a se proteger de vírus e programas maliciosos?

a) Backup.
b) PROXY.
c) Planilhas eletrônicas.
d) Antivírus.
e) Rede IP.

Comentários:

O software utilizado para auxiliar um usuário padrão a se proteger de vírus e outros programas maliciosos é também chamado de... antivírus.

Gabarito: Letra D

---

45. (CS-UFG / UFG – 2017) Antivírus são programas de computador voltados para a eliminação e o controle de pragas virtuais, tais como:

a) spyware e firewall.
b) spam e boot.
c) worms e cavalos de Troia.
d) macro e log.

Comentários:

(a) Errado, Firewall é uma ferramenta de proteção e segurança; (b) Errado, boot é o nome dado a inicialização de um sistema operacional; (c) Correto, ambos podem ser eliminados ou controlados por softwares antivírus; (d) Errado, macro é um conjunto de instruções e log é o processo de registro de informações.

Gabarito: Letra C

---

46. (IBADE / IPERON-RO – 2017) Um usuário precisa instalar em seu microcomputador um software antivírus de mercado, para se prevenir de ataques. Um software dessa categoria é o:

a) Media Player.
b) Switcher.
c) Kaspersky.
d) Adware.
e) Broadsheeet.

Comentários:

(a) Errado, isso é um exemplo de player de vídeo; (b) Errado, isso não existe; (c) Correto, isso é um exemplo de software antivírus; (d) Errado, isso é um exemplo de software malicioso; (e) Errado, isso não existe.

Gabarito: Letra C

---

47. (QUADRIX / CFO-DF – 2017) Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

Comentários:

Filtros Antispam vêm integrado à maioria dos webmails e clientes de e-mails para separar os e-mails desejados dos indesejados (chamados de spams). A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro "aprende" a distinguir as mensagens. Para realizar esse procedimento, ele precisa ter acesso ao conteúdo desses e-mails.

Gabarito: Errado

---

48. (IF/PA / IF/PA – 2016) O software que já vem integrado à maioria dos programas leitores de e-mails e que permite separar os e-mails desejados dos indesejados (como, por exemplo, propagandas) é o:

a) Antivírus.
b) Firewall.
c) Filtro Antispam.
d) Filtro de janelas de pop-up.
e) Algoritmo criptográfico.

Comentários:

O software que já vem integrado à maioria dos programas leitores de e-mails e que permite separar os e-mails desejados dos indesejados (como, por exemplo, propagandas) é o Filtro Antispam.

Gabarito: Letra C

---

49. (IDECAN / UE-RN – 2016) O software responsável por detectar, evitar e atuar na neutralização ou remoção de programas mal-intencionados denomina-se:

a) Rootkit.
b) Antivírus.
c) Backdoor.
d) Keylogger.

Comentários:

(a) Errado, isso é um exemplo de software mal-intencionado; (b) Correto, antivírus são softwares responsáveis por detectar, evitar e atuar na neutralização ou remoção de programas mal-intencionados; (c) Errado, isso é um exemplo de software mal-intencionado; (d) Errado, isso é um exemplo de software mal-intencionado;

Gabarito: Letra B

---

50. (UFCG / UFCG – 2016) Antivirus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus de computadores. São exemplos de antivirus disponíveis no mercado, EXCETO:

a) Avira Free Antivirus.
b) AVG AntiVirus.
c) Comodo.
d) Windows Defender.
e) Formoid.

Comentários:

(a) Correto, trata-se de um exemplo de antivírus; (b) Correto, trata-se de um exemplo de antivírus; (c) Correto, trata-se de um exemplo de antivírus; (d) Correto, trata-se de um exemplo de antivírus e antispyware nessa época; (e) Errado, isso não é um exemplo de antivírus.

Gabarito: Letra E

---

51. (CRO-SC / CRO-SC – 2016) São exemplos de programas antivírus todos os seguintes, EXCETO:

a) Karspersky
b) Avast
c) Quicken
d) AVG

Comentários:

(a) Correto, esse é um exemplo de programa antivírus; (b) Correto, esse é um exemplo de programa antivírus; (c) Errado, esse não é um exemplo de programa antivírus; (d) Correto, esse é um exemplo de programa antivírus.

Gabarito: Letra C

---

52. **(COPEVE-UFAL / UFAL – 2016)** Após a detecção de um vírus, normalmente os softwares antivírus oferecem duas opções para o usuário: deletar ou colocar em quarentena. Nesse contexto, quando é mais indicado colocar o arquivo em quarentena, ao invés de apagá-lo?

a) Quando o arquivo infectado é considerado importante para o bom funcionamento do sistema ou de grande valor para o usuário.

b) Quando o antivírus foi capaz de remover completamente o vírus do arquivo infectado, a fim de ficar um tempo em observação.

c) Quando o arquivo infectado possui tamanho longo, normalmente acima de 20MB, a fim de otimizar o tempo de execução do antivírus.

d) É sempre mais indicado excluir definitivamente o arquivo, caso contrário, o vírus volta à ativa na próxima vez que o computador for reiniciado.

e) Quando o arquivo infectado é um executável totalmente desconhecido que não pertence ao sistema operacional nem a nenhum software instalado pelo usuário.

Comentários:

(a) Correto. Se o arquivo for importante, recomenda-se colocá-lo em quarentena; (b) Errado. Nesse caso, é melhor removê-lo; (c) Errado, o tamanho é irrelevante para essa decisão; (d) Errado, por vezes o arquivo pode ser importante tanto para o usuário quanto para o sistema; (e) Errado, mesmo sendo um arquivo executável, pode ser um falso-positivo.

Gabarito: Letra A

---

53. **(IADES / ELETROBRÁS – 2015)** Os arquivos de computador podem ser contaminados por vírus. A forma mais comum de contaminação ocorre por meio de mensagens eletrônicas (e-mail). Para evitar contaminações e realizar a recuperação de arquivos contaminados, são utilizados os programas antivírus. A esse respeito, é correto afirmar que a área de armazenamento em que os programas antivírus costumam guardar os arquivos contaminados de um computador denomina-se:

a) lixeira.
b) disco rígido.
c) pasta spam.
d) área de trabalho.
e) quarentena.

Comentários:

A área de armazenamento em que os programas antivírus costumam guardar os arquivos contaminados de um computador é denominada... quarentena.

Gabarito: Letra E

---

54. (INAZ DO PARÁ / Prefeitura de Terra Alta – 2015) Atualmente, a informação representa o maior bem dentro de qualquer organização; assim, existem diversas formas de se garantir a proteção da mesma. Dentre os diversos procedimentos existentes, assinale qual pode ser considerada a forma mais segura para proteção desta informação:

a) Backup.
b) Firewall.
c) Ifconfig.
d) Antivírus.
e) Dump.

Comentários:

Questão horrorosa! Dependendo do critério utilizado, backup, firewall e antivírus podem ser consideradas formas seguras em certo nível para proteção de informação.

Gabarito: Letra D

---

55. (COSEAC / CLIN – 2015) São normalmente funcionalidades de um software antivírus as abaixo relacionadas, EXCETO:

a) impedir que um hacker explore vulnerabilidades em seu sistema.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) verificar continuamente os discos rígidos e discos removíveis.

Comentários:

(a) Errado, essa seria uma possível funcionalidade de firewalls; (b) Correto, analisar downloads é uma função comum de antivírus; (c) Correto, procurar programas maliciosos em anexos de e-mails é uma função comum de antivírus; (d) Correto, verificar discos rígidos e removíveis é uma função comum de antivírus.

Gabarito: Letra A

---

56. (PR-4 UFRJ/ UFRJ – 2015) Os antivírus são programas de computador concebidos para prevenir, detectar e eliminar vírus de um computador. São exemplos de antivírus:

a) AVG, Avast e Avira.
b) AVG, Hoax e FTP.
c) Hoax, Avast e Avira.
d) Spam, Keylogger e AVG.
e) Spam, Avast e Hoax.

Comentários:

(a) Correto, todos são exemplos de antivírus; (b) Errado, Hoax é um boato e FTP é um protocolo; (c) Errado, Hoax é um boato; (d) Errado, Spam é uma mensagem de e-mail indesejada e Keylogger é um software malicioso; (e) Errado, Spam é uma mensagem de e-mail indesejada e Hoax é um boato.

Gabarito: Letra A

---

57. **(FUNIVERSA / SEAP-DF – 2015)** Um dos procedimentos de segurança da informação é instalar no computador o anti-spyware e o antivírus, pois o anti-spyware é um aplicativo que complementa o antivírus.

Comentários:

De fato, antivírus não têm uma eficácia tão boa no combate aos spywares. Dessa forma, para manter o computador com uma proteção razoável, é interessante usar um antispyware, que complementa a ação do antivírus, combatendo os programas maliciosos que o antivírus tem problemas em combater.

Gabarito: Correto

---

58. **(UFBA / UFOB – 2014)** Para identificar um vírus, o antivírus faz uma comparação entre o arquivo que chega por algum meio de entrada e uma biblioteca de informações sobre os vários tipos de vírus, o que explica a importância de manter o antivírus sempre atualizado.

Comentários:

Perfeito! Essa biblioteca é chamada de arquivo de assinaturas. É bastante recomendável manter o arquivo de assinaturas sempre atualizado. Recomenda-se também configurar o antimalware para atualizá-lo automaticamente pela rede e, de preferência, diariamente.

Gabarito: Correto

---

59. **(FUMARC / Câmara Municipal de Mariana/MG – 2014)** São exemplos de softwares antivírus, EXCETO:

a) Avast.
b) AVG.
c) Kaspersky.
d) Microsoft Windows Defender, disponível no Windows 7.

Comentários:

(a) Correto, é um exemplo de software antivírus; (b) Correto, é um exemplo de software antivírus; (c) Correto, é um exemplo de software antivírus; (d) Errado, ele era apenas um antispyware na época dessa questão.

Gabarito: Letra D

60.(CETRO / FUNDAÇÃO CASA – 2014) Sobre os softwares antivírus, assinale a alternativa correta.

a) Algumas empresas mantêm softwares antivírus em seus websites e oferecem os serviços do software via Internet.
b) Cada antivírus protege contra um único tipo de software malicioso.
c) Cada antivírus utiliza somente uma estratégia de detecção de softwares maliciosos.
d) Não existem antivírus que protejam os computadores em tempo real.
e) A única coisa que o antivírus consegue fazer é detectar o vírus e eliminar os arquivos infectados.

Comentários:

(a) Correto, existem antivírus online capazes de escanear arquivos; (b) Errado, antivírus protegem contra diversos tipos de softwares maliciosos; (c) Errado, antivírus utilizam diversas estratégias de detecção de softwares maliciosos; (d) Errado, existem diversos antivírus capazes de proteger computadores em tempo real; (e) Errado, ele pode colocá-lo em quarentena.

Gabarito: Letra A

61.(COSEAC / Prefeitura de Niterói/RJ – 2014) São funções rotineiras de um programa antivírus as abaixo relacionadas, EXCETO:

a) identificar e eliminar vírus e outros tipos de malwares.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) possibilitar a atualização das assinaturas de novos vírus de forma automática.
e) efetuar o controle de configuração dos softwares na rede.

Comentários:

(a) Correto, programas antivírus têm como função identificar e eliminar vírus e outros tipos de malwares; (b) Correto, programas antivírus têm como função analisar downloads da Internet; (c) Correto, programas antivírus têm como função procurar programas maliciosos em anexos de e-mails; (d) Correto, programas antivírus têm função de possibilitar a atualização de assinaturas de novos vírus de forma automática; (e) Errado, programas antivírus não realizam controle de configuração de softwares na rede – essa não é uma de suas funções.

Gabarito: Letra E

---

62. (BIO-RIO / Prefeitura de Três Rios – 2014) Atualmente, com o objetivo de evitar a contaminação dos computadores é necessário instalar um software antivírus na máquina. Dois exemplos de antivírus são:

a) McAfee e Shirink
b) Safari e Linkedin
c) Avast e Psafe
d) AVG e Winrar
e) Bing e Android.

Comentários:

(a) Errado, Shirink não existe; (b) Errado, Safari é um navegador e Linkedin é uma rede social; (c) Correto, ambos são softwares antivírus; (d) Errado, Winrar é um compactador/descompactador de arquivos; (e) Errado, Bing é uma ferramenta de busca e Android é um sistema operacional móvel.

Gabarito: Letra C

---

63. (MPE-RS / MPE-RS – 2014) Código Malicioso é o termo genérico usado para referir programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Qual das alternativas abaixo NÃO apresenta um tipo de código malicioso?

a) Antivírus.
b) Bot.
c) Worm.
d) Spyware
e) Cavalo de Tróia.

Comentários:

(a) Correto, trata-se de um software para proteção contra código malicioso; (b) Errado, trata-se de um exemplo de código malicioso; (c) Errado, trata-se de um exemplo de código malicioso; (d)

Errado, trata-se de um exemplo de código malicioso; (e) Errado, trata-se de um exemplo de código malicioso.

Gabarito: Letra A

64.(BIO-RIO / EMGEPRON– 2014) A instalação de um antivírus em um microcomputador é de suma importância para o seu funcionamento satisfatório, no que diz respeito à segurança dos dados e ao próprio desempenho da máquina. Dois exemplos de programas antivírus são:

a) iTunes e Avast!
b) Avast! e McAfee
c) McAfee e WinZip
d) WinZip e iTunes.

Comentários:

(a) Errado, iTunes é um player de música; (b) Correto, ambos são programas antivírus; (c) Errado, WinZip é um compactador/descompactar de arquivos; (d) Errado, WinZip é um compactador e descompactar de arquivos, e iTunes é um player de música.

Gabarito: Letra B

65.(UFBA / UFBA – 2013) A instalação e o uso de programas "antivírus" aumentam a segurança dos arquivos armazenados no computador.

Comentários:

Perfeito! Eles ajudam bastante a melhorar o nível de segurança dos arquivos armazenados em um computador.

Gabarito: Correto

---

66. (AOCP / Colégio Pedro II – 2013) Antivírus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus do computador. Assinale a alternativa que NÃO representa um antivírus.

a) Avast.
b) AVG.
c) Microsoft Security Essentials.
d) Kaspersky.
e) WinRAR.

Comentários:

(a) Correto, trata-se de um antivírus; (b) Correto, trata-se de um antivírus; (c) Correto, trata-se de um antivírus; (d) Correto, trata-se de um antivírus; (e) Errado, trata-se de compactador e descompactador de arquivos.

Gabarito: Letra E

---

67. (FUNCAB / SC/CE – 2013) O software antivírus é um software da categoria dos(as):

a) sistemas operacionais.
b) linguagens de programação.
c) softwares utilitários.
d) firmwares.
e) softwares aplicativos.

Comentários:

Antivírus é um tipo de software utilitário, isto é, são utilizados para suprir deficiências dos sistemas operacionais, melhorando seus recursos.

Gabarito: Letra C

---

68. (FUNCAB / CODATA – 2013) Sobre sistemas antivírus, é correto afirmar:

a) Garantem integralmente a segurança das informações em seu computador.
b) Distribuem os arquivos contaminados pela rede do seu computador, visando a enfraquecer o vírus.
c) Por padrão, movem para a lixeira arquivos contaminados do seu computador.
d) Os programas antivírus examinam os arquivos antes de abri-los e notificam o usuário do computador, caso encontrem um arquivo potencialmente não seguro.
e) garantem a recuperação de arquivos danificados por Cavalo de Troia.

Comentários:

(a) Errado, eles não garantem integralmente a segurança das informações de um computador; (b) Errado, eles impedem a distribuição de arquivos contaminados; (c) Errado, eles notificam o usuário para que ele decida o que fazer; (d) Correto, eles realmente examinam o arquivo e notificam o usuário quando encontram arquivos potencialmente perigosos; (e) Errado, não há garantia de recuperação de arquivos infelizmente.

Gabarito: Letra D

---

69. (CETRO / Prefeitura de Manaus – 2012) Quanto ao processo de quarentena, que alguns softwares antivírus oferecem, é correto afirmar que:

a) quarentena é uma área separada em um disco rígido.

b) apesar de isolar os arquivos, a quarentena não consegue impedir que outros arquivos sejam infectados pelo software suspeito.

c) somente o software antivírus tem a capacidade de colocar um software suspeito em quarentena.

d) após determinado tempo, os arquivos em quarentena são eliminados automaticamente.

e) arquivos em quarentena sempre são eliminados do computador, já que não existe solução para o problema deles (infecção).

Comentários:

(a) Correto, quarentena é uma área virtual onde o antivírus armazena arquivos identificados como possíveis vírus enquanto ele aguarda uma confirmação de identificação; (b) Errado, ela consegue – sim – impedir que outros arquivos sejam infectados porque ela isola o arquivo que infecta; (c) Errado, um usuário pode colocar um software suspeito em quarentena manualmente; (d) Errado, eles não são eliminados até que o usuário o deseje; (e) Errado, eles não são necessariamente eliminados do computador.

Gabarito: Letra A

---

70. (FUNCAB / SESC-BA – 2012) Considere que o técnico da área de suporte da empresa na qual você trabalha tenha detectado, em seu computador, um Cavalo de Troia. O recurso de computador que pode ter auxiliado nessa localização foi:

a) Ferramenta de Busca Google
b) Firewall
c) Sistema Antivírus
d) Gerenciador de Tarefas.
e) Fragmentador.

Comentários:

O recurso de computador que pode ter auxiliado na localização de um software malicioso como um Cavalo de Troia é o Sistema Antivírus.

Gabarito: Letra C

---

71. (UECE-CEV / SEPLAG-CE – 2011) O software concebido com o objetivo de prevenir, detectar e eliminar programas maliciosos é denominado:

a) Bloco de Notas.
b) Microsoft Office.
c) Windows Explorer.
d) Antivírus.

Comentários:

(a) Errado, isso é um editor de texto; (b) Errado, isso é uma suíte de ferramentas de escritório; (c) Errado, isso é um navegador web; (d) Correto, isso é um software concebido com o objetivo de prevenir, detectar e eliminar programas maliciosos.

Gabarito: Letra D

---

72. (PONTUA / TRE-SC – 2011) Os sistemas antivírus são programas que têm o objetivo de detectar e, então, anular ou eliminar os vírus encontrados no computador. Marque V (Verdadeiro) e F (Falso) para os exemplos de programas antivírus:

( ) Norton.
( ) WinZip.
( ) McAfee.
( ) Kaspersky.
( ) Word.

A sequência CORRETA, de cima para baixo, é:

a) F – F – V – V – V.
b) V – F – V – V – F.
c) F – V – F – F – V.
d) V – V – V – V – F.

Comentários:

(V) Norton é um exemplo de programa antivírus; (F) WinZip é um compactador/descompactador de arquivos; (V) McAfee é um exemplo de programa antivírus; (V) Kaspersky é um exemplo de programa antivírus; (F) Word é um processador de texto.

Gabarito: Letra B

---

73. **(FUNCAB / Prefeitura de Porto Velho/RO – 2009)** Às vezes, os sistemas Antivírus detectam vírus desconhecidos que não podem ser eliminados com o conjunto de ferramentas disponíveis. Qual a função existente nos sistemas antivírus que permite isolar arquivos potencialmente infectados no seu computador?

a) Scanear;
b) Colocar em quarentena;
c) Reparar;
d) Congela;
e) Purgar.

Comentários:

A função existente nos sistemas antivírus que permite isolar arquivos potencialmente infectados em um computador é chamada de... quarentena.

Gabarito: Letra B

LISTA DE QUESTÕES – CESPE

1. **(CESPE / TRT8 – 2022)** Certo TRT deseja implementar uma solução de segurança cibernética que combine inteligência artificial, detecção comportamental e algoritmos de aprendizado de máquina para antecipar e prevenir ameaças conhecidas e desconhecidas.

   Com base nessa situação hipotética, assinale a opção que indica a solução requerida.

   a) NGAV.
   b) IPS
   c) IDS
   d) NIST
   e) WebProxy

2. **(CESPE / PC-AL – 2021)** A heurística é um dos métodos de detecção das ferramentas antimalware – como antivírus, antirootkit e antispyware – que se baseiam nas estruturas, instruções e características que o código malicioso possui para identificá-lo.

3. **(CESPE / BNB– 2018)** Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes.

4. **(CESPE / Polícia Federal – 2018)** Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

5. **(CESPE / CRBM – 2018)** O antispyware é conhecido como uma ferramenta complementar ao antivírus que deve ser executada frequentemente para checagem de possíveis ameaças que possam ter contaminado o sistema.

6. **(CESPE / CFO/DF – 2017)** Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

7. **(CESPE / TRE-PI – 2016)** A remoção de códigos maliciosos de um computador pode ser feita por meio de:

   a) anti-spyware.
   b) detecção de intrusão.
   c) anti-spam.
   d) anti-phishing.
   e) filtro de aplicações.

8. **(CESPE / TRE-MT – 2015)** A função principal de uma ferramenta de segurança do tipo antivírus é:

   a) monitorar o tráfego da rede e identificar possíveis ataques de invasão.
   b) verificar arquivos que contenham códigos maliciosos.
   c) fazer becape de segurança dos arquivos considerados críticos para o funcionamento do computador.
   d) bloquear sítios de propagandas na Internet.
   e) evitar o recebimento de mensagens indesejadas de email, tais como mensagens do tipo spams.

9. **(CESPE / Telebras – 2015)** Como os antivírus agem a partir da verificação da assinatura de vírus, eles são incapazes de agir contra vírus cuja assinatura seja desconhecida.

10. **(CESPE / TRT-10 Região – 2013)** Um computador em uso na Internet é vulnerável ao ataque de vírus, razão por que a instalação e a constante atualização de antivírus são de fundamental importância para se evitar contaminações.

11. **(CESPE / SESA-ES – 2013 – Letra C)** O anti-spyware, ao contrário do antivírus, propaga a proteção contra os vírus existentes de maneira semelhante a um antídoto, o que evita a contaminação de outros computadores da rede.

12. **(CESPE / Banco da Amazônia – 2012)** Antispywares são softwares que monitoram as máquinas de possíveis invasores e analisam se, nessas máquinas, há informações armazenadas indevidamente e que sejam de propriedade do usuário de máquina eventualmente invadida.

13. **(CESPE / Polícia Federal – 2012)** A fim de se proteger do ataque de um spyware — um tipo de vírus (malware) que se multiplica de forma independente nos programas instalados em um computador infectado e recolhe informações pessoais dos usuários —, o usuário deve instalar softwares antivírus e antispywares, mais eficientes que os firewalls no combate a esse tipo de ataque.

14. **(CESPE / PEFOCE – 2012)** O antivírus, para identificar um vírus, faz uma varredura no código do arquivo que chegou e compara o seu tamanho com o tamanho existente na tabela de alocação de arquivo do sistema operacional. Caso encontre algum problema no código ou divergência de tamanho, a ameaça é bloqueada.

15. **(CESPE / TCE-RO – 2012)** A manutenção da atualização dos antivírus auxilia no combate às pragas virtuais, como os vírus, que são mutantes.

16. **(CESPE / TRE/RJ – 2012)** Recomenda-se utilizar antivírus para evitar phishing-scam, um tipo de golpe no qual se tenta obter dados pessoais e financeiros de um usuário.

17. **(CESPE / Banco da Amazônia – 2012)** As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.

18. **(CESPE / TJ/AC – 2012)** O antispyware é um software que se destina especificamente a detectar e remover spywares, enquanto o antivírus é uma ferramenta que permite detectar e remover alguns programas maliciosos, o que inclui certos tipos de spywares.

19. **(CESPE / TJ/AC – 2012)** As ferramentas antispam permitem combater o recebimento de mensagens consideradas spam e, em geral, baseiam-se na análise do conteúdo das mensagens.

20. **(CESPE / IFB – 2011)** Ferramentas como firewall e antivírus para estação de trabalho não ajudam a reduzir riscos de segurança da informação.

21. **(CESPE / FUB – 2009)** O aplicativo antivírus original dessa versão do Windows é o Symantec Norton 2003.

LISTA DE QUESTÕES – FCC

22. (FCC / TRF/4ª Região – 2019) Caso uma praga virtual seja muito forte e sua remoção por meio do processo de deleção de arquivos ou programas infectados possa afetar todo o funcionamento do computador, os antivírus devem executar um processo:

a) para isolar completamente o sistema operacional do sistema de arquivos.
b) para criptografar o arquivo ou programa infectado inteiro, antes renomeando-o em uma cópia com os caracteres $~ na frente de seu nome.
c) que visa manter o sistema operacional suspenso.
d) que visa manter o arquivo ou programa infectado em quarentena.
e) que se incumbe apenas de renomear o arquivo ou programa infectado com os caracteres $~ na frente de seu nome.

23. (FCC / SEMEF/Manaus – 2019) Um técnico tentou instalar uma aplicação no seu computador, mas o antivírus o impediu mostrando uma mensagem que o programa era legítimo, mas que poderia ser usado por criminosos para danificar o computador ou furtar dados pessoais. Analisando que as perdas que poderiam ser causadas pela execução do software seriam menores do que as perdas causadas pela não execução, o técnico pensou nas seguintes possibilidades para instalar e executar o software:

I. Incluir o software na lista de exclusão do antivírus, ou seja, na lista de programas que o antivírus não deverá verificar.

II. Mudar o nome do software para um nome amigável parecido com o nome recursos legítimos do sistema operacional, a fim de enganar o antivírus no momento da instalação e execução.

III. Desativar/Pausar o antivírus por um tempo determinado, ou seja, pelo tempo necessário para instalar e usar o software para o que necessita.

IV. Colocar o antivírus no modo de verificação apenas de disco rígido, de forma que ele não seja ativado quando perceber um possível malware carregado na memória.

Considerando que o técnico estava utilizando um dos principais antivírus do mercado, permitirá a instalação e execução do software APENAS o que consta em:

a) III.
b) I e III.
c) I e IV.
d) III e IV.
e) I e II.

24. **(FCC / TRT/4ª Região – 2015)** Ferramentas antimalware, como os antivírus, procuram detectar, anular ou remover os códigos maliciosos de um computador. Para que estas ferramentas possam atuar preventivamente, diversos cuidados devem ser tomados, por exemplo:

a) utilizar sempre um antimalware online, que é mais atualizado e mais completo que os locais.

b) configurar o antimalware para verificar apenas arquivos que tenham a extensão .EXE.

c) não configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives e discos externos), pois podem ser uma fonte de contaminação que o usuário não percebe.

d) atualizar o antimalware somente quando o sistema operacional for atualizado, para evitar que o antimalware entre em conflito com a versão atual do sistema instalado.

e) evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

25. **(FCC / MPE/AM – 2013)** Com relação à utilização correta de ferramentas antimalware, considere:

I. É aconselhável utilizar programas antimalware on-line quando se suspeitar que o antimalware local esteja desabilitado ou comprometido ou quando se necessitar de uma segunda verificação.

II. Devem ser configuradas para verificar apenas arquivos executáveis, pois são os únicos que podem conter vírus e outros tipos de malware.

III. Deve-se evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

IV. Não é recomendável ter um antimalware instalado no computador, pois os programas on-line além de serem mais eficientes, são suficientes para proteger o computador.

Está correto o que se afirma APENAS em:

a) I, II e III.
b) III e IV.
c) I e III.
d) II e IV.
e) I.

LISTA DE QUESTÕES – FGV

26. (FGV / CGU – 2022) Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

a) redução de custos e facilidade de atualização;
b) configuração simplificada e fácil instalação de API;
c) monitoramento completo e antivírus atualizado;
d) administração descentralizada e facilidade de integração com novas tecnologias;
e) bloqueio de ações indesejadas e controle no lado do usuário.

27. (FGV / PC-MA – 2012) Um funcionário em uma viagem de negócios teve de levar em seu notebook arquivos classificados para uma reunião com clientes. Ele foi então aconselhado pelo pessoal de suporte da empresa a instalar um antivírus em sua máquina. Resistindo à orientação recebida, o funcionário argumentou que:

I. O software antivírus deixa minha máquina muito lenta.
II. Eu não preciso de um software antivírus porque eu nunca abro arquivos anexados em e-mails de pessoas que eu não conheço.
III. Tantas pessoas usam a Internet, eu sou apenas um na multidão. Ninguém vai me achar.

São motivos válidos para a não instalação de um programa antivírus:

a) somente a opção I
b) somente a opção II
c) somente a opção III
d) somente as opções I e II
e) nenhuma das opções.

LISTA DE QUESTÕES – VUNESP

28. (VUNESP / PC-SP – 2022) Visando aumentar a proteção e a segurança dos computadores, diversas ferramentas *antimalware* podem ser utilizadas, como as *antirootkit*, que visam impedir que:

a) sejam capturadas e armazenadas posições do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o *mouse* é clicado.

b) sejam capturadas e armazenadas as teclas digitadas pelo usuário no teclado do computador.

c) um programa se instale para permitir o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

d) um conjunto de programas e técnicas escondam e assegurem a presença de um invasor ou de outro código malicioso em um computador comprometido.

e) um programa execute, além das funções para as quais foi aparentemente projetado, outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

29. (VUNESP / Câmara de Sertãozinho-SP – 2019) Programas antivírus representam uma importante ferramenta aos usuários de computadores, sendo que tais programas:

a) não atuam sobre arquivos presentes em mídias removíveis, como é o caso de pen drives.

b) não atuam sobre programas com determinadas extensões, como .pdf ou .docx.

c) não atuam sobre programas com tamanho de até 50 KB.

d) devem ser executados somente em dois momentos: quando o computador é ligado e quando é desligado.

e) devem ser mantidos atualizados, assim como as definições de vírus presentes nesses programas.

30. (VUNESP / Câmara de Monte Alto - SP – 2019) Um usuário necessita instalar, em seu computador, um programa antivírus. Duas das possíveis opções que ele pode selecionar para tal finalidade são os programas

a) McAfee e TrueCript.

b) Norton e Predator.
c) Bitdefender e 7-Zip.
d) AVG e Avast.
e) Kaspersky e WinRAR.

31. **(VUNESP / Prefeitura de Ribeirão Preto-SP – 2018)** A respeito da execução de um programa antivírus em um computador, é correto afirmar que:

a) somente pode ser feita em intervalos iguais ou maiores do que uma semana.
b) não pode ser feita quando não há Internet de banda larga disponível no computador.
c) só pode ser feita quando ocorre uma atualização do sistema operacional do computador.
d) pode ser programada para ocorrer, por exemplo, uma vez por dia.
e) não pode ser feita em sistemas operacionais instalados há mais de dois anos no computador.

LISTA DE QUESTÕES – CESGRANRIO

32. **(CESGRANRIO / Petrobrás – 2011)** Dentre as ferramentas que auxiliam a proteção de um computador, inclui-se o:

a) HTTP.
b) driver do HD.
c) FTP.
d) RSS.
e) antivirus.

LISTA DE QUESTÕES – DIVERSAS BANCAS

33. **(FUNDATEC / IPE SAÚDE – 2022)** Em segurança da informação, utiliza-se o antivírus para proteção do computador contra vírus, que são códigos maliciosos e podem comprometer o funcionamento da máquina, bem como a integridade dos dados nela armazenados. Quando a remoção de um vírus pode comprometer o funcionamento do computador, o antivírus adota o seguinte procedimento:

a) Coloca o vírus em quarentena durante um tempo, enquanto busca por mais problemas relacionados a ele.
b) Apaga o vírus imediatamente e conserta os danos causados pela sua remoção.
c) Solicita que o usuário repare todos os arquivos comprometidos pelo vírus utilizando outra ferramenta.
d) Não toma providência alguma, pois, ao remover o vírus, o computador pode ficar instável.
e) Desliga imediatamente o computador para que o vírus não contamine outros programas.

34. **(IDIB / Ministério da Economia – 2021)** São softwares que detectam e removem programas maliciosos, como vírus e worms, protegendo os sistemas de computador contra essas ameaças. Assinale a alternativa que apresenta um desses programas:

a) Pipefy
b) Asana
c) Comodo
d) Avant
e) Acrobat

35. **(QUADRIX / CONRERP/2ª Região – 2019)** O software antivírus, após sua instalação e configuração, não necessita de ser atualizado pelo fabricante, pois já contém uma lista de assinaturas válidas e consegue eliminar todas as formas de vírus.

36. **(OBJETIVA / Prefeitura de Tupanci do Sul - RS – 2019)** Atenção! Para responder às questões de Informática, a menos que seja explicitamente informado o contrário, considerar que os programas mencionados encontram-se na versão Português-BR e em sua configuração padrão de instalação, possuem licença de uso, o mouse está configurado para destros, um clique ou duplo clique correspondem ao botão esquerdo do mouse, e teclar corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Dessa forma, as teclas de atalho, os menus, os submenus, as barras, os ícones e os demais itens que compõem os programas abordados nesta prova encontram-se na configuração padrão.

Em conformidade com a Cartilha de Segurança para Internet, sobre mecanismos de segurança, assinalar a alternativa que preenche a lacuna abaixo CORRETAMENTE:

Ferramentas _____ são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

a) pop-up's
b) backups
c) antispam
d) antimalware

37. **(IBADE / SAAE de Vilhena - RO – 2019)** Qual dos softwares abaixo é um Anti-Virus?

a) Avast
b) Excel
c) Squirrel
d) WinRAR
e) WinZip

38. **(IADES / CAU-MT – 2019)** O antivírus tem como responsabilidade proteger o computador de potenciais arquivos maliciosos:

a) A capacidade de detecção de novas ameaças de um antivírus independe de ele estar atualizado.
b) O antivírus tem como principal responsabilidade proteger a navegação do usuário na internet.
c) São tão importantes para o funcionamento de um computador que todas essas máquinas já vêm com um antivírus previamente instalado.
d) Quando um antivírus está ativado, o computador está seguro contra qualquer tipo de ataque.
e) Uma das capacidades do antivírus é inspecionar os anexos do correio eletrônico, procurando por possíveis ameaças.

39. **(UECE-CEV / DETRAN/CE – 2018)** Um software antivírus é um programa responsável por:

a) dividir os recursos da máquina entre os processos em execução.
b) prevenir, procurar, detectar e remover programas maliciosos.
c) arranjar em espaço contíguo os arquivos contidos em disco.
d) realizar a atualização do sistema operacional.

40. **(FAPEC / UFMS – 2018)** A prevenção, detecção e a eliminação de vírus são feitos por aplicativos denominados antivírus. É um exemplo de antivírus:

a) AVG.
b) FTP.

c) Keylogger.
d) Spam.
e) Malware.

41. **(CPCON / Prefeitura de São José dos Pinhais-PB – 2018)** Alguns softwares de antivírus têm se popularizado bastante e construído marcas sólidas e facilmente reconhecíveis por seus usuários. NÃO é um exemplo de software antivírus:

a) McAfee.
b) NetBeans.
c) Avast.
d) Kaspersky.
e) Norton.

42. **(IF-CE / IF-CE – 2017)** São ações desejáveis em um programa de antivírus:

a) proteção contra arquivos infectados de e-mail e varredura à procura de vírus em tempo real.
b) verificação contínua de defeitos de discos rígidos e varredura à procura de vírus em tempo real.
c) alerta de instalação de aplicativos infectados e impedimento de formatação de disco rígido.
d) proteção contra arquivos infectados de e-mail e atualização de softwares aplicativos.
e) atualização automática do programa de antivírus e criptografia de mensagens de e-mail.

43. **(IESES / Prefeitura de São José do Cerrito – 2017)** O software que utilizaríamos para protegermos nossos arquivos de programas maliciosos que desejassem controlar nosso computador são da categoria de softwares de:

a) Gerenciamento de Banco de Dados.
b) Antivírus.
c) Backup.
d) Processamento de Textos.

44. **(QUADRIX / CRB 6ª Região – 2017)** Em um ambiente público, com um microcomputador e um sistema operacional para desktop com acesso à internet, as diversas vulnerabilidades e falhas de segurança são uma constante preocupação ao usuário, seja navegando na internet ou acessando o microcomputador. Qual das seguintes alternativas auxilia um usuário padrão a se proteger de vírus e programas maliciosos?

a) Backup.
b) PROXY.
c) Planilhas eletrônicas.
d) Antivírus.
e) Rede IP.

45. **(CS-UFG / UFG – 2017)** Antivírus são programas de computador voltados para a eliminação e o controle de pragas virtuais, tais como:

a) spyware e firewall.
b) spam e boot.
c) worms e cavalos de Troia.
d) macro e log.

46. **(IBADE / IPERON-RO – 2017)** Um usuário precisa instalar em seu microcomputador um software antivírus de mercado, para se prevenir de ataques. Um software dessa categoria é o:

a) Media Player.
b) Switcher.
c) Kaspersky.
d) Adware.
e) Broadsheeet.

47. **(QUADRIX / CFO-DF – 2017)** Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

48. **(IF/PA / IF/PA – 2016)** O software que já vem integrado à maioria dos programas leitores de e-mails e que permite separar os e-mails desejados dos indesejados (como, por exemplo, propagandas) é o:

a) Antivírus.
b) Firewall.
c) Filtro Antispam.
d) Filtro de janelas de pop-up.
e) Algoritmo criptográfico.

49. **(IDECAN / UE-RN – 2016)** O software responsável por detectar, evitar e atuar na neutralização ou remoção de programas mal-intencionados denomina-se:

a) Rootkit.
b) Antivírus.
c) Backdoor.
d) Keylogger.

50. **(UFCG / UFCG – 2016)** Antivirus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus de computadores. São exemplos de antivirus disponíveis no mercado, EXCETO:

a) Avira Free Antivirus.

b) AVG AntiVirus.
c) Comodo.
d) Windows Defender.
e) Formoid.

51. **(CRO-SC / CRO-SC – 2016)** São exemplos de programas antivírus todos os seguintes, EXCETO:

a) Karspersky
b) Avast
c) Quicken
d) AVG

52. **(COPEVE-UFAL / UFAL – 2016)** Após a detecção de um vírus, normalmente os softwares antivírus oferecem duas opções para o usuário: deletar ou colocar em quarentena. Nesse contexto, quando é mais indicado colocar o arquivo em quarentena, ao invés de apagá-lo?

a) Quando o arquivo infectado é considerado importante para o bom funcionamento do sistema ou de grande valor para o usuário.

b) Quando o antivírus foi capaz de remover completamente o vírus do arquivo infectado, a fim de ficar um tempo em observação.

c) Quando o arquivo infectado possui tamanho longo, normalmente acima de 20MB, a fim de otimizar o tempo de execução do antivírus.

d) É sempre mais indicado excluir definitivamente o arquivo, caso contrário, o vírus volta à ativa na próxima vez que o computador for reiniciado.

e) Quando o arquivo infectado é um executável totalmente desconhecido que não pertence ao sistema operacional nem a nenhum software instalado pelo usuário.

53. **(IADES / ELETROBRÁS – 2015)** Os arquivos de computador podem ser contaminados por vírus. A forma mais comum de contaminação ocorre por meio de mensagens eletrônicas (e-mail). Para evitar contaminações e realizar a recuperação de arquivos contaminados, são utilizados os programas antivírus. A esse respeito, é correto afirmar que a área de armazenamento em que os programas antivírus costumam guardar os arquivos contaminados de um computador denomina-se:

a) lixeira.
b) disco rígido.
c) pasta spam.
d) área de trabalho.
e) quarentena.

54. **(INAZ DO PARÁ / Prefeitura de Terra Alta – 2015)** Atualmente, a informação representa o maior bem dentro de qualquer organização; assim, existem diversas formas de se garantir a proteção da mesma. Dentre os diversos procedimentos existentes, assinale qual pode ser considerada a forma mais segura para proteção desta informação:

a) Backup.
b) Firewall.
c) Ifconfig.
d) Antivírus.
e) Dump.

55. **(COSEAC / CLIN – 2015)** São normalmente funcionalidades de um software antivírus as abaixo relacionadas, EXCETO:

a) impedir que um hacker explore vulnerabilidades em seu sistema.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) verificar continuamente os discos rígidos e discos removíveis.

56. **(PR-4 UFRJ/ UFRJ – 2015)** Os antivírus são programas de computador concebidos para prevenir, detectar e eliminar vírus de um computador. São exemplos de antivírus:

a) AVG, Avast e Avira.
b) AVG, Hoax e FTP.
c) Hoax, Avast e Avira.
d) Spam, Keylogger e AVG.
e) Spam, Avast e Hoax.

57. **(FUNIVERSA / SEAP-DF – 2015)** Um dos procedimentos de segurança da informação é instalar no computador o anti-spyware e o antivírus, pois o anti-spyware é um aplicativo que complementa o antivírus.

58. **(UFBA / UFOB – 2014)** Para identificar um vírus, o antivírus faz uma comparação entre o arquivo que chega por algum meio de entrada e uma biblioteca de informações sobre os vários tipos de vírus, o que explica a importância de manter o antivírus sempre atualizado.

59. **(FUMARC / Câmara Municipal de Mariana/MG – 2014)** São exemplos de softwares antivírus, EXCETO:

a) Avast.
b) AVG.
c) Kaspersky.
d) Microsoft Windows Defender, disponível no Windows 7.

60. **(CETRO / FUNDAÇÃO CASA – 2014)** Sobre os softwares antivírus, assinale a alternativa correta.

a) Algumas empresas mantêm softwares antivírus em seus websites e oferecem os serviços do software via Internet.
b) Cada antivírus protege contra um único tipo de software malicioso.
c) Cada antivírus utiliza somente uma estratégia de detecção de softwares maliciosos.
d) Não existem antivírus que protejam os computadores em tempo real.
e) A única coisa que o antivírus consegue fazer é detectar o vírus e eliminar os arquivos infectados.

61. **(COSEAC / Prefeitura de Niterói/RJ – 2014)** São funções rotineiras de um programa antivírus as abaixo relacionadas, EXCETO:

a) identificar e eliminar vírus e outros tipos de malwares.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) possibilitar a atualização das assinaturas de novos vírus de forma automática.
e) efetuar o controle de configuração dos softwares na rede.

62. **(BIO-RIO / Prefeitura de Três Rios – 2014)** Atualmente, com o objetivo de evitar a contaminação dos computadores é necessário instalar um software antivírus na máquina. Dois exemplos de antivírus são:

a) McAfee e Shirink
b) Safari e Linkedin
c) Avast e Psafe
d) AVG e Winrar
e) Bing e Android.

63. **(MPE-RS / MPE-RS – 2014)** Código Malicioso é o termo genérico usado para referir programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Qual das alternativas abaixo NÃO apresenta um tipo de código malicioso?

a) Antivírus.
b) Bot.
c) Worm.
d) Spyware
e) Cavalo de Tróia.

64. **(BIO-RIO / EMGEPRON– 2014)** A instalação de um antivírus em um microcomputador é de suma importância para o seu funcionamento satisfatório, no que diz respeito à segurança dos dados e ao próprio desempenho da máquina. Dois exemplos de programas antivírus são:

a) iTunes e Avast!
b) Avast! e McAfee
c) McAfee e WinZip
d) WinZip e iTunes.

65. (UFBA / UFBA – 2013) A instalação e o uso de programas "antivírus" aumentam a segurança dos arquivos armazenados no computador.

66. (AOCP / Colégio Pedro II – 2013) Antivírus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus do computador. Assinale a alternativa que NÃO representa um antivírus.

a) Avast.
b) AVG.
c) Microsoft Security Essentials.
d) Kaspersky.
e) WinRAR.

67. (FUNCAB / SC/CE – 2013) O software antivírus é um software da categoria dos(as):

a) sistemas operacionais.
b) linguagens de programação.
c) softwares utilitários.
d) firmwares.
e) softwares aplicativos.

68. (FUNCAB / CODATA – 2013) Sobre sistemas antivírus, é correto afirmar:

a) Garantem integralmente a segurança das informações em seu computador.
b) Distribuem os arquivos contaminados pela rede do seu computador, visando a enfraquecer o vírus.
c) Por padrão, movem para a lixeira arquivos contaminados do seu computador.
d) Os programas antivírus examinam os arquivos antes de abri-los e notificam o usuário do computador, caso encontrem um arquivo potencialmente não seguro.
e) garantem a recuperação de arquivos danificados por Cavalo de Troia.

69. (CETRO / Prefeitura de Manaus – 2012) Quanto ao processo de quarentena, que alguns softwares antivírus oferecem, é correto afirmar que:

a) quarentena é uma área separada em um disco rígido.

b) apesar de isolar os arquivos, a quarentena não consegue impedir que outros arquivos sejam infectados pelo software suspeito.

c) somente o software antivírus tem a capacidade de colocar um software suspeito em quarentena.

d) após determinado tempo, os arquivos em quarentena são eliminados automaticamente.

e) arquivos em quarentena sempre são eliminados do computador, já que não existe solução para o problema deles (infecção).

70. **(FUNCAB / SESC-BA – 2012)** Considere que o técnico da área de suporte da empresa na qual você trabalha tenha detectado, em seu computador, um Cavalo de Troia. O recurso de computador que pode ter auxiliado nessa localização foi:

a) Ferramenta de Busca Google
b) Firewall
c) Sistema Antivírus
d) Gerenciador de Tarefas.
e) Fragmentador.

71. **(UECE-CEV / SEPLAG-CE – 2011)** O software concebido com o objetivo de prevenir, detectar e eliminar programas maliciosos é denominado:

a) Bloco de Notas.
b) Microsoft Office.
c) Windows Explorer.
d) Antivírus.

72. **(PONTUA / TRE-SC – 2011)** Os sistemas antivírus são programas que têm o objetivo de detectar e, então, anular ou eliminar os vírus encontrados no computador. Marque V (Verdadeiro) e F (Falso) para os exemplos de programas antivírus:

( ) Norton.
( ) WinZip.
( ) McAfee.
( ) Kaspersky.
( ) Word.

A sequência CORRETA, de cima para baixo, é:

a) F – F – V – V – V.
b) V – F – V – V – F.
c) F – V – F – F – V.
d) V – V – V – V – F.

73. **(FUNCAB / Prefeitura de Porto Velho/RO – 2009)** Às vezes, os sistemas Antivírus detectam vírus desconhecidos que não podem ser eliminados com o conjunto de ferramentas disponíveis. Qual a função existente nos sistemas antivírus que permite isolar arquivos potencialmente infectados no seu computador?

a) Scanear;
b) Colocar em quarentena;
c) Reparar;
d) Congela;
e) Purgar.

GABARITO

1. LETRA A
2. CORRETO
3. ERRADO
4. CORRETO
5. CORRETO
6. ERRADO
7. LETRA A
8. LETRA B
9. ERRADO
10. CORRETO
11. ERRADO
12. ERRADO
13. ERRADO
14. ERRADO
15. CORRETO
16. ERRADO
17. ERRADO
18. CORRETO
19. CORRETO
20. ERRADO
21. ERRADO
22. LETRA D
23. LETRA B
24. LETRA E
25. LETRA C
26. LETRA A
27. LETRA E
28. LETRA D
29. LETRA E
30. LETRA D
31. LETRA D
32. LETRA E
33. LETRA A
34. LETRA C
35. ERRADO
36. LETRA D
37. LETRA A
38. LETRA E
39. LETRA B
40. LETRA A
41. LETRA B
42. LETRA A
43. LETRA B
44. LETRA D
45. LETRA C
46. LETRA C
47. ERRADO
48. LETRA C
49. LETRA B
50. LETRA E
51. LETRA C
52. LETRA A
53. LETRA E
54. LETRA D
55. LETRA A
56. LETRA A
57. CORRETO
58. CORRETO
59. LETRA D
60. LETRA A
61. LETRA E
62. LETRA C
63. LETRA A
64. LETRA B
65. CORRETO
66. LETRA E
67. LETRA C
68. LETRA D
69. LETRA A
70. LETRA C
71. LETRA D
72. LETRA B
73. LETRA B

FIREWALL

Conceitos Básicos

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Para fazer uma aula, nós – professores – analisamos dezenas e dezenas de questões para focar apenas e tão somente naquilo que efetivamente cai em prova. Galera, segue a dica para vocês: **duas em cada três questões sobre esse assunto cobram apenas que você saiba a definição de Firewall**. Logo, nós vamos ver a seguir diversas definições diferentes para que vocês tenham uma noção geral suficiente para responder questões de prova. Vamos lá...

O que é um Firewall? Ele é um componente de segurança de uma rede privada! *Ok, mas ele é um software ou um hardware?* **Ele pode ser um software, pode ser um hardware ou pode ser um sistema composto por software e hardware**. Atualmente, os principais sistemas operacionais já trazem um firewall embutido em forma de *software* para proteger computadores domésticos contra acessos não autorizados vindos da Internet.

Se você utiliza o Windows, existe o Windows Firewall; se você utiliza o Linux, existe o IPTables/Netfilter; se você utiliza o MacOS, existe o Firewall Mac! **Dessa forma, quem possui um computador pessoal já possui um firewall embutido no próprio sistema operacional na forma de um software.** No entanto, empresas necessitam de uma segurança maior do que computadores pessoais, logo elas investem em firewalls mais robustos na forma de um hardware!

Na imagem abaixo, nós podemos ver que eles evidentemente são mais caros, podendo chegar a dezenas de milhares de reais. Vejam só:

Professor, eu quero me proteger, eu preciso comprar um desses para minha casa? Não, fera... fica tranquilo! O próprio roteador da sua casa já possui um firewall instalado, logo você não precisa disso para se proteger – quem precisa são organizações maiores que possuem dados mais críticos. **Dito tudo isso, eu gostaria que ficasse na memória de vocês que um firewall pode ser um hardware, um software ou a combinação de ambos**. *Fechou?*

(PCDF – 2015) Com relação aos dispositivos utilizados em políticas de segurança das organizações relacionadas à área de tecnologia da informação, denominados firewalls e muito úteis para minimizar crimes virtuais, assinale a alternativa correta.

a) São dispositivos, em forma de software e/ou de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou a recepção de acessos nocivos ou não autorizados de uma rede para outra.

b) São dispositivos, em forma de software e/ou de hardware existentes e habilitados no próprio sistema operacional dos computadores, que têm a função de evitar o tráfego de vírus entre computadores de uma mesma rede local, impedindo que tais vírus sejam transmitidos e/ou recebidos de um computador para outro.

c) São dispositivos em forma de software, não existindo em forma de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

d) São dispositivos em forma de software, não existindo em forma de hardware, que possuem a função de impedir o tráfego de vírus entre redes distintas, impedindo que tais vírus sejam transmitidos e/ou recebidos de uma rede para outra.

e) São dispositivos em forma de hardware, não existindo em forma de software, que possuem a função de impedir o tráfego de vírus entre redes distintas, impedindo que tais vírus sejam transmitidos e/ou recebidos de uma rede para outra.

Comentários: (a) Correto, podem ser hardware ou software com a função de regular o tráfego de dados entre redes e impedindo a transmissão/recepção de acessos nocivos ou não autorizados de uma rede para outra; (b) Errado, não é de uma mesma rede local e não impede necessariamente a transmissão/recepção de vírus; (c) Errado, existe em forma de software ou hardware; (d) Errado, existe em forma de software ou hardware e não impede necessariamente a transmissão/recepção de vírus; (e) Errado, existe em forma de software ou hardware e não impede necessariamente a transmissão/recepção de vírus (Letra A).

Bacana, mas o que diabos faz um firewall? Bem, traduzindo esse nome para a nossa língua, ele se chamaria Parede de Fogo. *Por que?* Ué, imagine uma barreira de fogo protegendo algo! *Quem é doido de atravessar o fogo?* **Logo, esse nome nos indica que ele se trata de uma barreira de proteção contra invasões.** No entanto, eu gostaria de explicá-lo com uma metáfora um pouco diferente! Vem comigo...

Imaginem uma casa de shows! Toda casa de shows precisa ter um muro para separar o interior da casa da parte exterior – caso contrário, qualquer um poderia entrar sem pagar e a casa iria à falência. **Agora imaginem que esse muro possua portas para a entrada e saída das pessoas, e que em cada porta existe um segurança enorme responsável por verificar a identidade das pessoas para bloquear aquelas menores de idade e permitir aquelas maiores de idade.**

O Firewall funciona de maneira similar: **ele controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.** *E o que seria essa política de segurança?* Trata-se de um conjunto de diretrizes da organização proibindo ou permitindo acesso aos seus ativos de informação por meio de regras.

Em outras palavras, o Firewall é capaz de bloquear todo e qualquer acesso que possa prejudicar a rede ou o computador, tais como: acesso não autorizado, tentativas de vazamentos de informações, exploração de vulnerabilidades, violação de segurança, invasões maliciosas, ataques de hackers, etc. **Ele verifica tentativas de acesso no fluxo de dados de uma rede e as bloqueia ou as permite a depender das configurações, regras ou diretrizes do firewall**.

É importante ressaltar que o Firewall faz tudo isso sem impedir o fluxo normal de dados. Logo, tudo que não violar as regras do Firewall continua a ser transmitido normalmente sem nenhum impedimento. **Assim, ele é capaz de isolar a rede interna de uma organização em geral da Internet, permitindo o tráfego de pacotes de informações que não violem as regras de acesso à rede e que outros sejam bloqueados.**

Professor, ele é capaz de proteger contra ataques internos? Para responder essa pergunta, é necessário falar um pouco sobre a posição de um firewall. *Como assim, Diego?* **Galera, um firewall tipicamente fica posicionado entre uma rede interna e a internet – nesse caso, ele é chamado de Firewall de Borda!** No entanto, em algumas situações, nós podemos ter outro firewall dentro da própria rede interna. *Por que, Diego?*

Porque, em algumas situações, um usuário pode alguns dados da rede interna a partir da Internet, mas não todos! *Como é, Diego?* Imagine um usuário acessando a intranet de uma organização a partir da internet para consultar o telefone de um setor dessa empresa. Ele estará acessando alguns dados da rede interna a partir da Internet. **No entanto, ele não poderá acessar – por exemplo – a folha de pagamentos dos funcionários.**

E como eu protejo o banco de dados que contém a folha de pagamentos dos funcionários se o usuário já conseguiu passar pelo firewall de borda e acessar a rede interna? **É possível fazê-lo inserindo um novo firewall para acessar o banco de dados chamado Firewall Interno.** Um funcionário do Banco Central pode passar pela catraca e entrar no banco, mas ele não pode passar da porta de aço para os cofres do banco sem autorização – nesse caso, existem duas barreiras!

Tudo isso que falamos é apenas para dizer que um firewall é utilizado tipicamente para impedir acessos não autorizados a uma rede interna vindos da Internet, mas ele pode – sim – ser utilizado para impedir ataques internos da rede. **Agora uma notícia triste: as bancas não têm um entendimento consolidado a respeito desse tema.** Você encontrará questões considerando apenas o Firewall de Borda. Infelizmente concurso tem dessas coisas...

(Polícia Federal – 2014) Embora os firewalls sejam equipamentos ou softwares utilizados no controle das conexões de uma rede, eles não protegem computadores contra ataques internos.

_____

Comentários: a questão não especifica o que ela quis dizer com ataques internos – *seriam ataques internos à rede ou seriam ataques internos ao computador?* Firewalls podem – sim – proteger contra ataques internos à rede dependendo de onde eles estão posicionados. No entanto, a banca infelizmente não entendeu dessa forma (Correto).

(FUB – 2016) A utilização de firewalls em uma rede visa impedir acesso indevido dentro da própria rede e também acessos oriundos da Internet.

_____

Comentários: eles realmente podem impedir acesso indevido tanto da própria rede quanto de acessos oriundos da Internet (Correto).

Um firewall pode **ajudar** a impedir que hackers ou softwares maliciosos obtenham acesso ao seu computador através da internet. *Então firewall é a mesma coisa que um antivírus?* Não, não, não... firewall analisa pacotes de dados de acordo com uma política de acesso e age preventivamente para bloquear/conceder acesso; já antivírus utilizam técnicas de assinatura, heurística, entre outros para identificar e destruir de forma reativa malwares que já estão dentro de um sistema.

Nós acabamos de dizer que o firewall pode impedir ataques advindos de dentro da própria rede dependendo de seu posicionamento. **Adicionalmente, esses ataques podem ser combatidos por meio da utilização de antivírus e outros antimalwares**. Logo, para melhor proteger o seu computador e a sua rede, recomenda-se utilizar um firewall e um antivirus/antimalware. Legal, agora vamos falar um pouco mais detalhadamente de como o firewall funciona...

Um firewall pode funcionar de duas maneiras: **modo restritivo** – impedindo todas as transmissões de dados que não sejam expressamente permitidas; **ou modo permissivo** – permitindo todas as transmissões de dados que não sejam expressamente proibidas. Para explicar isso, nós vamos partir de um exemplo da matéria de Direito Administrativo. De acordo com Hely Lopes Meirelles, não existe liberdade nem vontade pessoal na Administração Pública.

Para o autor, enquanto na administração particular é lícito fazer tudo que a lei não proíba, na Administração Pública só é permitido fazer o que a lei autoriza. Logo, um cidadão comum pode fazer absolutamente tudo que ele quiser, desde que isso não seja proibido por lei; já um servidor público não pode fazer absolutamente nada que não seja permitido por lei. Advinhem só: regras de firewalls funcionam da mesma maneira.

Em geral, o firewall é como um servidor público, isto é, ele trabalha em modo restritivo – impedindo todas as transmissões de dados que não sejam expressamente permitidas. *Legal, mas vamos um pouco mais a fundo!* Sempre que um firewall utilizar uma lista branca, significa que ele está configurado para trabalhar no modo restritivo; sempre que um firewall utilizar uma lista negra[1], significa que ele está configurado para trabalhar no modo permissivo. *Como é, professor?*

Galera, eu acabei de me casar! Sim, agora jogo no time dos casados (Êêê ... 😟). Quem já se casou sabe que um momento tenso é a hora de fazer a lista de convidados. Eu posso listar todo mundo que eu não quero que vá no casamento, colocá-los em uma lista negra e entregar na portaria. No dia do casamento, todo mundo que parar na portaria da casa de festas vai se identificar para o porteiro. **Todo mundo que não estiver na lista negra poderá entrar... inclusive penetras!!!**

Ora, então no dia do meu casamento, eu preferi fazer uma lista branca como em um firewall restritivo. *Por que?* **Porque se chega na portaria alguém que eu não gosto, penetras ou desconhecidos, o porteiro não deixará entrar**! *Aliás, uma breve história?* No dia do casamento, eu cheguei de carro na casa de festas e falei que era o noivo. O porteiro achou que era brincadeira e requisitou minha identidade. Juro para vocês...

(TRF3 – 2014) Existem duas abordagens fundamentais para criar políticas de firewall para minimizar definitivamente a vulnerabilidade em relação ao mundo externo mantendo confiável a funcionalidade desejada das máquinas na rede interna. Com relação a estas abordagens, considere as asserções a seguir.

A implementação de uma abordagem de lista branca é mais segura que a implementação de uma abordagem de lista negra para definir um conjunto de regras para o firewall

PORQUE

na abordagem de lista branca todos os pacotes podem passar, exceto aqueles que se enquadram nas regras definidas especificamente na lista.

Acerca dessas asserções, é correto afirmar:

a) A primeira asserção é uma proposição verdadeira e a segunda é uma proposição falsa.
b) As duas asserções são proposições verdadeiras e a segunda é a justificativa correta da primeira.
c) A primeira asserção é uma proposição falsa e a segunda uma proposição verdadeira.

[1] Atenção: recentemente fui alertado por um aluno que a nomenclatura "Lista Negra" tem cunho racista. Eu gostaria deixar claro que essa nomenclatura não foi inventada por mim – ela é utilizada por toda a bibliografia consagrada e por diversas bancas de concursos.

d) As duas asserções são proposições verdadeiras, mas a segunda não é a justificativa correta da primeira.
e) Tanto a primeira quanto a segunda asserções são proposições falsas.

Comentários: lista branca realmente é mais seguro que lista negra, mas a questão inverteu na segunda asserção (Letra A).

É importante destacar que o conjunto de regras de de uma organização é chamado de Lista de Controle de Acesso (*Access Control List*). Vejamos as principais técnicas utilizadas por firewalls:

TÉCNICA	DESCRIÇÃO
CONTROLE DE SERVIÇOS	Determina os tipos de serviços de internet que podem ser acessados, de entrada ou saída. O firewall pode filtrar o tráfego com base no endereço IP e número de porta TCP; pode oferecer software de proxy que recebe e interpreta cada solicitação de serviço antes de passá-la adiante, ou pode hospedar o próprio software do servidor, como um serviço web ou de correio.
CONTROLE DE DIREÇÃO	Determina a direção em que determinadas solicitações de serviço podem ser iniciadas e permitidas para fluir através do firewall.
CONTROLE DE USUÁRIO	Controla o acesso a um serviço de acordo com qual usuário está tentando acessá-lo. Essa característica normalmente é aplicada aos usuários dentro do perímetro do firewall (usuários locais). Ela também pode ser aplicada ao tráfego que chega de usuários externos; esse último exige alguma forma de tecnologia de autenticação segura.
CONTROLE DE COMPORTAMENTO	Controla como determinados serviços são utilizados. Por exemplo: o firewall pode filtrar e-mail para eliminar spam ou pode permitir o acesso externo a apenas uma parte da informação em um servidor web local.

(Polícia Federal – 2018) Um firewall implementa uma política de controle de comportamento para determinar que tipos de serviços de Internet podem ser acessados na rede.

Comentários: um firewall realmente implementa uma política de controle de comportamento, mas a questão descreveu – na verdade – uma política de controle de serviço (Errado).

Tipos de Firewall

O firewall é considerado uma tecnologia antiga na indústria de segurança, mas ainda não pode ser definido como estável, pois ele continua em um constante processo de evolução. Isso acontece, principalmente, devido ao aumento da complexidade das redes das organizações, que adicionam cada vez mais características e funcionalidades que precisam ser protegidas. **Os primeiros firewalls foram implementados em roteadores por serem os pontos de ligação natural entre duas redes.**

Com o passar do tempo, as coisas mudaram rapidamente, de modo que a própria definição de que o firewall deve separar duas redes foi modificada. **O mundo tornou-se mais integrado, e os serviços básicos, hoje, são o acesso à web, acesso a bancos de dados via internet, acesso a serviços internos da organização pela internet, serviços de áudio, video, videoconferência, voz sobre IP (Voice Over IP - VoIP), entre tantos outros.**

Com isso, as organizações têm cada vez mais usuários utilizando uma maior variedade de serviços. Os usuários muitas vezes acessam serviços fundamentais, como se estivessem fisicamente dentro da organização, como acontece nos ambientes cooperativos. **Dessa maneira, os novos requisitos de segurança fizeram com que os firewalls se tornassem mais complexos, resultando nos avanços verificados nas tecnologias.**

Além disso, diferentes nomes surgiram para tecnologias de firewalls supostamente novas, tais como firewall pessoal ou individual, mas que, como será visto a seguir, são, na realidade, apenas firewalls com novas funcionalidades ou fins específicos. Além dos avanços da tecnologia e das funcionalidades inseridas nos firewalls, outros serviços, recursos ou funções auxiliares passaram a ser incorporados. **Vejamos algumas dessas funções que podem ser realizadas por um firewall...**

FUNÇÕES AUXILIARES
Implementar recursos de NAT (Network Address Translation);
Implementar DMZ (Delimitarized Zone – Zona Desmilitarizada);
Implementar funções de balanceamento de carga;
Implementar funções de antispoofing;
Implementar funções de autenticação de usuário;
Implementar funções de criptografia de comunicações (VPN – Virtual Private Network);
Implementar funções de alta disponibilidade;
Implementar filtros de URL, Spam e E-mails;
Implementar bloqueios de alguns tipos de Ataque de DoS (Denial of Service - Negação de Serviço);
Implementar bloqueios de tráfego na camada de enlace por meio do Endereço MAC;

Podemos considerar, portanto, que atualmente existe uma tendência de adicionar cada vez mais funcionalidades aos firewalls, que podem não estar relacionadas necessariamente à segurança. No entanto, a organização que adotar essa abordagem deve estar ciente de que, quanto mais funções um firewall possuir, maiores as chances de algo dar errado e mais complexa a administração. **Logo, apesar de poder ter essas funções auxiliares, elas não são o foco principal do recurso de firewall.**

(CRF/ES – 2019) Criptografar comunicações e autenticar usuário são algumas das funções auxiliares dos firewalls.

_____

Comentários: essas realmente são algumas das funções auxiliares de firewalls (Correto).

Firewall Pessoal

INCIDÊNCIA EM PROVA: MÉDIA

Apesar da grande quantidade de funcionalidades, *antimalwares* não são capazes de impedir que um atacante tente explorar – pela rede – alguma vulnerabilidade existente em seu computador e nem de evitar o acesso não autorizado, caso haja algum *backdoor* nele instalado. Logo, além da instalação do *antimalware*, **é necessário utilizar um firewall pessoal**, que é um tipo de *firewall* utilizado para proteger um computador contra acessos não autorizados provenientes da internet.

Quando bem configurado, o firewall pessoal pode ser capaz de:

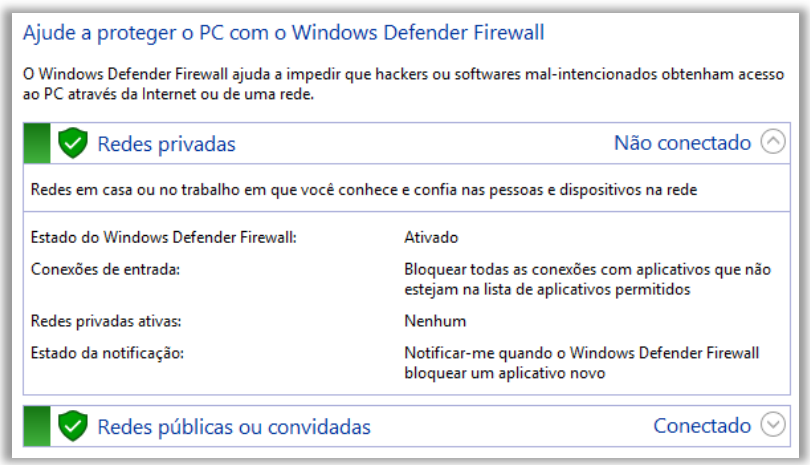
- registrar as tentativas de acesso aos serviços habilitados no seu computador e bloquear o envio para terceiros de informações coletadas por invasores e códigos maliciosos;
- bloquear as tentativas de invasão e de exploração de vulnerabilidades do seu computador e possibilitar a identificação das origens destas tentativas;
- analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado;
- evitar que um código malicioso já instalado seja capaz de se propagar, impedindo que vulnerabilidades em outros computadores sejam exploradas.

Alguns sistemas operacionais possuem *firewall* pessoal integrado (Windows Defender Firewall[2], por exemplo). Caso o sistema instalado em seu computador não possua um ou você não queira utilizá-lo, há diversas opções disponíveis (pagas ou gratuitas). Você também pode optar por um antimalware com funcionalidades de firewall pessoal integradas. No entanto, é importante ter alguns cuidados, tais como:

- antes de obter um firewall pessoal, verifique a procedência e certifique-se de que o fabricante é confiável e de que o firewall instalado esteja ativo;
- configure seu firewall para registrar a maior quantidade de informações possíveis (desta forma, é possível detectar tentativas de invasão ou rastrear as conexões de um invasor).

[2] No Windows 7, o Windows Defender era apenas um *antispyware*; no Windows 8 e 8.1, o Windows Defender era mais completo – como um *antimalware*; no Windows 10, essa ferramenta foi unificada ao Windows Defender Firewall, que exerce a função de *antimalware* e *firewall*.

Não confundam antivírus com *firewall*: o primeiro é responsável por proteger seu computador do ataque de vírus, detectando, identificando e eliminando o *malware* envolvido; o segundo é responsável por controlar ou bloquear tentativas de acesso ao seu computador sem a devida autorização – principalmente por meio de *backdoors*. **Por essa razão, eventualmente é necessário liberar os programas que você utiliza e também algumas portas de comunicação**.



Sabemos que worms possuem a capacidade de se propagar por meio de conexões de rede usando portas desativadas ou abandonadas. **Dessa forma, o firewall é capaz de impedir a sua propagação, funcionando como uma ferramenta preventiva**. É importante salientar que o firewall não é um antimalware, portanto – apesar de poder bloquear a propagação – ele não é capaz de eliminar o worm. *Bacana?*

(TJ/PR – 2014) É uma funcionalidade de um firewall pessoal:

a) Separar os e-mails desejados dos indesejados (spams).

b) Analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado.

c) Verificar vulnerabilidades nos programas instalados no computador e determinar quais devem ser atualizados.

d) Alertar o usuário quando uma página suspeita de ser falsa é acessada.

_____

Comentários: é analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado (Letra B).

Filtro de Pacotes

INCIDÊNCIA EM PROVA: ALTA

Queridos alunos, vocês se lembram que nós falamos anteriormente que um firewall é basicamente um muro com várias portas? **Pois é, cada porta oferece acesso a um serviço!** Sempre que um computador se conecta à Internet, ele possui 65536 portas de comunicação. *Como assim, Diego?* Lembrem-se da nossa aula de redes: se eu quiser utilizar o serviço de envio de e-mails, eu utilizo o Protocolo SMTP na Porta 587.

E se eu quiser utilizar aquele serviço que transforma um nome em um IP e vice-versa? Eu utilizo o Protocolo DNS na Porta 53. *E se eu quiser acessar um página web?* Eu posso fazê-lo utilizando o Protocolo HTTP na Porta 80 ou o Protocolo HTTPS na Porta 443. Galera, existem milhares de serviços e cada um é oferecido em uma porta. *O que o firewall de pacotes tem a ver com isso?* **Bem, ele basicamente é responsável por permitir ou bloquear o tráfego nessas portas.**

Então, imaginem que os servidores de um órgão estão muito com a produtividade muito baixa e que o gestor identifique que o motivo é porque eles estão frequentemente acessando o Whatsapp! *O que ele pode fazer?* **Bem, ele pode bloquear algumas portas.** Dessa forma, se o firewall de pacotes for configurado para bloquear as portas 5222 e 5223, ninguém mais conseguirá enviar/receber mensagens. *Sério, professor?* Sim, senhor...

Como toda informação que entra ou sai de uma rede vem dentro de um Pacote IP, o Filtro de Pacotes funciona como um tipo de firewall que examina os pacotes em relação ao protocolo e porta, e aplica regras baseado em uma política de segurança pré-estabelecida. Ele é considerado um firewall *stateless* (estático ou sem estado de sessão), porque ele analisa os pacotes independente de serem provenientes de uma nova sessão ou de uma conexão existente.

Em suma: **a tecnologia de filtro de pacotes funciona na camada de rede e de transporte da Arquitetura TCP/IP**, de modo que realiza as decisões de filtragem com base nas informações do cabeçalho dos pacotes, tais como endereço de origem, endereço de destino, porta de origem, porta de destino, listas de controle de acesso e direção das conexões (da rede interna para rede externa ou da rede externa para a rede interna).

O fato de trabalhar na camada de rede e de transporte faz com que ele seja simples, fácil, barato e flexível de ser implementado. Dessa forma, muitos roteadores tem também essa capacidade. Em contrapartida, o filtro de pacotes garanteum menor grau de segurança, uma vez que os pacotes podem facilmente ser falsificados ou criados especificamente para que passem pelas regras de filtragem pré-definidas.

Infelizmente, esse tipo de firewall possui inúmeros problemas, tais como o difícil gerenciamento em ambientes complexos, vulnerabilidade em relação a diversos tipos de ataques, não oferece autenticação de usuário, incompatibilidade com diversos serviços, limitação com relação a logs, problemas com fragmentação de pacotes, entre outros. **Por essas razões, esse tipo de firewall praticamente não é mais utilizado atualmente.**

(PC/ES – 2015) Se, ao acessar um endereço da Internet, o sítio correspondente mostrar-se inacessível, esse problema poderá estar relacionado com o filtro de pacotes utilizado pelo administrador da rede para aumentar a segurança do ambiente.

_____

Comentários: ele realmente analisa os pacotes de redes e utiliza regras que permitem ou bloqueiam pacotes em redes ou máquinas.

(ABIN – 2018) Filtros de pacotes tradicionais são considerados firewall porque podem executar uma política de filtragem com base na combinação de endereços e números de porta, examinando cada datagrama e determinando, a partir de regras específicas, se ele deve passar ou ficar.

_____

Comentários: a questão está impecável! Eles são um tipo de firewall e podem executar filtragens com base nos endereços e portas ao examinar cada datagrama (outro nome para pacote) a partir de regras específicas (Correto).

Filtro de Estado de Sessão

INCIDÊNCIA EM PROVA: MÉDIA

Em contraste com o firewall anterior, esse é um firewall *stateful* (com estado de sessão). *Professor, esse negócio de sessão não entrou na minha cabeça ainda!* Calma, vai entrar agora! *O que é uma sessão?* **É simplesmente uma conexão!** Quando eu ligo para a minha esposa e ela atende, trata-se de uma conexão – a partir daí, nós podemos conversar; quando dois lutadores de boxe batem as luvas, trata-se de uma conexão – a partir daí, eles podem lutar.

E por que o filtro de pacotes não tem estado? **Porque ele não cria uma conexão, logo ele não guarda registros de pacotes anteriores que tenham sido recebidos**. Assim esse firewall inspecionará cada pacote isoladamente para verificar se sua entrada será permitida ou se será bloqueada. É como se uma pessoa no meio da rua absolutamente do nada chegasse em mim e dissesse: "*Meu irmão disse que não vai!*".

Eu vou ficar completamente confuso! *Quem é você? Quem é seu irmão? Ele não vai para onde?* **Notem que essa pessoa aleatória não se identificou para mim, logo ela não abriu uma conexão**. Se ela chegasse e dissesse: "*Fala, Diego! Lembra de mim do futebol? Sou irmão do Danilo!*". Eu falaria: "*Opa, tudo bem com você?*". Aí ela poderia dizer: "*Na próxima segunda-feira eu vou para o jogo, mas o meu irmão disse que não vai!*".

Vocês percebem a diferença agora? Antes de começar a falar outras coisas, ele abriu uma conexão comigo! Agora voltando... o filtro de pacotes terá que analisar todos os pacotes isoladamente para verificar se deixa passar ou não porque ele não possui estado de sessão. **Já o filtro de estado de sessão é capaz de lembrar de pacotes anteriores porque ele é capaz de manter uma sessão – também chamada de conexão – aberta.**

Por exemplo: o protocolo FTP é utilizado para a trasferência de arquivos. **Em redes de computadores, arquivos não são transmitidos integralmente – eles são divididos em pacotes e enviados um a um separadamente da origem até o destino**. Funciona assim: ele se conecta primeiro a uma porta de controle (Porta 21) usada apenas para configurar uma sessão e, em seguida, ele inicia uma segunda sessão em outra porta para enviar os dados em si (Porta 20).

Um firewall com estado de sessão sabe que existe uma sessão aberta! *Você se lembram que o arquivo é dividido em pacotes?* Pois é, o filtro de estado de sessão verificará apenas se cada pacote é referente àquela sessão aberta – se for, está permtido; se não, está bloqueado. Já o filtro de pacotes não sabe que existe uma sessão aberta, logo para cada um dos pacotes (e geralmente são milhões), ele verificará as regras (lista, protocolo e porta).

O firewall de estado de sessão é mais sofisticado, possuindo tanto uma tabela de regras quanto uma tabela de estado. Logo, quando esse firewall recebe um pacote de dados, ele verifica as regras, isto é, a lista negra/branca, protocolo e porta; e também o estado de sessão, isto é, se já existe uma conexão aberta. Caso o protocolo seja permitido, a porta esteja aberta, o pacote esteja na lista branca e já exista uma conexão ativa, ele permite a entrada do pacote.

É importante destacar que ele também trabalha nas camadas de rede e de transporte da Arquitetura TCP/IP. Ele possui todos os recursos que possuía um Filtro de Pacotes, porém tem a capacidade adicional de analisar uma tabela de estados, que guarda os estados de todas as conexões. Ele faz uma análise inicial para permitir a conexão e depois analisa apenas se os pacotes recebidos são de uma sessão ativa ou não.

(Receita Federal – 2012) Uma das tecnologias de firewall é o filtro de pacotes baseado em estados (stateful packet filter). Nesta tecnologia, as decisões de filtragem têm como referência:

a) informações do conteúdo dos pacotes de dados e uma tabela de estados das conexões.
b) apenas uma tabela de estados das conexões.
c) apenas as informações dos cabeçalhos dos pacotes de dados.
d) informações dos cabeçalhos dos pacotes de dados e uma tabela de estados das conexões.
e) apenas informações das conexões.

Comentários: (a) Errado, as decisões de filtragem não consideram o conteúdo de pacotes; (b) Errado, a tabela de estado das conexões apenas não é suficiente – é necessário também informações de cabeçalho (protocolo, porta, etc); (c) Errado, as informações de cabeçalho não são suficientes – é necessário também a tabela de estado das conexões; (d) Correto, são necessárias informações dos cabeçalhos dos pacotes de dados e uma tabela de estados das conexões; (e) Errado, as informações de conexão não são suficientes (Letra D).

Proxy

INCIDÊNCIA EM PROVA: BAIXA

Professor, o que é um Proxy? **Proxy[3] é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.** *Entenderam algo? Bulhufas, né?* Pois é... então, vamos utilizar nossas queridas metáforas! Você deve concordar comigo que nosso país possui uma quantidade absurda de impostos. Então, algumas pessoas preferem fazer compras em lojas fora do país e pagar o frete para cá.

No entanto, muitas lojas estrangeiras não realizam a entrega em nosso país! *E aí, o que fazer?* **É possível utilizar um serviço de encaminhamento de encomendas como Shipito, MyParcel, ViaBox, entre outras**. *Como funciona?* Bem, vamos ver o que diz o site do Shipito: *"Com a Shipito você pode comprar nos sites onlines como o eBay, Amazon e Walmart, enviar suas compras para o nosso armazém e, em seguida, enviaremos os pacotes para você"*.

Em outras palavras, você compra um produto em uma loja em outro país, manda entregar no armazém do Shipito, e o Shipito envia o produto para a sua casa no Brasil. *Sacaram a ideia?* **Então, essa empresa funciona como um Proxy, isto é, ela age como um intermediário para requisições de clientes solicitando recursos de outras empresas**. O Proxy é basicamente um Procudador! Agora vamos voltar para o mundo dos computadores...

Um servidor é simplesmente um computador especializado em algum serviço! Por exemplo: um servidor web é especializado em gerenciar requisições de páginas web; um servidor de impressão é especializado em gerenciar requisições de uma impressora; um servidor de arquivos é especializado

[3] Também conhecido como Gateway de Aplicação ou – quando funciona como um firewall, pode ser chamado de Gateway Firewall ou Firewall de Aplicação (porque atua nos protocolos da Camada de Aplicação, como FTP, SMTP, HTTP, etc).

em gerenciar requisições de arquivos; e assim por diante. Quando você acessa o site do Estratégia Concursos, você está acessando o Servidor Web do Estratégia Concursos.

E, nesse contexto, existem diversos outros, tais como: servidor de aplicação, de banco de dados, de mídia, de e-Mail, etc além do... servidor proxy. **Logo, assim como os outros, ele tambem é um servidor. Nesse caso, ele é o servidor responsável e especializado por gerenciar requisições – recebê-las de usuários e repassá-las ao servidor.** *Interessante, mas eu não estou entendendo qual é a relação disso com o firewall?* Calma lá...

Nós vimos que o filtro de pacotes se baseava nas informações disponíveis nos cabeçalhos da camada de rede e de transporte (IP e TCP/UDP). No entanto, algumas vezes precisamos filtrar o acesso baseado nas informações ou conteúdos da própria aplicação. *Como é, Diego?* Suponha, por exemplo, que uma organização queira impedir que seus funcionários acessem sites de notícias, de redes sociais e de conteúdo pornográfico por meio de sua rede interna.

Nesse caso, essa organização pode utilizar um filtro de pacotes? Não, porque não será viável! **O filtro de pacotes realiza a filtragem por meio do cabeçalho dos protocolos da camada de rede e transporte, porém ele não é capaz de filtrar conteúdos específicos.** Por exemplo: se ele bloqueia a Porta 80 (HTTP), os usuários da rede interna não conseguirão acessar nenhuma página web e não só aquelas de sites de notícias, redes sociais e conteúdo pornográfico.

Isso ocorre porque o filtro de pacotes não é capaz de dintinguir pacotes que chegam a uma mesma porta. *Qual é a solução?* **Instalar um servidor proxy, porque ele é capaz de fazer filtragens baseado nos dados da camada de aplicação (por meio do Endereço URL)[4].** Como todos os dados da aplicação – que entram e que saem – passam por ele, ele pode analisar esses dados e decidir pela permissão ou proibição do tráfego de dados.

Em outras palavras, os computadores da rede local que quiserem acessar uma página web devem requisitar ao servidor proxy, que fará a filtragem baseado nos dados da aplicação e fará a requisição à página web ou simplesmente enviar uma mensagem de "Acesso negado" e bloquear o acesso. **Além disso, ele pode oferecer recursos adicionais, como armazenamento em cache, controle de acesso e manutenção do anonimato.** *Vamos entender cada um deles...*

Imaginem uma unidade de um órgão público que trabalha com a tramitação de processos de diversos tipos. No contexto do poder executivo federal, existe uma página responsável pela gestão e processamento eletrônico de documentos e processos administrativos (SEI – Sistema Eletrônico de Informações). Basicamente todos os órgãos do poder executivo federal acessam essa página diariamente para tramitar seus processos administrativos.

---

[4] Um Proxy Firewall é capaz de trabalhar nas camadas de Rede, Transporte, Sessão e Aplicação do Modelo OSI – claro que ele primariamente realiza filtragens da camada de Aplicação.

Caso exista um proxy separando a rede local de um determinado órgão e a internet, esse proxy poderá armazenar temporariamente cópias de objetos frequentemente acessados dessa página web (imagens, documentos, arquivos e outros tipos de multimídia). *Para quê, professor?* Para que acessos futuros a essa página ocorram de forma mais rápida, consumindo menos banda de internet e otimizando o tráfego na rede, uma vez que cópias dos objetos já estarão armazenados.

Funciona de maneira semelhante ao cache de um navegador. Se você acessar uma página nova pela primeira vez, ela demorará um pouco mais a carregar do que uma página acessada com frequência. *Por que?* Porque o seu navegador também armazena localmente em cache objetos de uma página web para que futuramente essa página seja carregada mais rapidamente. Hoje em dia, a velocidade de internet é muito rápida, mas antigamente era bem fácil de perceber isso...

(CRMV/SC – 2017) Para conectar uma rede privativa (intranet) a uma rede pública (internet), muitas vezes os administradores de rede se valem de um servidor que tem por função receber os pedidos de um número IP interno (privativo) e encaminhá-lo, através de um número IP válido (publico), à internet de forma a obter o conteúdo desejado pelo usuário. Este servidor, por vezes, armazena uma cópia do conteúdo solicitado por um usuário, para entregá-lo, mais rapidamente a um segundo usuário se este mesmo conteúdo for novamente solicitado. Estamos, neste caso, falando de um servidor:

a) Web
b) Firewall
c) SMTP
d) Proxy

_____

Comentários: o servidor proxy armazena uma cópia do conteúdo solicitado por um usuário, para entregá-lo, mais rapidamente a um segundo usuário se este mesmo conteúdo for novamente solicitado (Letra D).

Professor, se eu tenho o cache do navegador, qual é a utilidade do cache do proxy? O cache do navegador armazena dados temporários apenas de páginas web acessadas pelo seu computador; o cache do proxy armazena dados temporários de páginas web acessadas por todos os computadores da rede interna. **Outro recurso de um proxy é o controle de acesso para execução de uma política de segurança (Ex: sites de notícias, redes sociais e conteúdo pornográfico).**

O proxy pode realizar o controle de acesso a endereços da internet bloqueando páginas através de seus endereços e/ou palavras previamente definidas[5]. Importante: o proxy mantém um log de todas as tentativas de acesso a páginas web. Logo, se você insiste em tentar acessar páginas web bloqueadas por um proxy no seu trabalho, saiba que ele mantém um registro de todas as suas tentativas. Vários alunos já me mandaram mensagem preocupados com essa informação :P

[5] É possível bloquear, inclusive, o acesso e download de arquivos executáveis.

Por fim, um firewall pode ser utilizado para manter o anonimato. *Como, Diego?* Um hacker pode acessar um web proxy qualquer na internet para cometer crimes ou realizar atividades maliciosas sem ter o seu endereço exposto (IP). **Se alguém for tentar rastreá-lo, descobrirão o endereço do proxy e, não, seu endereço verdadeiro.** *Isso é sempre ruim, professor?* Não, essa é uma excelente alternativa para cidadãos de países autoritários burlarem a censura.

Vocês sabiam que a China não permite que seus cidadãos acessem o Google, Facebook, Wikipedia, Netflix, Zoom, Bing, Instagram, Twitter, Youtube, etc? **Uma alternativa para os chineses é a utilização de proxies web espalhados pelo mundo (é claro que o governo chinês também tenta barrar o acesso aos proxies).** Nós vimos muitas informações sobre proxy, mas é interessante vermos como sua definição já foi cobrada em prova:

DEFINIÇÕES DE PROXY
Servidor que visa intermediar as mensagens de nível de aplicação entre clientes internos e servidores externos, para impor uma política de segurança de uma empresa.
Servidor que funciona como intermediário entre um navegador da web e a Internet.
Servidor que permite realizar um controle de acesso a endereços da internet, bloqueando páginas através de seus endereços e/ou palavras previamente definidas.
Servidor que age como intermediário nas requisições entre componentes da rede e entidades externas ou internas a ela de modo a simplificar ou controlar a sua complexidade.
Servidor (sistema de computador ou uma aplicação) que atua como um intermediário entre os computadores de uma rede e a Internet.

Professor, um proxy é um firewall? Galera, um proxy possui diversos recursos! **Quando um proxy faz um controle de acesso à rede – limitando ou bloqueando conexões – ele está fazendo o papel de um firewall.** Já quando ele está apenas gerenciando requisições de clientes para servidores sem fazer nenhum tipo de controle de acesso para uma política de segurança específica, ele não está fazendo o papel de um firewall – ele está sendo apenas um intermediário.

(Polícia Federal – 2018) Servidores proxy que atuam em nível de aplicação conseguem bloquear acesso a arquivos executáveis em conexões HTTP, o que não pode ser realizado com filtros de pacotes.

Comentários: filtros de pacotes atuam nas camadas de rede e transporte, logo nada podem fazer para bloquear acesso a arquivos executáveis. Já os servidores proxy podem, sim, bloquear acesso a esse tipo de arquivo porque eles são capazes de filtrar conteúdos na camada de aplicação (Correto).

(Polícia Federal – 2018) Marta utiliza uma estação de trabalho que executa o sistema operacional Windows 10 e está conectada à rede local da empresa em que ela trabalha. Ela acessa usualmente os sítios da intranet da empresa e também sítios da Internet pública. Após navegar por vários sítios, Marta verificou o histórico de navegação e identificou que um dos sítios acessados com sucesso por meio do protocolo HTTP tinha o endereço 172.20.1.1.

Tendo como referência essa situação hipotética, julgue o item a seguir.

Por meio do serviço de proxy para rede local, Marta poderá acessar, a partir da sua estação de trabalho, tanto os sítios da intranet quanto os sítios da Internet pública.

Comentários: proxy é um servidor que serve de intermediário na comunicação de um computador cliente de uma rede local geralmente com um servidor da rede pública (internet), logo – por meio do serviço de proxy para rede local, Marta realmente poderá acessar, a partir da sua estação de trabalho, tanto os sítios da intranet quanto sítios da internet. *Professor, qual é o sentido de utilizar um proxy para acessar à intranet a partir da própria rede local?* Em regra, isso é muito pouco utilizado, mas pode haver algum caso em que mesmo os acessos internos devem ser controlados. Como a questão apenas menciona que Marta poderá acessar sítios da intranet ou internet, não há nenhum erro na questão (Correto).

É importante mencionar os firewalls híbridos, que basicamente misturam os elementos das três tecnologias apresentadas anteriormente. *Fechado?* Por fim, uma pergunta que muitos alunos fazem no fórum de dúvidas trata da diferença entre Proxy e VPN (Virtual Private Network). **Nós sabemos que quando você se conecta a um Servidor Proxy, ele se torna um intermediário entre o seu dispositivo e a internet.**

Todo o seu tráfego de internet é redirecionado através do Servidor Proxy, fazendo com que pareça ter vindo do endereço IP do Servidor Proxy. A conexão com um Servidor Proxy mascara o endereço IP e permite que você acesse conteúdo censurado. No entanto, eles não criptografam seu tráfego, logo, qualquer informação que você troque através da conexão pode ser interceptada por outras pessoas que também estão conectadas ao servidor, como hackers ou ladrões de identidade.

Uma VPN oferece diversos benefícios similares aos serviços fornecidos por um Servidor Proxy, no entanto a sua função principal – que a difere da VPN – é proteger e criptografar os dados entre seu dispositivo e a Internet.

Por fim, é importante mencionar o WAF (Web Application Firewall) – tipo específico de Firewall de Aplicação que opera apenas na web – filtrando, monitorando e bloqueando tráfego HTTP.

RESUMO

DEFINIÇÃO DE FIREWALL

São dispositivos, em forma de software e/ou de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou a recepção de acessos nocivos ou não autorizados de uma rede para outra. Ele controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.

TÉCNICA	DESCRIÇÃO
CONTROLE DE SERVIÇOS	Determina os tipos de serviços de internet que podem ser acessados, de entrada ou saída. O firewall pode filtrar o tráfego com base no endereço IP e número de porta TCP; pode oferecer software de proxy que recebe e interpreta cada solicitação de serviço antes de passá-la adiante, ou pode hospedar o próprio software do servidor, como um serviço web ou de correio.
CONTROLE DE DIREÇÃO	Determina a direção em que determinadas solicitações de serviço podem ser iniciadas e permitidas para fluir através do firewall.
CONTROLE DE USUÁRIO	Controla o acesso a um serviço de acordo com qual usuário está tentando acessá-lo. Essa característica normalmente é aplicada aos usuários dentro do perímetro do firewall (usuários locais). Ela também pode ser aplicada ao tráfego que chega de usuários externos; esse último exige alguma forma de tecnologia de autenticação segura.
CONTROLE DE COMPORTAMENTO	Controla como determinados serviços são utilizados. Por exemplo: o firewall pode filtrar e-mail para eliminar spam ou pode permitir o acesso externo a apenas uma parte da informação em um servidor web local.

TIPOS DE FIREWALL	DESCRIÇÃO
FIREWALL PESSOAL	Software utilizado para proteger um único computador, controlando o tráfego dos dados contra acessos não autorizados provenientes da internet.
FILTRO DE PACOTES	Firewall mais antigo capaz de executar uma política de filtragem com base na combinação de regras específicas (protocolo, porta e lista negra/branca) para examinar cada pacote – sem estado.
FILTRO DE ESTADO DE SESSÃO	Firewall mais moderno que analisa informações dos cabeçalhos dos pacotes de dados e cria uma tabela de estados de conexões para realizar a filtragem baseado nas conexões – com estado.

PROXY

- Proxy é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Ele funciona como um Firewall no sentido de que é capaz de impedir que sua rede interna seja exposta à Internet – redirecionando solicitações da/para web quando necessário e podendo realizar análise de conteúdo da aplicação.

DEFINIÇÕES DE PROXY
Servidor que visa intermediar as mensagens de nível de aplicação entre clientes internos e servidores externos, para impor uma política de segurança de uma empresa.
Servidor que funciona como intermediário entre um navegador da web e a Internet.
Servidor que permite realizar um controle de acesso a endereços da internet, bloqueando páginas através de seus endereços e/ou palavras previamente definidas.
Servidor que age como intermediário nas requisições entre componentes da rede e entidades externas ou internas a ela de modo a simplificar ou controlar a sua complexidade.
Servidor (sistema de computador ou uma aplicação) que atua como um intermediário entre os computadores de uma rede e a Internet.

MAPA MENTAL

Firewall

Conceitos básicos

- O FIREWALL É UMA BARREIRA CONTRA INVASÕES.
- PODE SER UM SOFTWARE, UM HARDWARE OU A COMBINAÇÃO DE AMBOS.
- OS PRINCIPAIS SISTEMAS OPERACIONAIS JÁ TRAZEM O FIREWALL EMBUTIDO (SOFTWARE).
- CONTROLA, ANALISA, REGISTRA, POLICIA, MONITORA, REGULA E FILTRA O TRÁFEGO OU MOVIMENTAÇÃO DA ENTRADA/SAÍDA DE DADOS, DETECTANDO AMEAÇAS E BLOQUEANDO O ACESSO QUE NÃO ESTEJA EM CONFORMIDADE COM A POLÍTICA DE SEGURANÇA DA ORGANIZAÇÃO.
- NÃO IMPEDE O FLUXO NORMAL DE DADOS.
- NÃO SUBSTITUI O ANTIVÍRUS (ELES TÊM FUNÇÕES ≠).
  - FIREWALL: CONTROLA/BLOQUEIA TENTATIVAS DE ACESSO.
  - ANTIVÍRUS: DETECTA E ELIMINA MALWARES.

- MODO PERMISSIVO: PERMITE TODAS AS TRASMISSÕES DE DADOS QUE NÃO ESTEJAM EXPRESSAMENTE PROIBIDAS.
- LISTA NEGRA.

- MODO RESTRITIVO: IMPEDE TODAS AS TRANSMISSÕES DE DADOS QUE NÃO ESTEJAM EXPRESSAMENTE PERMITIDAS.
- LISTA BRANCA.

Proxy

- É UM SERVIDOR QUE AGE COMO UM INTERMEDIÁRIO PARA REQUISIÇÕES DE CLIENTES, SOLICITANDO RECURSOS DE OUTROS SERVIDORES.
- NO PROCESSO DE MEDIAÇÃO, O PROXY MASCARA O ENDEREÇO IP DO CLIENTE, REDUZINDO AS CHANCES DE ATAQUES OU INTERCEPTAÇÃO NA COMUNICAÇÃO.
- FUNCIONA DE FORMA SEMELHANTE A UM FIREWALL QUANDO É CONFIGURADO P/ PERMITIR OU NÃO ALGUNS TIPOS DE SOLICITAÇÃO (DE ENTRADA OU DE SAÍDA DE DADOS).

Tipos de firewall

① Firewall pessoal

- SOFTWARE UTILIZADO PARA PROTEGER UM ÚNICO COMPUTADOR, CONTROLANDO O TRÁFEGO DOS DADOS CONTRA ACESSOS NÃO AUTORIZADOS PROVENIENTES DA INTERNET.
- REGISTRA AS TENTATIVAS DE ACESSO AOS SERVIÇOS HABILITADOS NO COMPUTADOR.
- BLOQUEIA O ENVIO P/ TERCEIROS DE INFORMAÇÕES COLETADAS POR INVASORES E MALWARES.
- BLOQUEIA TENTATIVAS DE INVASÃO E DE EXPLORAÇÃO DE VULNERABILIDADES.
  - E POSSIBILITA A IDENTIFICAÇÃO DAS ORIGENS DESSAS TENTATIVAS.
- ANALISA CONTINUAMENTE O CONTEÚDO DAS CONEXÕES E BARRA MALWARES.
- BARRA A COMUNICAÇÃO ENTRE UM INVASOR E UM CÓDIGO MALICIOSO JÁ INSTALADO.
- EVITA QUE MALWARES JÁ INSTALADOS SE PROPAGUEM PELA REDE (EX: WORMS).

② Filtro de Pacotes

- RESPONSÁVEL POR PERMITIR OU BLOQUEAR O TRÁFEGO NAS PORTAS DE COMUNICAÇÃO.
- EXAMINA OS PACOTES IP EM RELAÇÃO AO PROTOCOLO E PORTA, E APLICA REGRAS BASEADO EM UMA POLÍTICA DE SEGURANÇA PRÉ-ESTABELECIDA.
- É UM FIREWALL STATELESS (ESTÁTICO OU SEM ESTADO DE SESSÃO/CONEXÃO).
  - NÃO CRIA UMA CONEXÃO, POR ISSO NÃO GUARDA REGISTROS DE PACOTES QUE TENHAM SIDO RECEBIDOS.
  - ANALISA CADA PACOTE INDEPENDENTE DE SER PROVENIENTE DE UMA NOVA SESSÃO OU DE UMA CONEXÃO EXISTENTE.

③ Filtro de Estado de Sessão

- É UM FIREWALL STATEFULL (COM ESTADO DE SESSÃO/CONEXÃO).
  - É CAPAZ DE LEMBRAR DE PACOTES ANTERIORES, PORQUE CONSEGUE MANTER UMA SESSÃO (CONEXÃO) ABERTA.
- VERIFICA AS REGRAS (LISTA BRANCA/NEGRA), PROTOCOLO E PORTA APENAS UMA VEZ P/ PERMITIR A CONEXÃO, DEPOIS ANALISA APENAS O ESTADO DE SESSÃO (SE EXISTE CONEXÃO ABERTA).
  - VERIFICA SE CADA PACOTE É REFERENTE A UMA DETERMINADA SESSÃO. SE FOR, ESTÁ PERMITIDO; SE NÃO FOR, ESTÁ BLOQUEADO.

QUESTÕES COMENTADAS – CESPE

1. **(CESPE / DPE-RO – 2021)** Vários pacotes de dados que chegaram a um sistema de firewall foram bloqueados ao terem sido verificados, por não haver, no firewall, informações de estado de conexão para os endereços referidos nos pacotes e os serviços relacionados.

   Nessa situação hipotética, a atividade que permitiu verificar e invalidar os pacotes de dados no firewall é denominada:

   a) filtragem de pacotes stateless.
   b) filtragem de proxy de aplicação.
   c) inspeção de pacotes stateful.
   d) filtragem de pacotes fragmentados.
   e) inspeção profunda de protocolo.

Comentários:

O firewall que verifica o estado de uma conexão e invalidar os pacotes de dados é o *stateful*.

Gabarito: Letra C

---

2. **(CESPE / CGE - CE – 2019)** Para proteger a comunicação em uma organização que possui várias redes internas de computadores interligadas entre si e também à Internet contra ações maliciosas no tráfego dos dados, o mecanismo a ser utilizado é o:

   a) registro de logs.
   b) antispam
   c) firewall
   d) antispyware
   e) controlador de domínio.

Comentários:

O mecanismo que permite proteger a comunicação em uma organização que possui várias redes internas de computadores interligadas entre si e também à Internet contra ações maliciosas no tráfego dos dados é o firewall.

Gabarito: Letra C

---

3. **(CESPE / Polícia Federal – 2018)** Marta utiliza uma estação de trabalho que executa o sistema operacional Windows 10 e está conectada à rede local da empresa em que ela trabalha. Ela acessa usualmente os sítios da intranet da empresa e também sítios da Internet pública. Após

navegar por vários sítios, Marta verificou o histórico de navegação e identificou que um dos sítios acessados com sucesso por meio do protocolo HTTP tinha o endereço 172.20.1.1.

Tendo como referência essa situação hipotética, julgue o item a seguir.

A despeito das configurações dos ativos de segurança corporativos e do serviço de firewall instalado na estação de trabalho, Marta poderá acessar remotamente sua estação de trabalho usando a Conexão de Área de Trabalho Remota, a partir de outra estação conectada à Internet.

Comentários:

Essa questão é mais de português do que de informática. A locução prepositiva "a despeito de" tem o sentido de "independente de". *Logo, vamos reler o item dessa forma?*

Independente das configurações dos ativos de segurança corporativos e do serviço de firewall instalado na estação de trabalho, Marta poderá acessar remotamente sua estação de trabalho usando a Conexão de Área de Trabalho Remota, a partir de outra estação conectada à Internet.

Opa... independente, não! Pode haver configurações no firewall que impeçam Marta de utilizar o acesso remoto a partir de outra estação conectada à internet.

Gabarito: Errado

---

4. **(CESPE / Polícia Federal – 2018)** Um firewall é uma combinação de hardware e software que isola da Internet a rede interna de uma organização, permitindo o gerenciamento do fluxo de tráfego e dos recursos da rede e o controle, pelo administrador de rede, do acesso ao mundo externo.

Comentários:

Perfeito, perfeito, perfeito! Impecável definição de firewall! *Professor, mas um firewall não pode ser somente um software, sem hardware?* Pode, mas isso não invalida a questão! Lembrem-se que uma questão só está errada se tiver um erro e não há nenhum erro na questão porque existem firewalls que são uma combinação de hardware e software.

Gabarito: Correto

---

5. **(CESPE / Polícia Federal – 2018)** Um dos objetivos do firewall é monitorar todo o tráfego de dados entrando e saindo de uma rede local e entrar em ação ao identificar um sniffer externo.

Comentários:

Um dos objetivos do firewall realmente é monitorar todo o tráfego de dados entrando e saindo de uma rede, no entanto ele não é capaz de entrar em ação ao identificar um sniffer externo. *Por que?* Porque ele não é capaz de detectá-lo! Lembrem-se que o firewall é como uma parede que separa duas redes. Ele nada pode fazer contra o que ocorre internamente ou externamente – sua ação está limitada ao que atravessa a parede.

Gabarito: Errado

---

6. **(CESPE / Polícia Federal – 2018)** Em um firewall, devem ser controlados não apenas os pacotes que entram em uma rede privada, mas também aqueles que saem da rede para a Internet.

Comentários:

Perfeito! Ele controla tudo que entra e sai de uma rede.

Gabarito: Correto

---

7. **(CESPE / EMAP – 2018)** Os administradores de rede fazem uso do firewall statefull para filtrar pacotes baseados em endereços de IP, protocolos, portas e estado das conexões.

Comentários:

Impecável! Filtros de estado de sessão filtram dados por meio do endereço lógico, protocolo, porta e estado das conexões.

Gabarito: Correto

---

8. **(CESPE / TRE BA - 2017)** Assinale a opção que apresenta a solução que permite filtrar tentativas de acessos não autorizados oriundos de outros ambientes e redes externas, contribuindo para a melhora do estado de segurança da informação de ambientes computacionais.

a) certificado digital
b) chave de criptografia
c) rootkits
d) firewall
e) antivírus

Comentários:

O Firewall é um componente de segurança de uma rede privada (hardware, software ou uma combinação de ambos) que controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização. Ele é capaz de bloquear todo

e qualquer acesso que possa prejudicar a rede ou o computador, tais como: acesso não autorizado, tentativas de vazamentos de informações, exploração de vulnerabilidades, violação de segurança, invasões maliciosas, ataques de hackers, etc.

Gabarito: Letra D

---

9. **(CESPE / FUB – 2016)** Ferramentas de firewall são amplamente utilizadas em redes de computadores, de maneira a permitir ou negar determinado fluxo de pacotes. Com relação a firewall convencional de rede, julgue o item subsecutivo.

   Um firewall é capaz de verificar tanto o endereço IP de origem quanto o endereço IP de destino em um pacote de rede.

Comentários:

Perfeito! Para realizar a filtragem, ele verifica o cabeçalho das camadas de redes e transportes, logo analisam tanto o endereço de origem quanto o endereço de destino de um pacote na rede.

Gabarito: Correto

---

10. **(CESPE / FUB – 2016)** Firewall é um recurso utilizado para restringir alguns tipos de permissões previamente configuradas, a fim de aumentar a segurança de uma rede ou de um computador contra acessos não autorizados.

Comentários:

Firewall é um recurso utilizado para restringir todo acesso não previamente autorizado (lista branca) ou permitir todo acesso não previamente proibido (lista negra) a fim de aumentar a segurança de uma rede ou de um computador. A banca generalizou ambos os casos como "*restringir alguns tipos de permissões previamente configuradas*" – eu achei essa redação bem esquisita!

Gabarito: Correto

---

11. **(CESPE / FUB – 2016)** Firewall é capaz de verificar tanto o endereço IP de origem quanto o endereço IP de destino em um pacote de rede.

Comentários:

Perfeito! Um filtro de pacotes, por exemplo, analise os cabeçalhos das camadas de redes e transporte, logo é capaz de verificar tanto o endereço IP de origem quanto o endereço IP de destino em um pacote de rede.

Gabarito: Correto

---

12. (CESPE / TCE-PA – 2016) Por padrão, um WAF (Web Application Firewall) é capaz de utilizar as camadas de rede, de transporte e de aplicação da pilha TCP/IP.

Comentários:

Por padrão, ele atua apenas na camada de aplicação!

Gabarito: Errado

---

13. (CESPE / MEC – 2015) Uma das características mais importantes do proxy é a restrição de acesso a sítios não autorizados, executada por meio de listas de controle de acesso (access control lists).

Comentários:

Todo firewall executa a política de segurança de uma organização por meio de Listas de Controle de Acesso. Proxies podem executar essa política baseado na restrição de acesso a sítios não autorizados (filtros de pacotes e filtros de estado de sessão não são capazes de filtrar pelo endereço de uma página).

Gabarito: Correto

---

14. (CESPE – TCU – 2015) O firewall é capaz de proteger o computador tanto de ataques de crackers quanto de ataques de vírus.

Comentários:

Eu lembro que essa questão deu muuuuuuuuuuuuuita polêmica na época. O lance é o seguinte: notem que a questão afirma que "*o firewall é capaz de proteger o computador tanto de ataques de crackers quanto de ataques de vírus*". Como ele diz "capaz", esse item só estaria errado caso não houvesse nenhuma possibilidade de um firewall proteger um computador do ataque de um vírus - e isso não é correto!

O firewall é capaz de filtrar pacotes de dados de acordo com uma determinada política de segurança. Quando um vírus ataca um computador, sua atividade maliciosa pode acabar sendo bloqueada por um firewall, logo o firewall foi capaz de proteger o computador. Ele não detecta nem elimina malwares, mas é capaz – eventualmente – de proteger de seus ataques e atividades maliciosas. Questão bastante difícil e que teve centenas de recursos, mas todos foram indeferidos.

Gabarito: Correto

---

15. (CESPE/ MTE - 2013) O firewall é um sistema antivírus que inibe a infecção de novos tipos de vírus. Para ser eficiente, o firewall deve ser atualizado frequentemente.

Comentários:

Firewall é um sistema antivírus? Não, eles são complementares e possuem funções diferentes. Firewall geralmente não é capaz de inibir a infecção de novos tipos de vírus. Além disso, ele não tem a necessidade de ser atualizado frequentemente como nos antivírus!

Gabarito: Errada

---

16. (CESPE / MPU – 2013) Uma das funções dos firewalls é implementar políticas relativas à separação do tráfego interno e externo à rede a ser protegida, visto que eles filtram o tráfego de entrada e saída de rede.

Comentários:

Perfeito! Ele realmente isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros.

Gabarito: Correto

---

17. (CESPE/ PC AL - 2012) Um firewall do tipo stateful não verifica o estado de uma conexão.

Comentários:

Como assim? Pelo contrário, um firewall do tipo stateful é aquele que verifica o estado de uma conexão! O firewall do tipo stateless que não verifica!

Gabarito: Errada

---

18. (CESPE / Polícia Federal - 2012) Quando a solicitação de conexão do tipo UDP na porta 21 for recebida por estação com firewall desligado, caberá ao sistema operacional habilitar o firewall, receber a conexão, processar a requisição e desligar o firewall. Esse procedimento é realizado porque a função do UDP na porta 21 é testar a conexão do firewall com a Internet.

Comentários:

Totalmente errado! O Firewall não é ligado por conta de uma tentativa de conexão: você o configura para estar habilitado ou não! Ademais, a porta 21 é a famosa porta de controle do Protocolo FTP, que é o protocolo utilizado para transferência de arquivos. Por fim, trata-se de uma Porta TCP e, não, UDP.

Gabarito: Errada

---

19. **(CESPE / MCT - 2012)** Um firewall serve, basicamente, para filtrar os pacotes que entram e(ou) saem de um computador e para verificar se o tráfego é permitido ou não.

Comentários:

Perfeito! O firewall controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.

Gabarito: Correta

---

20. **(CESPE / FNDE - 2012)** Para proteger um computador contra os efeitos de um worm, pode-se utilizar, como recurso, um firewall pessoal.

Comentários:

CESPE é CESPE, né?! Olha a pegadinha dessa questão: firewall pessoal é incapaz de detectar ou desativar um worm, no entanto ele pode – sim – ajudar a proteger contra os efeitos de um worm! Não há nada de errado na questão porque dependendo do tipo de worm, ele pode tentar realizar coisas que podem ser bloqueadas pelo firewall pessoal.

Gabarito: Correta

---

21. **(CESPE / TJ-AC - 2012)** Em um computador com o Windows instalado, o firewall detecta e desativa os vírus e worms que estejam contaminando o computador.

Comentários:

Firewall é uma solução de hardware ou software (o mais usado pela maioria dos usuários domésticos) que monitora o tráfego de dados e libera acesso apenas aos sítios de interesse do usuário, ou seja, ele só aceita receber e enviar dados de e para sítios considerados seguros, para evitar invasões perpetradas por hackers e crackers. O Firewall nada poderá fazer para detectar ou desativar um vírus ou worm – para tal, utilizam-se antivírus!

Gabarito: Errada

---

22. **(CESPE – ANAC – 2012)** Um firewall pessoal é uma opção de ferramenta preventiva contra worms.

Comentários:

Firewall é uma solução de hardware ou software que monitora o tráfego de dados e libera acesso apenas aos sítios de interesse do usuário, ou seja, ele só aceita receber e enviar dados de e para

sítios considerados seguros. Deste modo, o firewall pode auxiliar a evitar que um worm explore uma possível vulnerabilidade de algum programa do computador.

O examinador foi preguiçoso e só modificou a ordem das palavras da questão anterior. De todo modo, ele é realmente uma opção preventiva contra worms.

Gabarito: Correto

---

23. (CESPE / IFB - 2011) Ferramentas como firewall e antivírus para estação de trabalho não ajudam a reduzir riscos de segurança da informação.

Comentários:

Como assim? É claro que ajudam a reduzir riscos de segurança da informação!

Gabarito: Errada

---

24. (CESPE / AL ES - 2011) Existem diversos dispositivos que protegem tanto o acesso a um computador quanto a toda uma rede. Caso um usuário pretenda impedir que o tráfego com origem na Internet faça conexão com seu computador pessoal, a tecnologia adequada a ser utilizada nessa situação será o:

a) multicast.
b) instant message.
c) miniDim.
d) firewall.
e) Ipv6.

Comentários:

(a) Errado, Multicast é a entrega de informação para múltiplos destinatários simultaneamente; (b) Errado, Instant Message é a tecnologia que permite enviar e receber mensagens instantaneamente; (c) Errado, MiniDim é uma família de conectores elétricos de multiplos pinos, que são usados em muitas aplicações; (d) Correto, Firewall é a tecnologia adequada para impedir que o tráfego com origem na Internet faça conexão com seu computador pessoal; (e) Errado, Ipv6 é a versão mais atual do Protocolo de Internet.

Gabarito: Letra D

---

25. (CESPE / SEDUC-AM – 2011) Um firewall pessoal é um software ou programa utilizado para proteger um computador contra acessos não autorizados provenientes da Internet.

Comentários:

O firewall pessoal realmente é utilizado para proteger um computador contra acessos não autorizados da internet.

Gabarito: Correto

QUESTÕES COMENTADAS – FCC

26. (FCC / Prefeitura de Teresina - PI – 2016) A proteção das informações e dos sistemas das organizações requer o uso de recursos de proteção como os firewalls, utilizados para:

a) ajudar a impedir que a rede privada da empresa seja acessada sem autorização a partir da Internet.

b) liberar o uso de todos os serviços de rede somente aos usuários registrados pelo administrador da rede.

c) garantir que cada pacote de dados seja entregue com segurança apenas ao destinatário informado, reduzindo assim o tráfego na rede.

d) garantir que nenhum colaborador possa comprometer a segurança das informações da organização.

e) garantir que os computadores da rede não sejam infectados por malwares ou atacados por hackers.

Comentários:

(a) Correto, essa é a função de um firewall; (b) Errado, isso seria um controle de acesso, que não é função de um firewall; (c) Errado, não há nenhuma relação com firewall; (d) Errado, não há nenhuma relação com firewall; (e) Errado, isso seria a função de um antimalware.

Gabarito: Letra A

---

27. (FCC / SEFAZ PE - 2014) Um dos mecanismos básicos de segurança da informação é um componente de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Este componente de segurança existe na forma de software, de hardware ou da combinação de ambos. Atualmente, os principais sistemas operacionais trazem este componente embutido na forma de software para proteger computadores contra acessos não autorizados vindos da Internet. O texto descreve o componente conhecido como:

a) firewall.
b) sniffer.
c) antivirus.
d) proxy.
e) scandisk.

Comentários:

Componente de uma rede de computadores? Aplicar uma política de segurança? Existe na forma de software, hardware ou uma combinação de ambos? Principais sistemas operacionais trazem este componente? Protege computadores contra acessos não autorizados? Só pode estar se referindo ao Firewall.

Gabarito: Letra A

28.(FCC / MPE-SE – 2013) Um determinado tipo de servidor permite que páginas comumente acessadas na internet sejam armazenadas localmente. Quando tais páginas são requisitadas, suas cópias locais são transferidas para o usuário de forma transparente e, por estarem já armazenadas no servidor local, são retornadas de forma muito mais ágil. Estes servidores são chamados de:

a) WAN.
b) DDoS.
c) Web Servers.
d) PPP.
e) Proxy.

Comentários:

Servidor capaz de armazenar páginas localmente? Páginas carregadas de forma mais rápida? Trata-se de um Proxy!

Gabarito: Letra E

29.(FCC / TJ-PE - 2012) Ajuda a impedir que hackers ou programas mal-intencionados acessem um computador via internet ou por uma rede. Software ou hardware que verifica as informações provenientes da Internet, ou de uma rede, e as bloqueia ou permite que elas cheguem ao seu computador, dependendo das configurações. Trata-se de:

a) criptograma.
b) keylogger.
c) screenlogger.
d) cavalo de troia
e) firewall

Comentários:

Impede acesso mal-intencionado via internet ou rede? Software ou hardware? Bloqueia ou permite informações? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

30. (FCC / TRE-PR - 2012) Uma barreira protetora que monitora e restringe as informações passadas entre o seu computador e uma rede ou a Internet, fornece uma defesa por software contra pessoas que podem tentar acessar seu computador de fora sem a sua permissão é chamada de:

a) ActiveX.
b) Roteador.
c) Chaves públicas.
d) Criptografia.
e) Firewall.

Comentários:

Barreira protetora? Monitora e restringe as informações passadas? Fornece defesa contra acessos sem permissão? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

31. (FCC / TJ-PE – 2012) Um dos tipos existentes de firewall é o filtro de camada da aplicação. Neste modo, o bloqueio é realizado ao se analisar:

a) a aplicação das regras para determinada camada, como por exemplo camadas IP ou ethernet.

b) endereços de origem e destinos ou números de portas dos pacotes enviados e/ou recebidos.

c) listas brancas ou negras que possuem os nomes das aplicações bloqueadas ou liberadas para uma determinada topologia.

d) detalhes específicos de cada aplicação, como por exemplo, cabeçalhos de mensagens de e-mail.

e) a quantidade de acessos de uma aplicação em um endereço ou porta específica da internet em um determinado período de tempo, evitando dessa forma ataques como o denial-of-service (DoS).

Comentários:

Observe que o enunciado trata "neste modo", isto é, especificamente no modo de filtro de camada de aplicação. Logo, pode-se afirmar que o bloqueio não se dá pela camada IP, endereço, número de porta, topologia ou quantidade de acessos. O bloqueio se dá por conta de detalhes específicos de cada aplicação como, por exemplo, cabeçalhos de mensagens de e-mail.

Gabarito: Letra D

---

32. (FCC / TRF 1ª REGIÃO - 2011) Dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede de computadores de uma empresa. Sua função consiste em regular o tráfego de dados entre essa rede e a internet e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados. Trata-se de:

a) antivírus.
b) firewall.
c) mailing.
d) spyware.
e) adware.

Comentários:

(a) Errado, antivírus são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional; (b) Correto, firewall controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização; (c) Errado, mailing é a ação de expedir mensagens eletrônicas; (d) Errado, spyware é uma ferramenta que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros; (e) Errado, adware é um código que apresenta anúncios, cria ícones ou modifica itens do sistema operacional com o intuito de exibir alguma propaganda.

Gabarito: Letra B

---

33. (FCC / INFRAERO - 2011) O controle de transmissão de dados em uma rede de computadores, filtrando e permitindo ou não a passagem dos dados, é a principal função realizada pelo dispositivo denominado:

a) firewall.
b) firmware.
c) modem.
d) roteador.
e) antivírus.

Comentários:

(a) Correto, firewall realiza o controle de transmissão de dados em uma rede de computadores, filtrando e permitindo ou não a passagem dos dados; (b) Errado, firmware são instruções operacionais programadas diretamente no hardware de um equipamento eletrônico; (c) Errado,

modem é um dispositivo eletrônico que modula um sinal digital numa onda analógica; (d) Errado, roteador é um dispositivo que encaminha pacotes de dados entre redes de computadores, criando um conjunto de redes de sobreposição; (e) Errado, antivírus são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional.

Gabarito: Letra A

QUESTÕES COMENTADAS – FGV

34. (FGV / TRT-MA – 2022) Os firewalls podem ser um meio eficaz de proteger sistemas e redes contra ameaças de segurança. Com relação às suas limitações, analise os itens a seguir.

I. Não são capazes de proteger contra os ataques que contornam o firewall.
II. Não protegem contra ameaças internas, como funcionários insatisfeitos ou que cooperam com um atacante externo.
III. Não protegem contra a transferência de programas ou arquivos infectados com vírus.

Está correto o que se afirma em:

a) I, apenas.
b) II, apenas.
c) III, apenas.
d) I, II e III.
e) II e III, apenas.

Comentários:

(I) Correto. De fato, se não passa pelo firewall, não há como ele atuar; (II) Correto. Ele também não pode fazer nada quando a ameaça é interna (exceto em algumas configurações); (III) Correto. Ele realmente não protege contra a transferência de programas ou arquivos infectados com vírus.

Gabarito: Letra D

---

35. (FGV / TJDFT – 2022) Um órgão que lida com muitos documentos sigilosos sinalizou para sua equipe de Tecnologia da Informação (TI) sua preocupação quanto a uma invasão cibernética e roubo desses documentos. Para incrementar a segurança da rede desse órgão, a equipe de TI instalou um equipamento capaz de verificar as conexões TCP em andamento antes de permitir a passagem de um determinado pacote.

O equipamento instalado pela equipe de TI utiliza recursos de:

a) IDS (Intrusion Detection System);
b) gateway VPN;
c) gateway de aplicação;
d) filtro de pacotes tradicionais;
e) filtro de estado.

Comentários:

Equipamento capaz de verificar conexões TCP em andamento antes de permitir a passagem de um determinado pacote é o Filtro de Estado. Note que a questão fala em verificar conexões em andamento antes de permitir a passagem do pacote, isto é, ele analisa se já há uma conexão estabelecida – por essa razão, é chamado de filtro de inspeção de estado de sessão/conexão.

Gabarito: Letra E

---

36. (FGV / TJ-RS – 2020) No contexto da segurança em redes de computadores, o termo firewall pode ser considerado uma espécie de:

a) mecanismo de autenticação;
b) programa de transferência de arquivos seguro;
c) mecanismo que verifica e bloqueia spam de correio eletrônico;
d) antivírus, que pesquisa os arquivos em busca de programas malignos;
e) filtro, que restringe o tráfego de mensagens com sites e outros recursos.

Comentários:

(a) Errado, existem firewalls que podem realizar essa função de forma auxiliar, mas esse não é o padrão; (b) Errado, um firewall definitivamente não tem nenhuma relação com transferência de arquivos seguros; (c) Errado, existem firewalls que podem realizar essa função de forma auxiliar, mas esse não é o padrão; (d) Errado, firewalls definitivamente não são um antivírus; (e) Correto, ele realmente é uma espécie de filtro capaz de restringir o tráfego de mensagens com sites e outros recursos.

Gabarito: Letra E

---

37. (FGV / COMPESA – 2018) O perímetro de segurança da técnica de defesa em profundidade visa a aumentar a segurança da borda da rede. O componente do perímetro que visa a intermediar as mensagens de nível de aplicação entre clientes internos e servidores externos, para impor a política de segurança da empresa, é o:

a) Gateway VPN.
b) Firewall de Estado.
c) Firewall Proxy.
d) IDS.
e) DMZ.

Comentários:

Intermediar as mensagens de nível de aplicação entre clientes internos e servidores externos, para impor a política de segurança da empresa? Trata-se do Firewall Proxy!

Gabarito: Letra C

38. (FGV / AL-RO – 2018) Com o objetivo de restringir o acesso à Internet a um determinado aplicativo em um computador com sistema operacional Windows 10, deve-se configurar o componente do sistema chamado:

a) Firewall.
b) Blacklist.
c) tabela IP.
d) painel de controle.
e) driver de rede.

Comentários:

O componente que permite restringir o acesso à internet a um determinado aplicativo em um computador é o Firewall.

Gabarito: Letra A

39. (FGV / SEFIN-RO – 2018) Assinale a opção que descreve corretamente um firewall:

a) Um dispositivo de segurança de rede que monitora o tráfego de entrada e saída, e admite ou bloqueia tráfegos específicos de acordo com as regras de segurança estabelecidas.

b) Um antivírus que atua diretamente na conexão de uma rede interna, protegida, com o mundo exterior, de acordo com o tipo de malware a ser evitado.

c) Um nome genérico para um conjunto de procedimentos que realizam a autenticação de usuários de aplicações Web em uma rede protegida.

d) Um processo de criptografia dedicado aos procedimentos de codificação/decodificação do tráfego de entrada e saída de uma rede protegida.

e) Um servidor de nomes Web, utilizado para converter as palavras que compõem uma URL para o endereço IP correspondente.

Comentários:

(a) Correto, essa é a perfeita definição de firewall; (b) Errado, firewall definitivamente não é um antivírus; (c) Errado, isso seria um servidor de autenticação; (d) Errado, esse não é o conceito de um firewall; (e) Errado, isso seria um DNS (Domain Name System).

Gabarito: Letra A

40. (FGV / IBGE – 2016) Com relação aos firewalls, analise as afirmativas a seguir:

I. Um firewall de filtragem de pacotes faz as filtragens nas camadas de redes e de transporte.
II. Um firewall proxy faz as filtragens nas camadas de transporte e aplicação.
III. São uma combinação de softwares e hardwares instalados entre a rede interna de uma organização e a Intranet.

a) I;
b) II;
c) III;
d) I e II;
e) I e III.

Comentários:

(I) Correto, ele realmente opera nas camadas de redes e transporte; (II) Correto, um proxy é capaz de operar nas camadas de redes, transporte e aplicação. No entanto, a banca considerou esse item como errado em seu gabarito oficial – eu discordo; (III) Errado, eles são um hardware e/ou software instalado entre duas redes – a intranet é a rede interna, logo não faz sentido.

Gabarito: Letra A

---

41. (FGV / COMPESA - 2016) A ferramenta no sistema operacional Windows 2012, que impede o acesso de usuários não autorizados ao computador por meio das redes de computadores, controlando o fluxo de dados de entrada e saída, é denominado:

a) controlador de domínio.
b) criptografia.
c) software antivírus.
d) software antispyware.
e) firewall.

Comentários:

Impede o acesso de usuários não autorizados? Controle de fluxo de dados de entrada e saída? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

42. (FGV / TJ-BA - 2015) O software ou hardware utilizado para rejeitar ou permitir que informações da internet entrem no computador é o:

a) firewall;
b) cavalo de tróia (trojan);
c) anti-spyware;
d) certificado digital;
e) anti-vírus.

Comentários:

Software ou hardware? Rejeitar ou permitir que informações da internet entre no computador? Só pode estar se referindo ao Firewall!

Gabarito: Letra A

---

43. **(FGV / DPE RJ - 2014)** O sistema MS Windows oferece um recurso de segurança de rede que ajuda a impedir que programas mal-intencionados, ou hackers externos, obtenham acesso ao seu computador por meio da Internet, ou de outra rede qualquer. Esse recurso, que também ajuda a impedir que seus dados sejam enviados para outros computadores, é denominado:

a) Active-X.
b) Antivirus.
c) Filtro de linha.
d) Firewall.
e) Gerenciador de Tarefas.

Comentários:

Recurso de segurança? Impedir acesso ao computador? Impedir que dados sejam enviados para outros computadores? Só pode estar se referindo ao Firewall!

Gabarito: Letra D

QUESTÕES COMENTADAS – VUNESP

44.(VUNESP / PC-SP – 2022) Um dispositivo de segurança muito utilizado para proteger um computador contra acessos não autorizados vindos da Internet é o firewall pessoal. Quando esse dispositivo é configurado adequadamente, ele é capaz de alguns tipos de proteção, como:

a) bloquear todo o tráfego de saída e liberar todo o tráfego de entrada do computador, bloqueando o acesso a outros computadores e serviços, e permitindo que o computador seja acessado por outros computadores e serviços, o que é uma prática de alta segurança.

b) analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado.

c) impedir a execução de programas maliciosos baixados pelo usuário.

d) impedir que vírus ainda não conhecidos pelo programa antivírus contaminem o computador.

e) impedir que programas de e-mail baixem spam.

Comentários:

(a) Errado. Tudo errado nesse item, o firewall pessoal não bloqueia todo tráfego de saída nem libera todo tráfego de entrada e isso não é uma prática de alta segurança; (b) Correto; (c) Errado, ele não é capaz de impedir a execução de programas maliciosos baixados pelo usuário; (d) Errado, ele não é capaz de impedir que vírus ainda não conhecidos pelo programa antivírus contaminem o computador; (e) Errado, ele não é capaz de impedir que programas de e-mail baixem spam.

Gabarito: Letra B

45.(VUNESP / TJ-SP – 2012) O tipo de firewall que atua sobre o FTP, o SMTP, dentre outras aplicações, é também denominado de firewall:

a) de filtragem de pacotes
b) de transporte
c) de pacotes
d) proxy
e) sniffer

Comentários:

Aquele que trabalha na camada de aplicação é conhecido como proxy.

Gabarito: Letra D

46.(VUNESP / TJM SP - 2011) Um Firewall é um equipamento de rede utilizado para proteger a rede local de computadores. Considerando o modelo OSI para a interconexão de sistemas abertos, o Firewall atua no(s) nível(is), ou camada(s),

a) 4 e 5.
b) 5 e 7.
c) 2 e 3.
d) 3 e 4.
e) 6 e 7.

Comentários:

O Firewall pode trabalhar analisando protocolos – tradicionalmente, os protocolos que são conhecidos pelo Firewall se encontram nas camadas de Rede (IP, ICMP) e de Transporte (TCP, UDP). Há também protocolos da camada de aplicação!

Dessa forma, poderíamos ter como resposta qualquer combinação de Rede (3), Transporte (4) ou Aplicação (7). Como só há uma dessas combinações na resposta, ela é a correta!

Gabarito: Letra D

QUESTÕES COMENTADAS – CESGRANRIO

47. (CESGRANRIO / BB – 2021) Existem soluções de hardware e software que buscam minimizar as chances de um ataque a sistemas computacionais ser bem-sucedido. Dentre tais soluções de segurança, há uma que monitora o tráfego de entrada e saída de rede, funcionando como um filtro de pacotes, permitindo ou não a sua liberação a partir de um conjunto de regras específicas. Essa solução é o:

a) Antimalware.
b) Dispositivo USB.
c) Firewall.
d) Phishing.
e) SQL injection.

Comentários:

(a) Errado, essa é uma solução para prevenir, detectar e eliminar malwares; (b) Errado, isso é um dispositivo de entrada/saída de dados; (c) Correto; (d) Errado, isso é um tipo de fraude utilizada para enganar usuários e obter informações confidenciais; (e) Errado, esse é um tipo de ameaça de segurança que se aproveita de falhas de segurança em bases de dados.

Gabarito: Letra C

---

48. (CESGRANRIO / PETROBRAS - 2015) Um grupo de torcedores, insatisfeitos com o resultado do jogo em que seu time sofreu uma goleada, planejou invadir a rede de computadores do estádio onde ocorreu a disputa para tentar alterar o placar do jogo. Os torcedores localizaram a rede, porém, entre a rede interna e a externa, encontraram uma barreira que usou tecnologia de filtragem dos pacotes que eles estavam tentando enviar.

Essa barreira de segurança de filtro dos pacotes é o:

a) firewall
b) antivírus
c) antispam
d) proxy
e) PKI

Comentários:

Barreira entre a rede interna e externa? Tecnologia de filtragem dos pacotes? Só pode estar se referindo ao Firewall!

Gabarito: Letra A

49.(CESGRANRIO / BANCO DO BRASIL - 2014) Informações importantes de uma pessoa que teve seu computador invadido foram coletadas e enviadas para terceiros. Um amigo, especialista em informática, sugere-lhe a instalação de um programa que bloqueie o acesso de outros computadores que estejam tentando se conectar a programas instalados em seu computador. Esse tipo de programa é chamado de:

a) bloqueador de pop-ups.
b) antivírus.
c) filtro antispam.
d) filtro antiphishing.
e) firewall.

Comentários:

Para bloquear o acesso de outros computadores que estejam tentando se conectar a programas instalados em seu computador, recomenda-se utilizar um Firewall!

Gabarito: Letra E

50.(CESGRANRIO/ BANCO DA AMAZÔNIA - 2014) Um dos recursos presentes no Windows, desde a versão XP, é o Windows Firewall. Esse recurso tem o objetivo de:

a) aumentar a segurança do sistema.
b) melhorar o desempenho do sistema.
c) tornar o sistema mais acessível e prático.
d) melhorar a comunicação dos usuários com a Microsoft.
e) facilitar o uso do sistema por pessoas com necessidades especiais.

Comentários:

(a) Correto, ele realmente tem a função de aumentar a segurança do sistema; (b) Errado, ele não tem qualquer objetivo de melhorar o desempenho do sistema; (c) Errado, ele não torna o sistema mais acessível e prático; (d) Errado, ele definitivamente não tem nenhuma relação com a melhora da comunicação dos usuários com a Microsoft; (e) Errado, ele não tem o objetivo de facilitar o uso do sistema por pessoas com necessidades especiais.

Gabarito: Letra A

51.(CESGRANRIO / TRANSPETRO - 2012) Sistemas operacionais, como o Windows, trazem, em suas versões atuais, um programa no qual um dos objetivos é ajudar a impedir a invasão por hackers ou softwares mal-intencionados aos computadores dos usuários, podendo pôr em risco as informações neles contidas.

Esse tipo de programa consta, normalmente, nas políticas de proteção e segurança das empresas e é conhecido como:

a) administrador
b) decodificador
c) firewall
d) host
e) script

Comentários:

Ajuda a impedir a invasão? Consta nas políticas de proteção e segurança? Só pode estar se referindo ao Firewall!

Gabarito: Letra C

---

52. (CESGRANRIO / CEF – 2012) Firewall é um software ou hardware que verifica informações vindas da Internet ou de uma outra rede. Dentre os ataques que NÃO são neutralizados por um firewall, inclui-se o ataque de:

a) golpe de phishing
b) ping of death
c) rootkits
d) hackers
e) worms

Comentários:

Firewalls são capazes de neutralizar ataques de ping of death, rootkits, hackers ou worms, no entanto não são capazes de neutralizar o golpe de phishing (exceto firewall pessoal). Lembrando que o phishing é um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente, logo ele não pode fazer nada.

Gabarito: Letra A

---

53. (CESGRANRIO / PETROBRÁS – 2008) Em uma corporação, os serviços proxy são aplicações ou programas que têm acesso à Internet e à sua rede interna. Eles requerem dois componentes básicos que são, respectivamente,

a) cliente e servidor.
b) cliente e multiplexador.
c) multiplexador e roteador.

d) roteador e protocolo.
e) servidor e multiplexador.

Comentários:

Serviços de Proxy seguem o paradigma cliente-servidor – lembrando que um proxy é um servidor que age como um intermediário entre as requisições dos clientes.

Gabarito: Letra A

QUESTÕES COMENTADAS – DIVERSAS BANCAS

54. **(FUNDATEC / IPE SAÚDE – 2022)** As tabelas que definem, a partir da origem e do destino de cada pacote, se eles são permitidos, monitorados ou bloqueados pelo firewall são denominadas:

a) Tabelas de configuração do firewall.
b) Tabelas de alocação de pacotes.
c) Listas de histórico de uso da rede pelo usuário.
d) Listas de usuários da rede.
e) Listas de controle de acesso.

Comentários:

Essa questão pode confundir um pouco, mas vimos que os firewalls executam as políticas de segurança de uma organização por meio de Listas de Controle de Acesso (ACL). Por outro lado, o item (a) também poderia – a meu ver – ser uma resposta para questão. Logo, caberia recurso!

Gabarito: Letra E

---

55. **(FUNDATEC / IPE SAÚDE – 2022)** Existe um recurso que desempenha importante papel na proteção do perímetro da rede, protegendo a rede interna da rede externa, que normalmente é desprotegida. Esse recurso é denominado:

a) Roteador.
b) Firewall.
c) Hub.
d) Switch.
e) Access point.

Comentários:

O equipamento que filtra os dados entre a rede interna e externa é o... firewall.

Gabarito: Letra B

---

56. **(IDIB / Ministério da Economia – 2021)** Segundo a definição técnica de Firewall, ele é um dispositivo em uma rede de computadores, um programa ou equipamento físico, cujo objetivo é aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP. De acordo com essa definição, assinale a alternativa correta:

a) Firewall não protege contra a infecção de vírus ou outros tipos de malware, a não ser que já tenha esta função "acoplada" no appliance.

b) Snort é um programa do tipo firewall que também funciona como antivírus.

c) Uma de suas funções é o monitoramento do tráfego da rede, verificando somente os pacotes que entram na rede.

d) Uma de suas funções é o monitoramento do tráfego da rede, verificando apenas os pacotes que saem da rede.

e) O seu principal objetivo é proteger a integridade dos dados, não importando a confidencialidade deles.

Comentários:

(a) Correto; (b) Errado, ele é um software de detecção de intrusão; (c) Errado, ele verifica pacotes que entram e saem da rede; (d) Errado, ele verifica pacotes que entram e saem da rede; (e) Errado, também importa a proteção de sua confidencialidade.

Gabarito: Letra A

---

57. (FCM / PREF GUARANI - 2019) O programa utilizado para proteger um computador contra acessos não autorizados vindos da Internet é chamado:

a) Worm.
b) Firewall.
c) Spyware.
d) Google Drive.

Comentários:

O Firewall controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização. Ele é capaz de bloquear todo e qualquer acesso que possa prejudicar a rede ou o computador, tais como: acesso não autorizado, tentativas de vazamentos de informações, exploração de vulnerabilidades, violação de segurança, invasões maliciosas, ataques de hackers, etc.

(a) Worm é um tipo de software malicioso; (c) Spyware é um tipo de software malicioso; (d) Google Drive é um software de computação em nuvem.

Gabarito: Letra B

---

58. (FUNCERN / PREFEITURA DE PIRANHAS - 2019) Alan tem uma empresa autônoma de programação e se preocupa muito com a segurança da sua rede local. Para impedir uma

tentativa de acesso a sua rede a partir de hosts externos, ou qualquer tipo de invasão, Alan instalou na sua rede um:

a) antivírus.
b) bootloader.
c) firewall.
d) placa de diagnóstico

Comentários:

Impedir tentativas de acesso à rede por hosts externos podem ser realizadas por meio de um Firewall. (a) Antivírus não são capazes de impedir invasões; (b) Bootloader são softwares que auxiliam a inicialização do sistema operacional; (c) Placa de Diagnóstico é um dispositivo de hardware que auxilia a reparação de equipamentos.

Gabarito: Letra C

---

59. **(CETAP / PREF DE ANANINDEUA - 2019)** Firewall é uma solução de segurança baseada em hardware ou software (mais comum), onde sua função é:

a) separar os e-mails desejados dos indesejados (spams).
b) alertar o usuário quando há um problema no teclado.
c) alertar o usuário que há uma nova atualização do Word2010.
d) Controlar a movimentação de todos os dados do computador através da internet. Prevenir o vazamento de informações do computador para a internet, fazendo o bloqueio de acesso de softwares maliciosos que podem prejudicar o computador.

Comentários:

(a) Errado, isso é um antispam; (b) Errado, esse item não faz o menor sentido; (c) Errado, esse item não faz o menor sentido; (d) Correto, ele é realmente capaz de controlar a movimentação de todos os dados do computador através da internet. Prevenir o vazamento de informações do computador para a internet, fazendo o bloqueio de acesso de softwares maliciosos que podem prejudicar o computador.

Gabarito: Letra D

---

60. **(IF-PA / IF-PA - 2019)** É uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros, trata-se do:

a) browser.
b) firewall.

c) link.
d) plugin.
e) outlook.

Comentários:

O Firewall é um componente de segurança de uma rede privada (hardware, software ou uma combinação de ambos) que controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.

(a) Browser é simplesmente um navegador web; (c) Link é um elemento que permite conectar recursos web; (d) Plugin é um programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica; (e) Outlook é um cliente de e-mail da Microsoft.

Gabarito: Letra B

---

61. (IBADE / PREF DE CUJUBIM - 2018) Em uma rede de computadores, necessita-se instalar um equipamento que vai aplicar uma política de segurança à rede, realizando filtros de pacotes. Esse equipamento é um:

a) Firewall.
b) Wimax
c) Bridge.
d) Modem Dial-up.
e) Concentrador.

Comentários:

O Firewall é um componente de segurança de uma rede privada (hardware, software ou uma combinação de ambos) que controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização – um dos tipos desse equipamento é o Filtro de Pacotes.

(b) Wimax é uma rede wireless de grandes distâncias; (c) Bridge é um equipamento de rede da camada de enlace; (d) Modem Dial-Up é um equipamento que permite o acesso à internet por meio de linha telefônica; (e) Concentrador é um equipamento de rede da camada física.

Gabarito: Letra A

62.(IDIB / PREFEITURA DE PLANALTINA DE GOIÁS - 2018) Acerca dos conhecimentos de Firewall, marque a alternativa incorreta acerca de seu funcionamento.

a) Controla o tráfego de uma rede.
b) Previne o acesso não autorizado a uma rede de computadores.
c) Determina qual conteúdo é autorizado a circular em uma rede.
d) Substitui a utilização de antivírus.

Comentários:

(a) Correto, Firewall realmente controla o tráfego de uma rede; (b) Correto, Firewall realmente previne o acesso não autorizado a uma rede de computadores; (c) Correto, Firewall realmente determina qual conteúdo é autorizado a circular em uma rede (Ex: Proxy); (d) Errado, Firewall realmente não substitui a utilização de antivírus – eles são componentes complementares.

Gabarito: Letra D

63.(UECE-CEV / FUNCEME - 2018) Assinale a opção que corresponde à correta definição de firewall.

a) Software malicioso que se infiltra em computadores com o intuito de roubar ou danificar dados.

b) Programa de cifragem e deciframento de mensagens destinado a proteger dados dos usuários durante a navegação na web.

c) Dispositivo de segurança de rede que age monitorando o tráfego e detectando possíveis ameaças.

d) Rede privada de computadores, à qual somente usuários devidamente autorizados e autenticados podem acessar.

Comentários:

(a) Errado, ele não é um software malicioso; (b) Errado, ele não é um programa de cifragem; (c) Correto, ele é realmente um dispositivo de segurança de rede (hardware ou software) que age monitorando o tráfego (entradas e saídas de dados) e detectando possíveis ameaças; (d) Errado, ele não é uma rede privada de computadores.

Gabarito: Letra C

64.(UFMT / UFSBA - 2017) No Microsoft Windows 7, a ferramenta nativa de segurança que pode ajudar a impedir que hackers ou softwares mal-intencionados obtenham acesso ao computador por uma rede ou pela Internet chama-se:

a) Firewall do Windows.
b) Windows Update.
c) Central de Ações.
d) Backup e Restauração.

Comentários:

A ferramenta nativa do Windows que permite ajudar a impedir que hackers ou softwares mal-intencionados obtenham acesso ao computador por uma rede ou pela Internet é o Firewall do Windows (na versão mais atual desse sistema operacional, chama-se Windows Defender Firewall).

Gabarito: Letra A

65.(IF-PA / IF-PA - 2016) O programa que auxilia na proteção das informações contidas em computador é:

a) Limpeza de Disco
b) Desfragmentador de disco
c) Windows Apdate
d) DropBox
e) Firewall

Comentários:

A questão trata do Firewall – lembrem-se que ele pode ser um hardware ou software. Dessa forma, pode ser considerado um programa que auxilia na proteção das informações contidas no computador.

Gabarito: Letra E

---

66. (QUADRIX / CFP - 2016) Os firewalls ajudam a impedir que crackers ou softwares mal-intencionados obtenham acesso ao seu computador através de uma rede ou da Internet. Assim, é correto afirmar que os firewalls:

a) normalmente comparam os dados recebidos pela rede com as diretivas de segurança e liberam ou bloqueiam os pacotes.

b) também impedem que os funcionários que trabalham na empresa executem ações que comprometam o funcionamento da rede interna de computadores.

c) fazem parte do Sistema Operacional do computador, por isso não podem vir incorporados a roteadores ou modems de banda larga.

d) já vêm instalados em todas as versões do Windows, mas não podem ser desabilitados e nem desinstalados.

e) dispensam a instalação de antivírus, pois bloqueiam automaticamente arquivos suspeitos recebidos pela rede.

Comentários:

(a) Correto, ele controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política ou diretiva de segurança da organização; (b) Errado, ele não pode fazer nada contra funcionários na rede interna da empresa; (c) Errado, eles podem – sim – vir incorporados a roteadores ou modems; (d) Errado, eles podem – sim – ser desabilitados; (e) Errado, eles são complementares aos antivírus e não os substituem.

Gabarito: Letra A

---

67. (GESTÃO CONCURSO / CONSURGE - 2016) Assinale a alternativa que apresenta corretamente o elemento do Windows 7 com a função de proteger o computador de ataque e intrusão.

a) Windows Help
b) Monitor de Recursos
c) Firewall
d) Prompt de Comando

Comentários:

No Windows 7, o elemento com a função de proteger o computador de ataque e intrusão é o Windows Firewall (renomeado para Windows Defender Firewall no Windows 10).

Gabarito: Letra C

---

68. (CETAP / PREF DE BARCARENA - 2016) No contexto da segurança da informação, existe um sistema que é usado para prevenir o acesso não autorizado de usuários da Internet a uma rede privada (intranet). Esse sistema pode ser implementado em hardware, software ou combinação de ambos. As mensagens que entram e saem da intranet devem passar por esse sistema que aplica suas políticas de segurança para permitir ou não a transmissão das mesmas. Esse sistema é denominado:

a) Antispyware.
b) Firewall
c) Cavalo de tróia.
d) Antivírus.
e) Adware.

Comentários:

Prevenir acesso não autorizado a uma rede privada? Pode ser um hardware, software ou ambos? Aplicação de políticas de segurança? Só pode estar se referindo ao Firewall!

Gabarito: Letra B

---

69. (UFMS / UFMS - 2015) Como é denominada a combinação de Hardware Software que impede tráfego não autorizado entre a rede de uma empresa e a Internet?

a) Antivírus
b) Gateway
c) Filtros
d) Switch
e) Firewall

Comentários:

Combinação de hardware e software? Impede tráfego não autorizado? Entre rede da empresa (privada) e internet? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

70. (FUNCAB / FUNASG - 2015) Os dispositivos capazes de serem configurados para proteger redes de computadores contra determinados tipos de invasão são os que têm função de:

a) hub.
b) upstream.
c) firewall.
d) repetidor.
e) modem.

Comentários:

Proteger redes de computadores contra invasão? Trata-se do Firewall!

Gabarito: Letra C

---

71. **(UMA CONCURSOS / PREF SÃO SEBASTIÃO DO CAÍ - 2015)** O sistema Operacional Microsoft Windows versão 8 possui uma ferramenta para proteção de informações oriundas da Internet. Esta ferramenta verifica dados provenientes da internet e pode permitir sua entrada ou bloqueá-los de acordo com as regras configuradas de maneira a evitar invasões por parte de Hackers ou outros invasores. A ferramenta em questão é:

a) Gerenciador de Redes.
b) Assistente de Compartilhamento.
c) Antivirus.
d) Firewall.

Comentários:

Pode permitir ou bloquear a entrada de dados? Baseado em regras pré-configuradas? Evita invasões de hackers? Só pode estar se referindo ao Firewall!

Gabarito: Letra D

---

72. **(CRF-TO / CRF-TO - 2015)** Qual mecanismo mais utilizado para aumentar a segurança de redes de computadores legados à internet:

a) Criptografia
b) Firewall
c) Autenticação
d) Controle de acesso

Comentários:

Aumentar segurança de redes de computadores? Todos os itens contemplam essa funcionalidade, no entanto o mecanismo mais utilizado para tal é o Firewall!

Gabarito: Letra B

---

73. **(COPESE-UFPI / UFPI - 2015)** Dado o seguinte conceito: "solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas". Assinale a alternativa que corresponde a este conceito.

a) Cavalo de Troia
b) Antivírus
c) Backdoor
d) Roteador

e) Firewall

Comentários:

Solução de segurança? Baseada em hardware ou software? A partir de regras ou instruções (política de segurança)? Determina quais operações de transmissão ou recepção de dados? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

74. **(QUADRIX / CREF 11ª REGIÃO - 2014)** O firewall pode ser utilizado para proteger um computador contra acessos não autorizados vindos da internet. As configurações do firewall dependem de cada fabricante, porém, de forma geral, a mais indicada é:

a) liberar todo tráfego de entrada e saída do computador, bloqueando as conexões conforme necessário.

b) liberar somente o tráfego de saída do computador e bloquear todo tráfego de entrada para todos os programas, evitando, assim, os ataques via rede.

c) bloquear todo tráfego de entrada e saída do computador, liberando as conexões conforme necessário.

d) liberar todo tráfego de saída do computador e bloquear todo trafego de entrada ao computador, liberando as conexões conforme necessário, de acordo com os programas usados.

e) bloquear todo tráfego de saída do computador e liberar todo trafego de entrada ao computador, bloqueando as conexões conforme necessário.

Comentários:

A configuração mais adequada é liberar todo o tráfego de saída do computador e bloquear todo o tráfego de entrada ao computador, liberando as conexões conforme necessário, de acordo com os programas usados – trata-se do modo restritivo ou lista branca.

Gabarito: Letra D

---

75. **(FUNDEP / IF SP - 2014)** A função do _____ é proteger o computador de ataques e intrusão. É a primeira linha de defesa.

Assinale a alternativa que completa CORRETAMENTE a lacuna.

a) painel de segurança.

b) firewall do windows.
c) monitor de recursos.
d) prompt de comando.

Comentários:

(a) Errado, esse recurso não existe no Windows; (b) Correto, esse recurso realmente protege o computador de ataques e intrusão; (c) Errado, esse recurso monitora componentes de um computador (CPU, HD, Rede, etc); (d) Errado, esse recurso exibe uma tela através da qual o usuário pode digitar comandos.

Gabarito: Letra B

---

76. (FUNDEP / HTRN MG - 2014) Assinale a alternativa que apresenta CORRETAMENTE o aplicativo do Windows 7 que permite configurar as opções de segurança.

a) Desfragmentador de disco.
b) Firewall do Windows.
c) Paint.
d) Monitor de recursos.

Comentários:

No Windows 7, o elemento com a função de proteger o computador de ataque e intrusão é o Windows Firewall (renomeado para Windows Defender Firewall no Windows 10).

Gabarito: Letra B

---

77. (COPESE-UFPI / UFPI - 2014) Sobre o conceito, uso e configuração de um firewall, é INCORRETO afirmar que:

a) Pode ser implementado via hardware ou software.

b) Permite aplicar uma política de segurança à rede a qual está conectado, controlando o fluxo de pacotes.

c) No firewall que implementa a filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro.

d) Quando configurado corretamente, também impede as colisões de pacotes melhorando o desempenho da rede.

e) Um firewall de filtragem de pacotes está vulnerável ao IP spoofing.

Comentários:

(a) Correto, ele pode realmente ser hardware ou software; (b) Correto, ele realmente pode aplicar uma política de segurança à rede controlando o fluxo de pacotes; (c) Correto, o Firewall de filtragem estática ou filtro de pacotes bloqueia ou libera dados meramente com base nas regras implantadas no firewall, não importando a ligação que cada pacote tem com o outro; (d) Errado, ele não tem nenhuma ingerência quanto à colisão de pacotes; (e) Correto, IP Spoofing é o mascaramento de endereços IP – é o nome dado à técnica de um atacante usar uma fonte de endereço IP falsa nos pacotes que ele enviar ao firewall. Esse tipo de firewall realmente está vulnerável a esse tipo de ataque.

Gabarito: Letra D

---

78. (NUCEPE / PC-PI - 2014) Dispositivo que tem o objetivo de filtrar todo o fluxo de dados que entra e sai de uma rede de computadores e bloqueia acesso não autorizado ao computador é chamado de:

a) firewall.
b) hub.
c) switch.
d) access point.
e) modem.

Comentários:

Filtrar fluxo de dados? Bloqueia acesso não autorizado? Só pode estar se referindo ao Firewall!

(b) Errado, Hub é um dispositivo de rede da camada física; (c) Errado, Switch é um dispositivo de rede da camada de enlace; (d) Errado, Access Point é um dispositivo de rede responsável por estender um sinal; (e) Modem é um dispositivo de rede responsável por modular sinais digitais e analógicos.

Gabarito: Letra A

---

79. (FUNDEP / CAU-MG - 2014) O aplicativo do Windows 7 que configura as opções de segurança para proteger o computador de hackers e programas mal intencionados é:

a) Lupa.
b) Firewall do Windows.
c) Informações do sistema.
d) Prompt de comando.

Comentários:

No Windows 7, o aplicativo que configura as opções de segurança para proteger o computador de hackers e programas mal intencionados é o Firewall do Windows.

Gabarito: Letra B

80.(UNIRIO / UNIRIO - 2014) Para proteger a rede (ou um sistema) de uma empresa, impedindo que hackers ou softwares mal-intencionados (como worms) obtenham acesso aos computadores através da rede ou da Internet, a empresa deve instalar um:

a) Bloqueador de Pop-ups.
b) Bloqueador de Spam.
c) Firewall.
d) DNS.
e) Phishing.

Comentários:

Proteger a rede? Impedir o acesso aos computadores através da rede ou internet? Só pode estar se referindo ao Firewall.

(a) Errado, ele apenas bloqueia os pop-ups; (b) Errado, ele apenas bloqueia e-mails indesejados; (d) Errado, ele é apenas um protocolo de conversão de Endereço IP e Domínio; (e) Errado, esse é um ataque de tentativa de obtenção de informações.

Gabarito: Letra C

81.(UFBA/ UFBA - 2013) Um firewall é um programa instalado em um computador para permitir o acesso à Internet.

Comentários:

Na verdade, um firewall não tem o objetivo de permitir acesso à internet – ele tem o objetivo de controlar, analisar, registrar, policiar, monitorar, regular e filtrar o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.

Gabarito: Errada

82.(FUNDEP/ IPSEMG - 2013) A ferramenta do Windows 7 que tem por função proteger a máquina de ataque e intrusão é o:

a) desfragmentador de disco.
b) firewall do windows.
c) painel de controle.
d) windows powershell.

Comentários:

Proteger de ataques e de invasões é a função do Firewall do Windows.

Gabarito: Letra B

---

83. (QUADRIX/ CRBIO 5ª REGIÃO - 2013) Como é chamado o software que ajuda a impedir que hackers acessem um computador pela network ou pela Internet verificando as informações provenientes destas proibindo ou permitindo suas transmissões?

a) Anti Spyware.
b) AntiVírus.
c) Scandisk.
d) Sniffer.
e) Firewall.

Comentários:

(a) Errado, antispyware não detecta a presença de um invasor, somente de um malware; (b) Errado, antivirus não detecta a presença de um invasor, somente de um malware; (c) Errado, scandisk é uma ferramenta de diagnóstico do DOS que procura e repara erros no sistema de arquivos de um disco rígido; (d) Errado, sniffer não é usado para proteção, pelo contrário, é usado por um invasor para conseguir dados de forma escusa; (e) Correto, firewall usa um política de permissões para liberar ou não, conexões que entram e saem de uma rede.

Gabarito: Letra E

---

84. (QUADRIX/ CRO GO - 2013) O programa usado para proteger um computador contra acessos não autorizados vindos da internet é conhecido como:

a) Filtro antispam.
b) Firewall pessoal.
c) Pharming.
d) Rootkit.
e) Antivírus.

Comentários:

(a) Errado, antispam não protege contra acessos não autorizados, ele protege contra mensagens de e-mail indesejadas; (b) Correto, Firewall Pessoal realmente é utilizado para proteger um computador contra acessos não autorizados vindos da internet; (c) Errado, pharming é um ataque ao sistema de nomes de domínio de um computador; (d) Errado, rootkit é um software malicioso usado para permitir o acesso privilegiado a um computador ou a uma área do software que não é permitida; (e) Errado, antivírus não protege um computador contra acessos não autorizados vindos da internet – ele protege apenas contra vírus.

Gabarito: Letra B

---

85. (IF-CE / IF-CE - 2012) É o mecanismo de segurança do sistema operacional, que impede que usuários não autorizados obtenham acesso ao computador através de uma rede, como a Internet:

a) firewall.
b) atualização automática.
c) proteção contra vírus.
d) backup.
e) configuração de sistema.

Comentários:

Mecanismo de segurança? Impede acesso de usuários não autorizados? Só pode estar se referindo ao Firewall!

Gabarito: Letra A

---

86. (QUADRIX / CRP 9ª REGIÃO - 2012) A segurança da informação é feita de diversas formas, inclusive por meio da instalação de hardwares e softwares específicos. O hardware ou software que verifica as informações provenientes da internet ou de uma rede, filtrando-as de forma a selecionar as que chegam ao seu computador, é chamado de:

a) Firewall.
b) Antivírus.
c) AntiSPAM.
d) Roteador.
e) Antispyware.

Comentários:

Hardware ou software? Filtra informações? Seleciona o que chega ao computador? Só pode estar se referindo ao Firewall!

Gabarito: Letra A

---

87. (OBJETIVA / EPTC - 2012) Existe um sistema de segurança em que há uma combinação de hardware e software. É utilizado em diversas ocasiões nas redes de muitas empresas para impedir o acesso externo não autorizado à sua rede interna ou à intranet. Conhecido também como "a parede de fogo", serve como proteção de um simples computador de usuário doméstico até uma rede inteira com diversos computadores. Esse tipo de sistema é chamado de:

a) MMC.
b) Firewall.
c) DHCP.
d) Wall End.

Comentários:

Combinação de hardware e software? Impedir acesso externo não autorizado? Conhecido como parede de fogo? Só pode estar se referindo ao Firewall!

Gabarito: Letra B

---

88. (FUNIVERSA / IFB - 2012) Em segurança da informação, há um mecanismo que filtra as comunicações de uma rede para outra que é baseado em certas regras de controle e determina quais conexões serão aceitas ou negadas. Esse mecanismo é denominado:

a) backdoor.
b) VLAN.
c) honeypot.
d) VPN.
e) firewall.

Comentários:

Filtra as comunicações de uma rede para outra? Baseado em certas regras de controle? Determina quais conexões serão aceitas ou negadas? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

89. (UNIRIO / UNIRIO - 2012) Complete a lacuna adequadamente: O principal objetivo do _____ é evitar o acesso não autorizado, via internet, aos computadores.

a) bloqueador de popup
b) bloqueador de spyware

c) antispam
d) firewall
e) antivírus

Comentários:

O principal objetivo do Firewall é evitar o acesso não autorizado, via internet, aos computadores. Nenhuma outra opção completa a lacuna adequadamente.

Gabarito: Letra D

90.(UPENET-IAUPE / JUCEPE - 2012) A segurança de informações é um problema nas redes de computadores e na Internet. Para controlar o tráfego de informações em redes de computadores e autorizar programas a acessarem a rede, que mecanismo pode ser usado para estabelecer filtros por meio de políticas de segurança?

Esse tipo de programa consta, normalmente, nas políticas de proteção e segurança das empresas e é conhecido como:

a) Proxy.
b) Cookie.
c) Telnet.
d) Firewall.
e) DNS.

Comentários:

Controlar o tráfego de informações? Autorizar programas a acessarem a rede? Estabelecer filtros por meio de políticas de segurança? Só pode estar se referindo ao Firewall!

Gabarito: Letra D

91.(TJ SC / TJ SC - 2011) É um recurso do Windows 7 que, dentre outras coisas, pode ajudar a impedir que um hacker obtenha acesso ao computador do usuário. Estamos falando do:

a) Live Mail
b) Backup
c) Firewall
d) Bloco de notas
e) Explorer

Comentários:

Ajuda a impedir que um hacker obtenha acesso ao computador do usuário? Só pode estar falando de Firewall!

Gabarito: Letra C

---

92. (FESMIP-BA / MPE-BA - 2011) O software que tem como finalidade verificar as informações vindas da rede, impedindo ou permitindo o acesso ao computador é:

a) Antivírus
b) Firewall
c) Malware
d) Spyware
e) Phishing

Comentários:

Firewall controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.

Gabarito: Letra B

---

93. (UFMT / PREF CUIABÁ - 2010) Assinale o software oferecido pelo Windows XP que limita ou impede o acesso aos dados do computador por outros computadores por meio de uma rede.

a) Antivírus
b) Contas de usuário
c) Antispywares
d) Firewall

Comentários:

Limita ou impede acesso a dados do computador por outros computadores por meio de uma rede? Só pode estar se referindo ao Firewall!

Gabarito: Letra D

---

94. (IVIN / PREF PIRACICABA - 2010) Com relação ao Firewall, marque a alternativa INCORRETA:

a) É uma barreira de proteção, que controla o tráfego de dados entre seu computador e a rede.
b) Pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização.
c) Regula o tráfego de dados entre redes distintas.

d) Impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.
e) É um dos programas antivírus mais eficazes no mercado

Comentários:

(a) Correto, ele realmente controla o tráfego de dados entre seu computador e a rede; (b) Correto, ele realmente pode ser usado para ajudar a impedir que, sua rede ou seu computador sejam acessados sem autorização; (c) Correto, ele – de fato – regula o tráfego de dados entre redes distintas; (d) Correto, ele impede a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra; (e) Errado, firewall não é o mesmo que antivírus – eles são dispositivos complementares.

Gabarito: Letra E

---

95. **(FUNRIO / MJ - 2009)** Qual o nome dado ao dispositivo de segurança que, uma vez instalado, controla e autoriza o tráfego de informações transferidas entre redes de computadores?

a) Telnet
b) Firewall.
c) Cookie
d) Safenet.
e) Java

Comentários:

Dispositivo de segurança? Controla e autoriza o tráfego de informações? Entre redes de computadores? Só pode estar se referindo ao Firewall!

Gabarito: Letra B

---

96. **(FUNRIO / DEPEN - 2009)** As redes de computadores e o advento da Internet trouxeram facilidades de comunicação através dos computadores, porém introduziram problemas de segurança de informações. Qual o nome do mecanismo em redes de computadores que controla e autoriza o tráfego de informações, estabelecendo filtros através de políticas de segurança?

a) Cookie
b) Proxy
c) Telnet
d) Winsock
e) Firewall

Comentários:

Mecanismo que controla e autoriza o tráfego de informações? Estabelece filtros através de políticas de segurança? Só pode estar se referindo ao Firewall!

Gabarito: Letra E

---

97. (AV MOREIRA / Prefeitura de Landri Sales - PI – 2021) Barreira eletrônica que impede que usuários não autorizados tenham acesso a determinados arquivos:

a) Firewall.
b) Host.
c) Interface.
d) Trigger.
e) Webificar.

Comentários:

Barreira eletrônica? Impede acesso a usuários não autorizados? Trata-se do Firewall – ele realmente é capaz de impedir acessos não autorizados a arquivos específicos.

Gabarito: Letra A

---

98. (COPESE - UFPI / ALEPI – 2020) O firewall é um mecanismo de segurança utilizado nas redes de computadores. Assinale a assertiva INCORRETA a respeito desse mecanismo.

a) A sua utilização não dispensa o uso de antivírus.
b) É responsável por controlar o tráfego de dados entre a rede interna e a externa, normalmente a internet, impedindo ataques maliciosos.
c) Pode ser implementado em nível de hardware e/ou software.
d) Geralmente protegem redes TCP/IP.
e) Protege os computares de uma rede contra malwares contidos em dispositivos externos de armazenamento, como pen drives.

Comentários:

(a) Correto, a utilização de um firewall não dispensa o uso de antivírus porque eles possuem funções diferentes; (b) Correto, essa é a função principal de um firewall; (c) Correto, firewall realmente pode ser hardware e/ou firewall; (d) Correto, elas – de fato – protegem redes TCP/IP; (e) Errado, essa é a função de um antimalware e, não, de um firewall. Lembrem-se sempre que firewalls são barreiras que permitem controlar o tráfego de dados entre redes.

Gabarito: Letra E

---

99. (IBFC / EBSERH – 2020) Assinale a única que identifica corretamente a definição básica e conceitual de um firewall:

a) é um poderoso recurso para proteger uma rede de antivírus.
b) recurso que permite criptografar tanto uma rede PAN como LAN.
c) é um dispositivo de hardware que converte sinais analógicos em digitais.
d) é a primeira linha de defesa tanto em uma rede pessoal como corporativa.
e) transforma uma rede geral do tipo WAN em uma rede tipicamente PAN.

Comentários:

(a) Errado, não faz sequer sentido lógico – não existe uma rede de antivírus; (b) Errado, apesar de poder criptografar eventualmente como função auxiliar, essa definitivamente não é uma definição básica e conceitual de firewall; (c) Errado, essa seria a definição de um modem; (d) Correto, ele realmente funciona como uma primeira barreira tanto em uma rede pessoal (doméstica) quanto em uma rede corporativa; (e) Errado, esse item também não faz qualquer sentido.

Gabarito: Letra D

---

100. (Dédalus Concursos / COREN-SC – 2020) Julgue as assertivas a seguir a respeito do firewall:

(__) - Um firewall é um modelo de programa que filtra as informações que chegam da conexão de internet na rede privada da empresa e nos computadores;

(__) - Os 3 principais tipos de firewall existentes no mercado são: Firewall de aplicação, Filtragem de pacotes e Inspeção de estados;

(__) - Stateful Packet Inspection (SPI), conhecido também como inspeção de dados, é uma arquitetura de firewall que examina os fluxos de tráfego de ponta a ponta na rede. Usam uma maneira inteligente de evitar o tráfego não autorizado, analisando os cabeçalhos dos pacotes e inspecionando o estado de cada um;

(__) - O firewall de filtro de pacotes pode impedir todos os tipos de ataques, pois ele tem a capacidade de enfrentar os ataques que usam vulnerabilidades nas camadas de aplicativos e lutar contra ataques de falsificação.

a) V-V-V-F.
b) F-V-F-F.
c) V-F-V-V.
d) F-F-F-V.
e) V-V-F-F.

Comentários:

(V) Um firewall realmente filtra dados entre redes; (V) Esses realmente são os principais tipos de firewall – sendo que o firewall de aplicação pode ser chamado de Proxy; (V) Filtro de Estado de Sessão realmente examina os fluxos de tráfego de uma rede, por meio de uma análise de cabeçalhos dos pacotes assim como o estado de uma conexão; (F) *Todos os tipos de ataques? Camada de Aplicativos?* Filtros de pacotes não são capazes de impedir todos os tipos de ataques; eles não funcionam na camada de aplicação e, sim, na camada de rede e transporte.

Gabarito: Letra A

---

101. (IBADE / Prefeitura de Linhares - ES – 2020) Redes de computadores conectadas à internet são alvos de invasões por parte de hackers. A ferramenta para permitir o acesso à rede apenas por endereços autorizados é:

a) Criptografia.
b) Firewall.
c) Certificado digital.
d) Antivírus.
e) Modem.

Comentários:

A ferramenta para permitir o acesso à rede apenas por endereços autorizados, filtrando o tráfego e bloqueando acessos não autorizados, é o Firewall.

Gabarito: Letra B

---

102. (IBADE / Prefeitura de Linhares - ES – 2020) Uma proteção para redes de computadores contra acessos não autorizados é:

a) Criptografia.
b) Antivírus.
c) Hub.
d) Firewall.
e) Modem.

Comentários:

A proteção para redes contra acessos não autorizados é o Firewall.

Gabarito: Letra D

---

103. (FAFIPA / CREA-PR – 2019) A utilização correta da segurança disponibilizada pelo Sistema Operacional Windows auxilia na proteção contra possíveis ataques. O sistema citado disponibiliza de uma ferramenta, que por sua vez, filtra a entrada e saída de pacotes na rede, funcionando como uma parede de proteção para seu computador. Essa ferramenta é:

a) Navegador.
b) Roteador.
c) Modem.
d) Firewall.
e) Controle de banda.

Comentários:

A ferramenta que filtra a entrada e a saída de pacotes na rede, funcionando como uma parede de proteção (uma espécie de muro de fogo) para o seu computador é o Firewall.

Gabarito: Letra D

---

104. (Crescer Consultorias / Prefeitura de Jijoca de Jericoacoara - CE – 2019) Sobre definições básicas de internet, intranet, proxy, redes de computadores e firewall, julgue as afirmativas abaixo:

I. Servidor Proxy tem como objetivo converter URLs (endereços em formato de texto) em endereços IP e vice-versa.

II. Um Firewall pode ser construído por softwares ou por Hardwares. O objetivo primário de um firewall é permitir ou bloquear tráfego baseado em regras definidas pelo administrador da rede, funcionando como filtro.

III. Intranet é uma rede restrita que utiliza os protocolos e tecnologias diferentes dos utilizados pela Internet. Usualmente uma intranet é constituída por conexões através das quais um ou mais computadores são conectados à internet.

a) Somente a afirmativa I está correta.
b) Somente a afirmativa II está correta.
c) Somente as afirmativas I e II estão corretas.
d) Somente as afirmativas II e III estão corretas.

Comentários:

(I) Errado, essa é a função do DNS e, não, do Proxy; (II) Correto, ele realmente é um hardware e/ou software capaz de permitir ou bloquear tráfego baseado em regras definidas pelo administrador da rede, funcionando como filtro; (III) Errado, ele utiliza exatamente as mesmas tecnologias utilizadas pela Internet.

Gabarito: Letra B

---

105. (QUADRIX / CREA-TO – 2019) Os firewalls não podem ser usados como interface com outros dispositivos de segurança, como, por exemplo, servidores de autenticação.

Comentários:

Não só podem como geralmente são utilizados como interface com outros dispositivos de segurança. O servidor de autenticação é um exemplo – ele fornece um serviço de rede que os aplicativos usam para autenticar as credenciais, como nomes de contas e senhas, de seus usuários.

Gabarito: Errado

---

106. (IBFC / Prefeitura de Candeias - BA – 2019) Analise as afirmativas referente ao firewall (parede de fogo):

a) Um firewall somente pode ser concebível tecnicamente se for puro hardware.
b) Um firewall somente pode ser concebível tecnicamente se for puro software.
c) Um firewall é somente um conceito virtual, portanto não é nem hardware e nem software.
d) Um firewall pode ser tanto hardware, software ou ambos.

Comentários:

Um firewall pode ser um hardware e/ou software.

Gabarito: Letra D

---

107. (UNIRV/GO / UNIRV/GO – 2017 – Item II) Proxy age como intermediário nas requisições entre componentes da rede e entidades externas ou internas a ela de modo a simplificar ou controlar a sua complexidade.

Comentários:

Ele realmente age como intermediário nas requisições entre componentes da rede e entidades externas ou internas a ela de modo a simplificar ou controlar a sua complexidade.

Gabarito: Correto

---

108. (Instituto Pró-Município / CRP-CE – 2019) Em muitas empresas para se conectar à Internet a partir da rede interna, se faz necessário configurar nas opções de rede ou no seu browser a conexão com um servidor intermediário. Este servidor administra as requisições para a Internet e os procedimentos de segurança sob elas. Como é conhecido esse servidor.

a) Proxy
b) Backup
c) FTP
d) DNS

Comentários:

O servidor proxy é responsável por funcionar como um servidor intermediário entre a internet e a rede interna de uma organização.

Gabarito: Letra A

---

109. (Instituto Acesso / Colégio Pedro II – 2015) Em um ambiente com sistema operacional Windows 7 e utilizando-se o navegador Internet Explorer é possível estabelecer configurações que habilitam o uso de um servidor Proxy. Neste contexto um Proxy é:

a) um servidor que funciona como intermediário entre um navegador da Web (como o Internet Explorer) e a Internet.

b) um servidor que fornece endereços IP dinâmicos aos computadores da rede local.

c)um serviço que somente permite o acesso de usuários que se autentiquem, tornando a rede mais segura.

d) uma ferramenta de busca customizada pelas empresas para acesso aos dados locais.

e) um servidor de correio eletrônico, que utilizando meios de comunicação seguros, garante o envio de mensagens

Comentários:

O proxy é um servidor que funciona como intermediário entre um navegador da web (como o Internet Explorer) e a Internet – nenhuma das outras opções faz qualquer sentido.

Gabarito: Letra A

---

110. (Crescer Consultoria / Prefeitura de Várzea Grande/PI – 2019) Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são conhecidos como:

a) Proxy
b) Criptografia

c) AntiSpam
d) Certificado Digital

Comentários:

Aquele que trabalha na camada de aplicação é conhecido como proxy.

Gabarito: Letra A

---

111. (CS-UFG / UFG – 2018) Em redes de computadores, um servidor (sistema de computador ou uma aplicação) que atua como um intermediário entre os computadores de uma rede e a Internet é conhecido como:

a) servidor de aplicação
b) servidor dhcp
c) servidor proxy
d) servidor dns

Comentários:

O servidor proxy é um sistema de computador/aplicação (hardware/software) que atua como intermediário entre os computadores de uma rede e a Internet.

Gabarito: Letra C

---

112. (FADESP / DETRAN/PA – 2019) Sobre aplicativos e procedimentos de Internet, o servidor que realiza a função de mediar as comunicações da rede de uma empresa com a Internet é denominado:

a) servidor de páginas.
b) servidor proxy.
c) servidor de arquivos.
d) servidor Web.
e) servidor FTP.

Comentários:

O servidor proxy é responsável por mediar as comunicações da rede de uma empresa com a Internet.

Gabarito: Letra B

---

113. (UECE-CEV / DETRAN-CE – 2018) Proxy é um servidor que age intermediando a Internet e a rede local.

Comentários:

O servidor proxy faz a intermediação entre requisições de uma rede privada local e a Internet.

Gabarito: Correto

LISTA DE QUESTÕES – CESPE

1. **(CESPE / DPE-RO – 2021)** Vários pacotes de dados que chegaram a um sistema de firewall foram bloqueados ao terem sido verificados, por não haver, no firewall, informações de estado de conexão para os endereços referidos nos pacotes e os serviços relacionados.

   Nessa situação hipotética, a atividade que permitiu verificar e invalidar os pacotes de dados no firewall é denominada:

   a) filtragem de pacotes stateless.
   b) filtragem de proxy de aplicação.
   c) inspeção de pacotes stateful.
   d) filtragem de pacotes fragmentados.
   e) inspeção profunda de protocolo.

2. **(CESPE / CGE - CE – 2019)** Para proteger a comunicação em uma organização que possui várias redes internas de computadores interligadas entre si e também à Internet contra ações maliciosas no tráfego dos dados, o mecanismo a ser utilizado é o:

   a) registro de logs.
   b) antispam
   c) firewall
   d) antispyware
   e) controlador de domínio.

3. **(CESPE / Polícia Federal – 2018)** Marta utiliza uma estação de trabalho que executa o sistema operacional Windows 10 e está conectada à rede local da empresa em que ela trabalha. Ela acessa usualmente os sítios da intranet da empresa e também sítios da Internet pública. Após navegar por vários sítios, Marta verificou o histórico de navegação e identificou que um dos sítios acessados com sucesso por meio do protocolo HTTP tinha o endereço 172.20.1.1.

   Tendo como referência essa situação hipotética, julgue o item a seguir.

   A despeito das configurações dos ativos de segurança corporativos e do serviço de firewall instalado na estação de trabalho, Marta poderá acessar remotamente sua estação de trabalho usando a Conexão de Área de Trabalho Remota, a partir de outra estação conectada à Internet.

4. **(CESPE / Polícia Federal – 2018)** Um firewall é uma combinação de hardware e software que isola da Internet a rede interna de uma organização, permitindo o gerenciamento do fluxo de tráfego e dos recursos da rede e o controle, pelo administrador de rede, do acesso ao mundo externo.

5. **(CESPE / Polícia Federal – 2018)** Um dos objetivos do firewall é monitorar todo o tráfego de dados entrando e saindo de uma rede local e entrar em ação ao identificar um sniffer externo.

6. **(CESPE / Polícia Federal – 2018)** Em um firewall, devem ser controlados não apenas os pacotes que entram em uma rede privada, mas também aqueles que saem da rede para a Internet.

7. **(CESPE / EMAP – 2018)** Os administradores de rede fazem uso do firewall statefull para filtrar pacotes baseados em endereços de IP, protocolos, portas e estado das conexões.

8. **(CESPE / TRE BA - 2017)** Assinale a opção que apresenta a solução que permite filtrar tentativas de acessos não autorizados oriundos de outros ambientes e redes externas, contribuindo para a melhora do estado de segurança da informação de ambientes computacionais.

   a) certificado digital
   b) chave de criptografia
   c) rootkits
   d) firewall
   e) antivírus

9. **(CESPE / FUB – 2016)** Ferramentas de firewall são amplamente utilizadas em redes de computadores, de maneira a permitir ou negar determinado fluxo de pacotes. Com relação a firewall convencional de rede, julgue o item subsecutivo.

   Um firewall é capaz de verificar tanto o endereço IP de origem quanto o endereço IP de destino em um pacote de rede.

10. **(CESPE / FUB – 2016)** Firewall é um recurso utilizado para restringir alguns tipos de permissões previamente configuradas, a fim de aumentar a segurança de uma rede ou de um computador contra acessos não autorizados.

11. **(CESPE / FUB – 2016)** Firewall é capaz de verificar tanto o endereço IP de origem quanto o endereço IP de destino em um pacote de rede.

12. **(CESPE / TCE-PA – 2016)** Por padrão, um WAF (Web Application Firewall) é capaz de utilizar as camadas de rede, de transporte e de aplicação da pilha TCP/IP.

13. **(CESPE / MEC – 2015)** Uma das características mais importantes do proxy é a restrição de acesso a sítios não autorizados, executada por meio de listas de controle de acesso (access control lists).

14. **(CESPE – TCU – 2015)** O firewall é capaz de proteger o computador tanto de ataques de crackers quanto de ataques de vírus.

15. **(CESPE/ MTE - 2013)** O firewall é um sistema antivírus que inibe a infecção de novos tipos de vírus. Para ser eficiente, o firewall deve ser atualizado frequentemente.

16. **(CESPE / MPU – 2013)** Uma das funções dos firewalls é implementar políticas relativas à separação do tráfego interno e externo à rede a ser protegida, visto que eles filtram o tráfego de entrada e saída de rede.

17. **(CESPE/ PC AL - 2012)** Um firewall do tipo stateful não verifica o estado de uma conexão.

18. **(CESPE / Polícia Federal - 2012)** Quando a solicitação de conexão do tipo UDP na porta 21 for recebida por estação com firewall desligado, caberá ao sistema operacional habilitar o firewall, receber a conexão, processar a requisição e desligar o firewall. Esse procedimento é realizado porque a função do UDP na porta 21 é testar a conexão do firewall com a Internet.

19. **(CESPE / MCT - 2012)** Um firewall serve, basicamente, para filtrar os pacotes que entram e(ou) saem de um computador e para verificar se o tráfego é permitido ou não.

20. **(CESPE / FNDE - 2012)** Para proteger um computador contra os efeitos de um worm, pode-se utilizar, como recurso, um firewall pessoal.

21. **(CESPE / TJ-AC - 2012)** Em um computador com o Windows instalado, o firewall detecta e desativa os vírus e worms que estejam contaminando o computador.

22. **(CESPE – ANAC – 2012)** Um firewall pessoal é uma opção de ferramenta preventiva contra worms.

23. **(CESPE / IFB - 2011)** Ferramentas como firewall e antivírus para estação de trabalho não ajudam a reduzir riscos de segurança da informação.

24. **(CESPE / AL ES - 2011)** Existem diversos dispositivos que protegem tanto o acesso a um computador quanto a toda uma rede. Caso um usuário pretenda impedir que o tráfego com origem na Internet faça conexão com seu computador pessoal, a tecnologia adequada a ser utilizada nessa situação será o:

    a) multicast.
    b) instant message.
    c) miniDim.
    d) firewall.
    e) Ipv6.

25. **(CESPE / SEDUC-AM – 2011)** Um firewall pessoal é um software ou programa utilizado para proteger um computador contra acessos não autorizados provenientes da Internet.

LISTA DE QUESTÕES – FCC

26. (FCC / Prefeitura de Teresina - PI – 2016) A proteção das informações e dos sistemas das organizações requer o uso de recursos de proteção como os firewalls, utilizados para:

a) ajudar a impedir que a rede privada da empresa seja acessada sem autorização a partir da Internet.

b) liberar o uso de todos os serviços de rede somente aos usuários registrados pelo administrador da rede.

c) garantir que cada pacote de dados seja entregue com segurança apenas ao destinatário informado, reduzindo assim o tráfego na rede.

d) garantir que nenhum colaborador possa comprometer a segurança das informações da organização.

e) garantir que os computadores da rede não sejam infectados por malwares ou atacados por hackers.

27. (FCC / SEFAZ PE - 2014) Um dos mecanismos básicos de segurança da informação é um componente de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Este componente de segurança existe na forma de software, de hardware ou da combinação de ambos. Atualmente, os principais sistemas operacionais trazem este componente embutido na forma de software para proteger computadores contra acessos não autorizados vindos da Internet. O texto descreve o componente conhecido como:

a) firewall.
b) sniffer.
c) antivirus.
d) proxy.
e) scandisk.

28. (FCC / MPE-SE – 2013) Um determinado tipo de servidor permite que páginas comumente acessadas na internet sejam armazenadas localmente. Quando tais páginas são requisitadas, suas cópias locais são transferidas para o usuário de forma transparente e, por estarem já armazenadas no servidor local, são retornadas de forma muito mais ágil. Estes servidores são chamados de:

a) WAN.
b) DDoS.

c) Web Servers.
d) PPP.
e) Proxy.

29. **(FCC / TJ-PE - 2012)** Ajuda a impedir que hackers ou programas mal-intencionados acessem um computador via internet ou por uma rede. Software ou hardware que verifica as informações provenientes da Internet, ou de uma rede, e as bloqueia ou permite que elas cheguem ao seu computador, dependendo das configurações. Trata-se de:

a) criptograma.
b) keylogger.
c) screenlogger.
d) cavalo de troia
e) firewall

30. **(FCC / TRE-PR - 2012)** Uma barreira protetora que monitora e restringe as informações passadas entre o seu computador e uma rede ou a Internet, fornece uma defesa por software contra pessoas que podem tentar acessar seu computador de fora sem a sua permissão é chamada de:

a) ActiveX.
b) Roteador.
c) Chaves públicas.
d) Criptografia.
e) Firewall.

31. **(FCC / TJ-PE – 2012)** Um dos tipos existentes de firewall é o filtro de camada da aplicação. Neste modo, o bloqueio é realizado ao se analisar:

a) a aplicação das regras para determinada camada, como por exemplo camadas IP ou ethernet.

b) endereços de origem e destinos ou números de portas dos pacotes enviados e/ou recebidos.

c) listas brancas ou negras que possuem os nomes das aplicações bloqueadas ou liberadas para uma determinada topologia.

d) detalhes específicos de cada aplicação, como por exemplo, cabeçalhos de mensagens de e-mail.

e) a quantidade de acessos de uma aplicação em um endereço ou porta específica da internet em um determinado período de tempo, evitando dessa forma ataques como o denial-of-service (DoS).

32. **(FCC / TRF 1ª REGIÃO - 2011)** Dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede de computadores de uma empresa. Sua

função consiste em regular o tráfego de dados entre essa rede e a internet e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados. Trata-se de:

a) antivírus.
b) firewall.
c) mailing.
d) spyware.
e) adware.

33. **(FCC / INFRAERO - 2011)** O controle de transmissão de dados em uma rede de computadores, filtrando e permitindo ou não a passagem dos dados, é a principal função realizada pelo dispositivo denominado:

a) firewall.
b) firmware.
c) modem.
d) roteador.
e) antivírus.

LISTA DE QUESTÕES – FGV

34. **(FGV / TRT-MA – 2022)** Os firewalls podem ser um meio eficaz de proteger sistemas e redes contra ameaças de segurança. Com relação às suas limitações, analise os itens a seguir.

I. Não são capazes de proteger contra os ataques que contornam o firewall.
II. Não protegem contra ameaças internas, como funcionários insatisfeitos ou que cooperam com um atacante externo.
III. Não protegem contra a transferência de programas ou arquivos infectados com vírus.

Está correto o que se afirma em:

a) I, apenas.
b) II, apenas.
c) III, apenas.
d) I, II e III.
e) II e III, apenas.

35. **(FGV / TJDFT – 2022)** Um órgão que lida com muitos documentos sigilosos sinalizou para sua equipe de Tecnologia da Informação (TI) sua preocupação quanto a uma invasão cibernética e roubo desses documentos. Para incrementar a segurança da rede desse órgão, a equipe de TI instalou um equipamento capaz de verificar as conexões TCP em andamento antes de permitir a passagem de um determinado pacote.

O equipamento instalado pela equipe de TI utiliza recursos de:

a) IDS (Intrusion Detection System);
b) gateway VPN;
c) gateway de aplicação;
d) filtro de pacotes tradicionais;
e) filtro de estado.

36. **(FGV / TJ-RS – 2020)** No contexto da segurança em redes de computadores, o termo firewall pode ser considerado uma espécie de:

a) mecanismo de autenticação;
b) programa de transferência de arquivos seguro;
c) mecanismo que verifica e bloqueia spam de correio eletrônico;
d) antivírus, que pesquisa os arquivos em busca de programas malignos;
e) filtro, que restringe o tráfego de mensagens com sites e outros recursos.

37. **(FGV / COMPESA – 2018)** O perímetro de segurança da técnica de defesa em profundidade visa a aumentar a segurança da borda da rede. O componente do perímetro que visa a intermediar as mensagens de nível de aplicação entre clientes internos e servidores externos, para impor a política de segurança da empresa, é o:

a) Gateway VPN.
b) Firewall de Estado.
c) Firewall Proxy.
d) IDS.
e) DMZ.

38. **(FGV / AL-RO – 2018)** Com o objetivo de restringir o acesso à Internet a um determinado aplicativo em um computador com sistema operacional Windows 10, deve-se configurar o componente do sistema chamado:

a) Firewall.
b) Blacklist.
c) tabela IP.
d) painel de controle.
e) driver de rede.

39. **(FGV / SEFIN-RO – 2018)** Assinale a opção que descreve corretamente um firewall:

a) Um dispositivo de segurança de rede que monitora o tráfego de entrada e saída, e admite ou bloqueia tráfegos específicos de acordo com as regras de segurança estabelecidas.

b) Um antivírus que atua diretamente na conexão de uma rede interna, protegida, com o mundo exterior, de acordo com o tipo de malware a ser evitado.

c) Um nome genérico para um conjunto de procedimentos que realizam a autenticação de usuários de aplicações Web em uma rede protegida.

d) Um processo de criptografia dedicado aos procedimentos de codificação/decodificação do tráfego de entrada e saída de uma rede protegida.

e) Um servidor de nomes Web, utilizado para converter as palavras que compõem uma URL para o endereço IP correspondente.

40. **(FGV / IBGE – 2016)** Com relação aos firewalls, analise as afirmativas a seguir:

I. Um firewall de filtragem de pacotes faz as filtragens nas camadas de redes e de transporte.
II. Um firewall proxy faz as filtragens nas camadas de transporte e aplicação.
III. São uma combinação de softwares e hardwares instalados entre a rede interna de uma organização e a Intranet.

a) I;
b) II;
c) III;
d) I e II;
e) I e III.

41. **(FGV / COMPESA - 2016)** A ferramenta no sistema operacional Windows 2012, que impede o acesso de usuários não autorizados ao computador por meio das redes de computadores, controlando o fluxo de dados de entrada e saída, é denominado:

a) controlador de domínio.
b) criptografia.
c) software antivírus.
d) software antispyware.
e) firewall.

42. **(FGV / TJ-BA - 2015)** O software ou hardware utilizado para rejeitar ou permitir que informações da internet entrem no computador é o:

a) firewall;
b) cavalo de tróia (trojan);
c) anti-spyware;
d) certificado digital;
e) anti-vírus.

43. **(FGV / DPE RJ - 2014)** O sistema MS Windows oferece um recurso de segurança de rede que ajuda a impedir que programas mal-intencionados, ou hackers externos, obtenham acesso ao seu computador por meio da Internet, ou de outra rede qualquer. Esse recurso, que também ajuda a impedir que seus dados sejam enviados para outros computadores, é denominado:

a) Active-X.
b) Antivirus.
c) Filtro de linha.
d) Firewall.
e) Gerenciador de Tarefas.

LISTA DE QUESTÕES – VUNESP

44.(VUNESP / PC-SP – 2022) Um dispositivo de segurança muito utilizado para proteger um computador contra acessos não autorizados vindos da Internet é o firewall pessoal. Quando esse dispositivo é configurado adequadamente, ele é capaz de alguns tipos de proteção, como:

a) bloquear todo o tráfego de saída e liberar todo o tráfego de entrada do computador, bloqueando o acesso a outros computadores e serviços, e permitindo que o computador seja acessado por outros computadores e serviços, o que é uma prática de alta segurança.

b) analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado.

c) impedir a execução de programas maliciosos baixados pelo usuário.

d) impedir que vírus ainda não conhecidos pelo programa antivírus contaminem o computador.

e) impedir que programas de e-mail baixem spam.

45.(VUNESP / TJ-SP – 2012) O tipo de firewall que atua sobre o FTP, o SMTP, dentre outras aplicações, é também denominado de firewall:

a) de filtragem de pacotes
b) de transporte
c) de pacotes
d) proxy
e) sniffer

46.(VUNESP / TJM SP - 2011) Um Firewall é um equipamento de rede utilizado para proteger a rede local de computadores. Considerando o modelo OSI para a interconexão de sistemas abertos, o Firewall atua no(s) nível(is), ou camada(s),

a) 4 e 5.
b) 5 e 7.
c) 2 e 3.
d) 3 e 4.
e) 6 e 7.

LISTA DE QUESTÕES – CESGRANRIO

47. **(CESGRANRIO / BB – 2021)** Existem soluções de hardware e software que buscam minimizar as chances de um ataque a sistemas computacionais ser bem-sucedido. Dentre tais soluções de segurança, há uma que monitora o tráfego de entrada e saída de rede, funcionando como um filtro de pacotes, permitindo ou não a sua liberação a partir de um conjunto de regras específicas. Essa solução é o:

a) Antimalware.
b) Dispositivo USB.
c) Firewall.
d) Phishing.
e) SQL injection.

48. **(CESGRANRIO / PETROBRAS - 2015)** Um grupo de torcedores, insatisfeitos com o resultado do jogo em que seu time sofreu uma goleada, planejou invadir a rede de computadores do estádio onde ocorreu a disputa para tentar alterar o placar do jogo. Os torcedores localizaram a rede, porém, entre a rede interna e a externa, encontraram uma barreira que usou tecnologia de filtragem dos pacotes que eles estavam tentando enviar.

Essa barreira de segurança de filtro dos pacotes é o:

a) firewall
b) antivírus
c) antispam
d) proxy
e) PKI

49. **(CESGRANRIO / BANCO DO BRASIL - 2014)** Informações importantes de uma pessoa que teve seu computador invadido foram coletadas e enviadas para terceiros. Um amigo, especialista em informática, sugere-lhe a instalação de um programa que bloqueie o acesso de outros computadores que estejam tentando se conectar a programas instalados em seu computador. Esse tipo de programa é chamado de:

a) bloqueador de pop-ups.
b) antivírus.
c) filtro antispam.
d) filtro antiphishing.
e) firewall.

50. **(CESGRANRIO/ BANCO DA AMAZÔNIA - 2014)** Um dos recursos presentes no Windows, desde a versão XP, é o Windows Firewall. Esse recurso tem o objetivo de:

a) aumentar a segurança do sistema.
b) melhorar o desempenho do sistema.
c) tornar o sistema mais acessível e prático.
d) melhorar a comunicação dos usuários com a Microsoft.
e) facilitar o uso do sistema por pessoas com necessidades especiais.

51. **(CESGRANRIO / TRANSPETRO - 2012)** Sistemas operacionais, como o Windows, trazem, em suas versões atuais, um programa no qual um dos objetivos é ajudar a impedir a invasão por hackers ou softwares mal-intencionados aos computadores dos usuários, podendo pôr em risco as informações neles contidas.

Esse tipo de programa consta, normalmente, nas políticas de proteção e segurança das empresas e é conhecido como:

a) administrador
b) decodificador
c) firewall
d) host
e) script

52. **(CESGRANRIO / CEF – 2012)** Firewall é um software ou hardware que verifica informações vindas da Internet ou de uma outra rede. Dentre os ataques que NÃO são neutralizados por um firewall, inclui-se o ataque de:

a) golpe de phishing
b) ping of death
c) rootkits
d) hackers
e) worms

53. **(CESGRANRIO / PETROBRÁS – 2008)** Em uma corporação, os serviços proxy são aplicações ou programas que têm acesso à Internet e à sua rede interna. Eles requerem dois componentes básicos que são, respectivamente,

a) cliente e servidor.
b) cliente e multiplexador.
c) multiplexador e roteador.
d) roteador e protocolo.
e) servidor e multiplexador.

LISTA DE QUESTÕES – DIVERSAS BANCAS

54. **(FUNDATEC / IPE SAÚDE – 2022)** As tabelas que definem, a partir da origem e do destino de cada pacote, se eles são permitidos, monitorados ou bloqueados pelo firewall são denominadas:

a) Tabelas de configuração do firewall.
b) Tabelas de alocação de pacotes.
c) Listas de histórico de uso da rede pelo usuário.
d) Listas de usuários da rede.
e) Listas de controle de acesso.

55. **(FUNDATEC / IPE SAÚDE – 2022)** Existe um recurso que desempenha importante papel na proteção do perímetro da rede, protegendo a rede interna da rede externa, que normalmente é desprotegida. Esse recurso é denominado:

a) Roteador.
b) Firewall.
c) Hub.
d) Switch.
e) Access point.

56. **(IDIB / Ministério da Economia – 2021)** Segundo a definição técnica de Firewall, ele é um dispositivo em uma rede de computadores, um programa ou equipamento físico, cujo objetivo é aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP. De acordo com essa definição, assinale a alternativa correta:

a) Firewall não protege contra a infecção de vírus ou outros tipos de malware, a não ser que já tenha esta função "acoplada" no appliance.

b) Snort é um programa do tipo firewall que também funciona como antivírus.

c) Uma de suas funções é o monitoramento do tráfego da rede, verificando somente os pacotes que entram na rede.

d) Uma de suas funções é o monitoramento do tráfego da rede, verificando apenas os pacotes que saem da rede.

e) O seu principal objetivo é proteger a integridade dos dados, não importando a confidencialidade deles.

57. **(FCM / PREF GUARANI - 2019)** O programa utilizado para proteger um computador contra acessos não autorizados vindos da Internet é chamado:

a) Worm.
b) Firewall.
c) Spyware.
d) Google Drive.

58. **(FUNCERN / PREFEITURA DE PIRANHAS - 2019)** Alan tem uma empresa autônoma de programação e se preocupa muito com a segurança da sua rede local. Para impedir uma tentativa de acesso a sua rede a partir de hosts externos, ou qualquer tipo de invasão, Alan instalou na sua rede um:

a) antivírus.
b) bootloader.
c) firewall.
d) placa de diagnóstico

59. **(CETAP / PREF DE ANANINDEUA - 2019)** Firewall é uma solução de segurança baseada em hardware ou software (mais comum), onde sua função é:

a) separar os e-mails desejados dos indesejados (spams).
b) alertar o usuário quando há um problema no teclado.
c) alertar o usuário que há uma nova atualização do Word2010.
d) Controlar a movimentação de todos os dados do computador através da internet. Prevenir o vazamento de informações do computador para a internet, fazendo o bloqueio de acesso de softwares maliciosos que podem prejudicar o computador.

60. **(IF-PA / IF-PA - 2019)** É uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros, trata-se do:

a) browser.
b) firewall.
c) link.
d) plugin.
e) outlook.

61. **(IBADE / PREF DE CUJUBIM - 2018)** Em uma rede de computadores, necessita-se instalar um equipamento que vai aplicar uma política de segurança à rede, realizando filtros de pacotes. Esse equipamento é um:

a) Firewall.
b) Wimax
c) Bridge.
d) Modem Dial-up.

e) Concentrador.

62. **(IDIB / PREFEITURA DE PLANALTINA DE GOIÁS - 2018)** Acerca dos conhecimentos de Firewall, marque a alternativa incorreta acerca de seu funcionamento.

a) Controla o tráfego de uma rede.
b) Previne o acesso não autorizado a uma rede de computadores.
c) Determina qual conteúdo é autorizado a circular em uma rede.
d) Substitui a utilização de antivírus.

63. **(UECE-CEV / FUNCEME - 2018)** Assinale a opção que corresponde à correta definição de firewall.

a) Software malicioso que se infiltra em computadores com o intuito de roubar ou danificar dados.

b) Programa de cifragem e deciframento de mensagens destinado a proteger dados dos usuários durante a navegação na web.

c) Dispositivo de segurança de rede que age monitorando o tráfego e detectando possíveis ameaças.

d) Rede privada de computadores, à qual somente usuários devidamente autorizados e autenticados podem acessar.

64. **(UFMT / UFSBA - 2017)** No Microsoft Windows 7, a ferramenta nativa de segurança que pode ajudar a impedir que hackers ou softwares mal-intencionados obtenham acesso ao computador por uma rede ou pela Internet chama-se:

a) Firewall do Windows.
b) Windows Update.
c) Central de Ações.
d) Backup e Restauração.

65. **(IF-PA / IF-PA - 2016)** O programa que auxilia na proteção das informações contidas em computador é:

a) Limpeza de Disco
b) Desfragmentador de disco
c) Windows Apdate
d) DropBox
e) Firewall

66. **(QUADRIX / CFP - 2016)** Os firewalls ajudam a impedir que crackers ou softwares mal-intencionados obtenham acesso ao seu computador através de uma rede ou da Internet. Assim, é correto afirmar que os firewalls:

a) normalmente comparam os dados recebidos pela rede com as diretivas de segurança e liberam ou bloqueiam os pacotes.

b) também impedem que os funcionários que trabalham na empresa executem ações que comprometam o funcionamento da rede interna de computadores.

c) fazem parte do Sistema Operacional do computador, por isso não podem vir incorporados a roteadores ou modems de banda larga.

d) já vêm instalados em todas as versões do Windows, mas não podem ser desabilitados e nem desinstalados.

e) dispensam a instalação de antivírus, pois bloqueiam automaticamente arquivos suspeitos recebidos pela rede.

67. **(GESTÃO CONCURSO / CONSURGE - 2016)** Assinale a alternativa que apresenta corretamente o elemento do Windows 7 com a função de proteger o computador de ataque e intrusão.

a) Windows Help
b) Monitor de Recursos
c) Firewall
d) Prompt de Comando

68. **(CETAP / PREF DE BARCARENA - 2016)** No contexto da segurança da informação, existe um sistema que é usado para prevenir o acesso não autorizado de usuários da Internet a uma rede privada (intranet). Esse sistema pode ser implementado em hardware, software ou combinação de ambos. As mensagens que entram e saem da intranet devem passar por esse sistema que aplica suas políticas de segurança para permitir ou não a transmissão das mesmas. Esse sistema é denominado:

a) Antispyware.
b) Firewall
c) Cavalo de tróia.
d) Antivírus.
e) Adware.

69. **(UFMS / UFMS - 2015)** Como é denominada a combinação de Hardware Software que impede tráfego não autorizado entre a rede de uma empresa e a Internet?

a) Antivírus

b) Gateway
c) Filtros
d) Switch
e) Firewall

70. **(FUNCAB / FUNASG - 2015)** Os dispositivos capazes de serem configurados para proteger redes de computadores contra determinados tipos de invasão são os que têm função de:

a) hub.
b) upstream.
c) firewall.
d) repetidor.
e) modem.

71. **(UMA CONCURSOS / PREF SÃO SEBASTIÃO DO CAÍ - 2015)** O sistema Operacional Microsoft Windows versão 8 possui uma ferramenta para proteção de informações oriundas da Internet. Esta ferramenta verifica dados provenientes da internet e pode permitir sua entrada ou bloqueá-los de acordo com as regras configuradas de maneira a evitar invasões por parte de Hackers ou outros invasores. A ferramenta em questão é:

a) Gerenciador de Redes.
b) Assistente de Compartilhamento.
c) Antivirus.
d) Firewall.

72. **(CRF-TO / CRF-TO - 2015)** Qual mecanismo mais utilizado para aumentar a segurança de redes de computadores legados à internet:

a) Criptografia
b) Firewall
c) Autenticação
d) Controle de acesso

73. **(COPESE-UFPI / UFPI - 2015)** Dado o seguinte conceito: "solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas". Assinale a alternativa que corresponde a este conceito.

a) Cavalo de Troia
b) Antivírus
c) Backdoor
d) Roteador
e) Firewall

74. **(QUADRIX / CREF 11ª REGIÃO - 2014)** O firewall pode ser utilizado para proteger um computador contra acessos não autorizados vindos da internet. As configurações do firewall dependem de cada fabricante, porém, de forma geral, a mais indicada é:

a) liberar todo tráfego de entrada e saída do computador, bloqueando as conexões conforme necessário.

b) liberar somente o tráfego de saída do computador e bloquear todo tráfego de entrada para todos os programas, evitando, assim, os ataques via rede.

c) bloquear todo tráfego de entrada e saída do computador, liberando as conexões conforme necessário.

d) liberar todo tráfego de saída do computador e bloquear todo trafego de entrada ao computador, liberando as conexões conforme necessário, de acordo com os programas usados.

e) bloquear todo tráfego de saída do computador e liberar todo trafego de entrada ao computador, bloqueando as conexões conforme necessário.

75. **(FUNDEP / IF SP - 2014)** A função do _____ é proteger o computador de ataques e intrusão. É a primeira linha de defesa.

Assinale a alternativa que completa CORRETAMENTE a lacuna.

a) painel de segurança.
b) firewall do windows.
c) monitor de recursos.
d) prompt de comando.

76. **(FUNDEP / HTRN MG - 2014)** Assinale a alternativa que apresenta CORRETAMENTE o aplicativo do Windows 7 que permite configurar as opções de segurança.

a) Desfragmentador de disco.
b) Firewall do Windows.
c) Paint.
d) Monitor de recursos.

77. **(COPESE-UFPI / UFPI - 2014)** Sobre o conceito, uso e configuração de um firewall, é INCORRETO afirmar que:

a) Pode ser implementado via hardware ou software.

b) Permite aplicar uma política de segurança à rede a qual está conectado, controlando o fluxo de pacotes.

c) No firewall que implementa a filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro.

d) Quando configurado corretamente, também impede as colisões de pacotes melhorando o desempenho da rede.

e) Um firewall de filtragem de pacotes está vulnerável ao IP spoofing.

78. **(NUCEPE / PC-PI - 2014)** Dispositivo que tem o objetivo de filtrar todo o fluxo de dados que entra e sai de uma rede de computadores e bloqueia acesso não autorizado ao computador é chamado de:

a) firewall.
b) hub.
c) switch.
d) access point.
e) modem.

79. **(FUNDEP / CAU-MG - 2014)** O aplicativo do Windows 7 que configura as opções de segurança para proteger o computador de hackers e programas mal intencionados é:

a) Lupa.
b) Firewall do Windows.
c) Informações do sistema.
d) Prompt de comando.

80. **(UNIRIO / UNIRIO - 2014)** Para proteger a rede (ou um sistema) de uma empresa, impedindo que hackers ou softwares mal-intencionados (como worms) obtenham acesso aos computadores através da rede ou da Internet, a empresa deve instalar um:

a) Bloqueador de Pop-ups.
b) Bloqueador de Spam.
c) Firewall.
d) DNS.
e) Phishing.

81. **(UFBA/ UFBA - 2013)** Um firewall é um programa instalado em um computador para permitir o acesso à Internet.

82. **(FUNDEP/ IPSEMG - 2013)** A ferramenta do Windows 7 que tem por função proteger a máquina de ataque e intrusão é o:

a) desfragmentador de disco.

b) firewall do windows.
c) painel de controle.
d) windows powershell.

83. (QUADRIX/ CRBIO 5ª REGIÃO - 2013) Como é chamado o software que ajuda a impedir que hackers acessem um computador pela network ou pela Internet verificando as informações provenientes destas proibindo ou permitindo suas transmissões?

a) Anti Spyware.
b) AntiVírus.
c) Scandisk.
d) Sniffer.
e) Firewall.

84. (QUADRIX/ CRO GO - 2013) O programa usado para proteger um computador contra acessos não autorizados vindos da internet é conhecido como:

a) Filtro antispam.
b) Firewall pessoal.
c) Pharming.
d) Rootkit.
e) Antivírus.

85. (IF-CE / IF-CE - 2012) É o mecanismo de segurança do sistema operacional, que impede que usuários não autorizados obtenham acesso ao computador através de uma rede, como a Internet:

a) firewall.
b) atualização automática.
c) proteção contra vírus.
d) backup.
e) configuração de sistema.

86. (QUADRIX / CRP 9ª REGIÃO - 2012) A segurança da informação é feita de diversas formas, inclusive por meio da instalação de hardwares e softwares específicos. O hardware ou software que verifica as informações provenientes da internet ou de uma rede, filtrando-as de forma a selecionar as que chegam ao seu computador, é chamado de:

a) Firewall.
b) Antivírus.
c) AntiSPAM.
d) Roteador.
e) Antispyware.

87. **(OBJETIVA / EPTC - 2012)** Existe um sistema de segurança em que há uma combinação de hardware e software. É utilizado em diversas ocasiões nas redes de muitas empresas para impedir o acesso externo não autorizado à sua rede interna ou à intranet. Conhecido também como "a parede de fogo", serve como proteção de um simples computador de usuário doméstico até uma rede inteira com diversos computadores. Esse tipo de sistema é chamado de:

a) MMC.
b) Firewall.
c) DHCP.
d) Wall End.

88. **(FUNIVERSA / IFB - 2012)** Em segurança da informação, há um mecanismo que filtra as comunicações de uma rede para outra que é baseado em certas regras de controle e determina quais conexões serão aceitas ou negadas. Esse mecanismo é denominado:

a) backdoor.
b) VLAN.
c) honeypot.
d) VPN.
e) firewall.

89. **(UNIRIO / UNIRIO - 2012)** Complete a lacuna adequadamente: O principal objetivo do _____ é evitar o acesso não autorizado, via internet, aos computadores.

a) bloqueador de popup
b) bloqueador de spyware
c) antispam
d) firewall
e) antivírus

90. **(UPENET-IAUPE / JUCEPE - 2012)** A segurança de informações é um problema nas redes de computadores e na Internet. Para controlar o tráfego de informações em redes de computadores e autorizar programas a acessarem a rede, que mecanismo pode ser usado para estabelecer filtros por meio de políticas de segurança?

Esse tipo de programa consta, normalmente, nas políticas de proteção e segurança das empresas e é conhecido como:

a) Proxy.
b) Cookie.
c) Telnet.
d) Firewall.
e) DNS.

91. **(TJ SC / TJ SC - 2011)** É um recurso do Windows 7 que, dentre outras coisas, pode ajudar a impedir que um hacker obtenha acesso ao computador do usuário. Estamos falando do:

a) Live Mail
b) Backup
c) Firewall
d) Bloco de notas
e) Explorer

92. **(FESMIP-BA / MPE-BA - 2011)** O software que tem como finalidade verificar as informações vindas da rede, impedindo ou permitindo o acesso ao computador é:

a) Antivírus
b) Firewall
c) Malware
d) Spyware
e) Phishing

93. **(UFMT / PREF CUIABÁ - 2010)** Assinale o software oferecido pelo Windows XP que limita ou impede o acesso aos dados do computador por outros computadores por meio de uma rede.

a) Antivírus
b) Contas de usuário
c) Antispywares
d) Firewall

94. **(IVIN / PREF PIRACICABA - 2010)** Com relação ao Firewall, marque a alternativa INCORRETA:

a) É uma barreira de proteção, que controla o tráfego de dados entre seu computador e a rede.
b) Pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização.
c) Regula o tráfego de dados entre redes distintas.
d) Impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.
e) É um dos programas antivírus mais eficazes no mercado

95. **(FUNRIO / MJ - 2009)** Qual o nome dado ao dispositivo de segurança que, uma vez instalado, controla e autoriza o tráfego de informações transferidas entre redes de computadores?

a) Telnet
b) Firewall.
c) Cookie
d) Safenet.

e) Java

96. (FUNRIO / DEPEN - 2009) As redes de computadores e o advento da Internet trouxeram facilidades de comunicação através dos computadores, porém introduziram problemas de segurança de informações. Qual o nome do mecanismo em redes de computadores que controla e autoriza o tráfego de informações, estabelecendo filtros através de políticas de segurança?

a) Cookie
b) Proxy
c) Telnet
d) Winsock
e) Firewall

97. (AV MOREIRA / Prefeitura de Landri Sales - PI – 2021) Barreira eletrônica que impede que usuários não autorizados tenham acesso a determinados arquivos:

a) Firewall.
b) Host.
c) Interface.
d) Trigger.
e) Webificar.

98. (COPESE - UFPI / ALEPI – 2020) O firewall é um mecanismo de segurança utilizado nas redes de computadores. Assinale a assertiva INCORRETA a respeito desse mecanismo.

a) A sua utilização não dispensa o uso de antivírus.
b) É responsável por controlar o tráfego de dados entre a rede interna e a externa, normalmente a internet, impedindo ataques maliciosos.
c) Pode ser implementado em nível de hardware e/ou software.
d) Geralmente protegem redes TCP/IP.
e) Protege os computares de uma rede contra malwares contidos em dispositivos externos de armazenamento, como pen drives.

99. (IBFC / EBSERH – 2020) Assinale a única que identifica corretamente a definição básica e conceitual de um firewall:

a) é um poderoso recurso para proteger uma rede de antivírus.
b) recurso que permite criptografar tanto uma rede PAN como LAN.
c) é um dispositivo de hardware que converte sinais analógicos em digitais.
d) é a primeira linha de defesa tanto em uma rede pessoal como corporativa.
e) transforma uma rede geral do tipo WAN em uma rede tipicamente PAN.

100. (Dédalus Concursos / COREN-SC – 2020) Julgue as assertivas a seguir a respeito do firewall:

(__) - Um firewall é um modelo de programa que filtra as informações que chegam da conexão de internet na rede privada da empresa e nos computadores;

(__) - Os 3 principais tipos de firewall existentes no mercado são: Firewall de aplicação, Filtragem de pacotes e Inspeção de estados;

(__) - Stateful Packet Inspection (SPI), conhecido também como inspeção de dados, é uma arquitetura de firewall que examina os fluxos de tráfego de ponta a ponta na rede. Usam uma maneira inteligente de evitar o tráfego não autorizado, analisando os cabeçalhos dos pacotes e inspecionando o estado de cada um;

(__) - O firewall de filtro de pacotes pode impedir todos os tipos de ataques, pois ele tem a capacidade de enfrentar os ataques que usam vulnerabilidades nas camadas de aplicativos e lutar contra ataques de falsificação.

a) V-V-V-F.
b) F-V-F-F.
c) V-F-V-V.
d) F-F-F-V.
e) V-V-F-F.

101. (IBADE / Prefeitura de Linhares - ES – 2020) Redes de computadores conectadas à internet são alvos de invasões por parte de hackers. A ferramenta para permitir o acesso à rede apenas por endereços autorizados é:

a) Criptografia.
b) Firewall.
c) Certificado digital.
d) Antivírus.
e) Modem.

102. (IBADE / Prefeitura de Linhares - ES – 2020) Uma proteção para redes de computadores contra acessos não autorizados é:

a) Criptografia.
b) Antivírus.
c) Hub.
d) Firewall.
e) Modem.

103. (FAFIPA / CREA-PR – 2019) A utilização correta da segurança disponibilizada pelo Sistema Operacional Windows auxilia na proteção contra possíveis ataques. O sistema citado

disponibiliza de uma ferramenta, que por sua vez, filtra a entrada e saída de pacotes na rede, funcionando como uma parede de proteção para seu computador. Essa ferramenta é:

a) Navegador.
b) Roteador.
c) Modem.
d) Firewall.
e) Controle de banda.

104. (Crescer Consultorias / Prefeitura de Jijoca de Jericoacoara - CE – 2019) Sobre definições básicas de internet, intranet, proxy, redes de computadores e firewall, julgue as afirmativas abaixo:

I. Servidor Proxy tem como objetivo converter URLs (endereços em formato de texto) em endereços IP e vice-versa.

II. Um Firewall pode ser construído por softwares ou por Hardwares. O objetivo primário de um firewall é permitir ou bloquear tráfego baseado em regras definidas pelo administrador da rede, funcionando como filtro.

III. Intranet é uma rede restrita que utiliza os protocolos e tecnologias diferentes dos utilizados pela Internet. Usualmente uma intranet é constituída por conexões através das quais um ou mais computadores são conectados à internet.

a) Somente a afirmativa I está correta.
b) Somente a afirmativa II está correta.
c) Somente as afirmativas I e II estão corretas.
d) Somente as afirmativas II e III estão corretas.

105. (QUADRIX / CREA-TO – 2019) Os firewalls não podem ser usados como interface com outros dispositivos de segurança, como, por exemplo, servidores de autenticação.

106. (IBFC / Prefeitura de Candeias - BA – 2019) Analise as afirmativas referente ao firewall (parede de fogo):

a) Um firewall somente pode ser concebível tecnicamente se for puro hardware.
b) Um firewall somente pode ser concebível tecnicamente se for puro software.
c) Um firewall é somente um conceito virtual, portanto não é nem hardware e nem software.
d) Um firewall pode ser tanto hardware, software ou ambos.

107. (UNIRV/GO / UNIRV/GO – 2017 – Item II) Proxy age como intermediário nas requisições entre componentes da rede e entidades externas ou internas a ela de modo a simplificar ou controlar a sua complexidade.

108. (Instituto Pró-Município / CRP-CE – 2019) Em muitas empresas para se conectar à Internet a partir da rede interna, se faz necessário configurar nas opções de rede ou no seu browser a conexão com um servidor intermediário. Este servidor administra as requisições para a Internet e os procedimentos de segurança sob elas. Como é conhecido esse servidor.

a) Proxy
b) Backup
c) FTP
d) DNS

109. (Instituto Acesso / Colégio Pedro II – 2015) Em um ambiente com sistema operacional Windows 7 e utilizando-se o navegador Internet Explorer é possível estabelecer configurações que habilitam o uso de um servidor Proxy. Neste contexto um Proxy é:

a) um servidor que funciona como intermediário entre um navegador da Web (como o Internet Explorer) e a Internet.

b) um servidor que fornece endereços IP dinâmicos aos computadores da rede local.

c)um serviço que somente permite o acesso de usuários que se autentiquem, tornando a rede mais segura.

d) uma ferramenta de busca customizada pelas empresas para acesso aos dados locais.

e) um servidor de correio eletrônico, que utilizando meios de comunicação seguros, garante o envio de mensagens

110. (Crescer Consultoria / Prefeitura de Várzea Grande/PI – 2019) Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são conhecidos como:

a) Proxy
b) Criptografia
c) AntiSpam
d) Certificado Digital

111. (CS-UFG / UFG – 2018) Em redes de computadores, um servidor (sistema de computador ou uma aplicação) que atua como um intermediário entre os computadores de uma rede e a Internet é conhecido como:

a) servidor de aplicação
b) servidor dhcp
c) servidor proxy

d) servidor dns

112. (FADESP / DETRAN/PA – 2019) Sobre aplicativos e procedimentos de Internet, o servidor que realiza a função de mediar as comunicações da rede de uma empresa com a Internet é denominado:

a) servidor de páginas.
b) servidor proxy.
c) servidor de arquivos.
d) servidor Web.
e) servidor FTP.

113. (UECE-CEV / DETRAN-CE – 2018) Proxy é um servidor que age intermediando a Internet e a rede local.

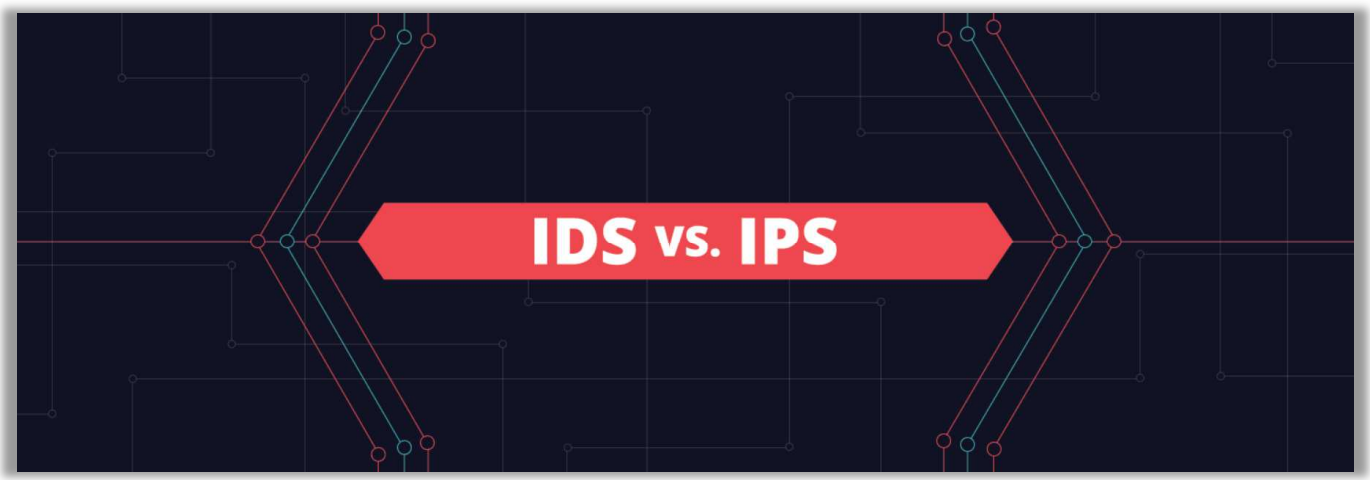
GABARITO

1. LETRA C
2. LETRA C
3. ERRADO
4. CORRETO
5. ERRADO
6. CORRETO
7. CORRETO
8. LETRA D
9. CORRETO
10. CORRETO
11. CORRETO
12. ERRADO
13. CORRETO
14. CORRETO
15. ERRADA
16. CORRETO
17. ERRADA
18. ERRADA
19. CORRETA
20. CORRETA
21. ERRADA
22. CORRETO
23. ERRADA
24. LETRA D
25. CORRETO
26. LETRA A
27. LETRA A
28. LETRA E
29. LETRA E
30. LETRA E
31. LETRA D
32. LETRA B
33. LETRA A
34. LETRA D
35. LETRA E
36. LETRA E
37. LETRA C
38. LETRA A
39. LETRA A
40. LETRA A
41. LETRA E
42. LETRA A
43. LETRA D
44. LETRA B
45. LETRA D
46. LETRA D
47. LETRA C
48. LETRA A
49. LETRA E
50. LETRA A
51. LETRA C
52. LETRA A
53. LETRA A
54. LETRA E
55. LETRA B
56. LETRA A
57. LETRA B
58. LETRA C
59. LETRA D
60. LETRA B
61. LETRA A
62. LETRA D
63. LETRA C
64. LETRA A
65. LETRA E
66. LETRA A
67. LETRA C
68. LETRA B
69. LETRA E
70. LETRA C
71. LETRA D
72. LETRA B
73. LETRA E
74. LETRA D
75. LETRA B
76. LETRA B
77. LETRA D
78. LETRA A
79. LETRA B
80. LETRA C
81. ERRADA
82. LETRA B
83. LETRA E
84. LETRA B
85. LETRA A
86. LETRA A
87. LETRA B
88. LETRA E
89. LETRA D
90. LETRA D
91. LETRA C
92. LETRA B
93. LETRA D
94. LETRA E
95. LETRA B
96. LETRA E
97. LETRA A
98. LETRA E
99. LETRA D
100. LETRA A
101. LETRA B
102. LETRA D
103. LETRA D
104. LETRA B
105. ERRADO
106. LETRA D
107. CORRETO
108. LETRA A
109. LETRA A
110. LETRA A
111. LETRA C
112. LETRA B
113. CORRETO

MECANISMOS AVANÇADOS

IDS/IPS

INCIDÊNCIA EM PROVA: BAIXA



Eu gostaria de começar esse tópico com a seguinte frase: se tem um grupo de seres humanos obstinados nesse mundo, esses são os hackers/crackers! Galera, eles são incansáveis – se alguém cria um mecanismo de segurança, eles arrumam uma maneira de burlá-lo. Existe uma guerra eterna entre hackers e analistas de segurança: um para tentar invadir sistemas e o outro para impedir a invasão. **Uma tecnologia utilizada para incrementar a segurança são os sistemas de invasão...**

Nós já sabemos que filtros de pacotes inspecionam cabeçalhos de protocolos de rede e de transporte quando estão decidindo quais pacotes deixarão passar através do firewall. **No entanto, para detectar alguns tipos de ataque, é preciso executar uma inspeção profunda de pacote, ou seja, é necessário olhar através não só dos campos de cabeçalho, mas também dentro dos dados da aplicação que o pacote carrega.**

O Proxy (ou Gateway de Aplicação) frequentemente faz inspeções profundas de pacote, mas ele tem uma grande desvantagem: ele só executa isso para uma aplicação específica, então se você possui diversos tipos diferentes de aplicações, são necessários diversos proxies diferentes. **Foi quando alguém pensou: existe espaço para mais um dispositivo que não apenas examine cabeçalhos de todos os pacotes, mas que faça uma inspeção profunda em cada pacote...**

Quando tal dispositivo observa o pacote suspeito – ou uma série de pacotes suspeitos – ele pode impedir que tais pacotes entrem na rede da organização; ou – quando a atividade só é vista como suspeita – o dispositivo pode deixar os pacotes passarem, mas envia um alerta ao administrador de rede, que pode examinar o tráfego minuciosamente e tomar as ações que ele achar mais adequadas. **Pois bem... eles foram criados!**

IDS (INTRUSION DETECTION SYSTEM)	Em português, Sistema de Detecção de Intrusão – trata-se de um dispositivo passivo que monitora a rede, detecta e alerta quando observa tráfegos potencialmente mal-intencionados, mas não os bloqueia.
IPS (INTRUSION PREVENTION SYTEM)	Em português, Sistema de Prevenção de Intrusão – trata-se de um dispositivo reativo ou proativo que monitora a rede, detecta e bloqueia quando observa tráfegos potencialmente mal intencionados.

(DETRAN/ES – 2010) As ferramentas de IDS (Sistema de Detecção de Intrusão) atuam de forma mais proativa que as ferramentas de IPS (Sistemas e Prevenção de Intrusão).

_____

Comentários: na verdade, o IPS é mais proativo que o IDS (Errado).

O IDS pode ser usado para detectar uma série de tipos de ataques, tais como: mapeamento de rede, varreduras de porta, ataques de negação de serviço, ataques de inundação de largura de banda, worms e vírus, ataques de vulnerabilidade de sistemas operações e de aplicações. **Para tal, ele não só precisa fazer uma inspeção profunda do pacote, como também precisa comparar cada pacote que passa com milhares de assinaturas.** *Como é isso, Diego?*

Sistemas IDS são classificados de modo geral tanto como sistemas baseados em assinatura[1]. Isso significa que ele mantém um banco de dados extenso de ataques de assinaturas, em que cada assinatura é um conjunto de regras relacionadas a uma atividade de invasão. Uma assinatura pode ser uma lista de características sobre um único pacote (Ex: número de porta, tipo de protocolo, sequência de bits) ou estar relacionada a uma série de pacotes.

As assinaturas são normalmente criadas por engenheiros de segurança de rede que tenham pesquisado ataques conhecidos. O administrador de rede pode personalizar as assinaturas ou inserir suas próprias no banco de dados. Dessa forma, cada que pacote que trafega na rede é analisado e comparado com as assinaturas no banco de dados. Se um pacote corresponder a uma assinatura do banco de dados, gera-se apenas um alerta e/ou um log (registro de evento)!

Apesar de serem amplamente executados, esses sistemas possuem diversas limitações. Acima de tudo, eles requerem conhecimento prévio do ataque para gerar uma assinatura precisa no banco de dados, isto é, eles são completamente cegos a novos ataques que ainda não foram registrados. **Outra desvantagem é que – mesmo que uma assinatura combine – isso pode não ser o resultado de um ataque, mas mesmo assim um alarme é gerado (é o famoso falso-positivo).**

(BASA – 2010) Os IDS e IPS embasados em detecção por assinatura podem apresentar ocorrência de falsos-positivos, sendo mais severos os efeitos nos IPS que nos IDS.

_____

[1] Há também sistemas de intrusão baseados em anomalias ou comportamentos, que procuram por fluxos de pacotes que são estatisticamente incomuns. Dessa forma, ele pode identificar comportamentos estranhos e bloquear preventivamente ataques. Uma vantagem é que ele é capaz de identificar ataques novos, que não possuem assinaturas no banco de dados; por outro lado, eles são bem menos eficientes que a assinatura em si.

Comentários: o falso-positivo ocorre quando um fluxo normal de dados é considerado como um ataque. No entanto, ambos podem apresentar falsos-positivos, sendo os efeitos mais severos no IPS que no IDS. *Por que?* Porque – diante de um falso-positivo - o IDS apenas gerará uma alerta na ocorrência normal, mas permitirá o tráfego de dados; já o IPS bloqueará uma ocorrência normal, impedindo o tráfego de dados (Correto).

Galera, vocês perceberam que ele é bastante semelhante ao antivírus baseado em assinatura em diversos aspectos? No entanto, eles monitoram uma rede e, não, um computador. Além disso, eles apenas geram alertas, mas não impedem o tráfego de dados. *E o IPS?* **O IPS executa tudo que o IDS executa, mas vai além – ele não só envia um alerta, ele age para impedir o ataque!** *Como?* Fazendo o que for preciso: fechando portas, interrompendo sessões, derrubando pacotes, etc.

(Polícia Federal – 2012) Os sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) utilizam metodologias similares na identificação de ataques, visto que ambos analisam o tráfego de rede em busca de assinaturas ou de conjunto de regras que possibilitem a identificação dos ataques.

_____

Comentários: realmente ambos utilizam metodologias similares no monitoramento e identificação de ataques, analisando o tráfego de rede em busca de assinaturas ou de conjuntos de regras que possibilitem a identificação dos ataques (Correto).

Agora chegamos ao nosso costumeiro desafio! Quero ver se você é bom mesmo... se você entendeu a diferença entre IDS e IPS, envie no **fórum de dúvidas** a explicação do meme abaixo :)

Obs: quando o IDS é usado para fornecer segurança a um dispositivo específico, é chamado de **HIDS (Host IDS)**; quando é para fornecer segurança a uma rede, é chamado de **NIDS (Network IDS)**.

HoneyPot

INCIDÊNCIA EM PROVA: BAIXA

Quem aí assistia O Ursinho Puff? Qualé... eu não sou tão velho assim, alguns de vocês devem ter assistido! *Quem se lembra o que ele mais adorava comer?* **Ele era completamente viciado em mel!** Eu não sei se vocês sabem, mas a caça de ursos é permitida em alguns lugares da América do Norte porque o crescimento populacional dessa espécie tem feito com que eles começassem a ocupar territórios humanos. Como eles praticamente não possuem predadores, sua caça é permitida!

Um dos principais problemas causados pela expansão de território dessa superpopulação de ursos é o furto de comida – sim, eles invadem ou restaurantes e roubam comida! Foi quando alguém teve a seguinte ideia: *e se nós deixássemos um pote de mel exposto como uma isca para atrair os ursos e, então, capturá-los?* **Foi isso que foi feito nesses locais para fazer um controle populacional artificial desses animais.** Vejam no vídeo abaixo como eles amam mel:

HTTPS://WWW.YOUTUBE.COM/WATCH?V=EJF6CGWJD84

Legal, mas o que isso tem a ver com a aula? É simples! **O Honeypot é um mecanismo de segurança que tem a função de propositalmente simular falhas ou vulnerabilidades em um sistema para colher informações sobre um invasor.** Em outras palavras, é uma armadilha para atrair invasores! Ele não oferece nenhum tipo de proteção ou reage contra ataques, podendo eventualmente ser considerado como uma espécie de sistema de detecção de intrusão.

Esse recurso de segurança pode ser utilizado para que o administrador de segurança aprenda sobre os ataques realizados contra sua organização, detectando e armazenando todos os tipos de ataques. *Vocês se lembram que os sistemas de intrusão podem ser baseados em assinaturas ou em comportamentos?* Pois é, o honeypot é uma forma de estudar o comportamento, obter informações sobre as técnicas de ataque mais utilizadas por invasores e armazená-las em bancos de dados.

Foi também a partir das investigações sobre ações criminosas de atacantes que foram criados os sistemas de prevenção de intrusão, que – além de alertar sobre um ataque em potencial – ainda é capaz de preveni-lo. **Em suma, esse recurso de segurança expões vulnerabilidades aos atacantes de forma atraente, enganando-o, fazendo-o pensar que esteja de fato explorando uma falha no sistema de forma a estudar seu comportamento e atrai-lo para longe de sistemas críticos.**

(ABIN – 2018) A detecção de intrusão pode ser realizada por meio do uso de honeypots, técnica que atrai o atacante para um ambiente não crítico, onde há informações falsas e aparentemente valiosas, encorajando-o a permanecer nesse ambiente o tempo suficiente para que os administradores possam registrar e rastrear seu comportamento.

_____

Comentários: essa técnica realmente permite atrair o atacante para um ambiente não crítico, onde há informações falsas e aparentemente valiosas, encorajando-o a permanecer nesse ambiente o tempo suficiente para que os administradores possam registrar e rastrear seu comportamento (Correto).

Eu nunca esqueço de um caso que aconteceu em uma cidade próxima à Brasília em que morador criou uma armadilha automática acionada por uma ratoeira para proteger a sua casa contra os assaltos de um costumeiro ladrão. Pois bem, o ladrão assaltou novamente e caiu na armadilha, que o matou imediatamente! **Trata-se de um mecanismo relativamente similar ao Honeypot, mas lembremos que ele não realiza ações – serve apenas para estudar as técnicas do invasor.**


MENU G1 JORNAL DA GLOBO

Edição do dia 14/07/2011

15/07/2011 00h49 - Atualizado em 15/07/2011 00h57

Morador cria armadilha com pólvora e mata assaltante em Brasília

Assaltante foi surpreendido por armadilha com cartuchos de pólvora e morreu na hora. Dono da casa, José Geraldo de Souza, deve responder processo por homicídio doloso.

HTTPS://WWW.YOUTUBE.COM/WATCH?V=QU_BHI9XEVC

DMZ

INCIDÊNCIA EM PROVA: BAIXA

Galera, nós já vimos que um firewall nem sempre é imune a ataques internos em uma rede de computadores! *Vocês se lembram o porquê?* **Porque o firewall é basicamente um muro, logo o que ele vai proteger vai depender de onde ele está posicionado!** Por exemplo: *é possível ter uma casa sem muro?* Sim! Em Brasília, há um bairro chamado Lago Sul em que grande parte das casas não possui nenhum muro.

No entanto, há um outro bairro aqui em que existem basicamente apenas condomínios. Todos esses condomínios possuem um muro ao redor, por vezes com câmeras de segurança, escolta armada, controle de acesso por identificação. **Diante de tantos recursos de segurança, alguns moradores não colocam muros em suas casas porque o próprio condomínio já oferece a segurança que ele considera suficiente.**

Agora voltando à nossa pergunta inicial: *um firewall protege contra ataques externos?* **Sim, ele protege uma rede interna de ataques provenientes da internet, da mesma forma que o muro do condomínio protege seus moradores de assaltantes e outros criminosos externos.** Só tem um detalhe: há condomínios nesse bairro que eu mencionei em que moram quase dez mil pessoas! *Ora, você realmente está protegido de ataques externos, mas está protegido de ataques internos?* Não!

Você ainda está vulnerável a algum vizinho que não vai com a sua cara ou com algum vizinho que seja basicamente um criminoso. *Por que?* **Porque o condomínio possui um muro de proteção que o protege de ataques externos, mas a sua casa não possui um muro de proteção que o protege de ataques internos.** *Viram agora que o firewall é apenas uma barreira de proteção, mas o que ele vai proteger dependerá de onde ele está posicionado?*

A solução encontrada por muitos moradores é construir um muro ao redor de casa além do muro ao redor do condomínio. Dessa forma, eles estarão protegidos de ataques externos e internos. De modo semelhante, a solução encontrada pelos cientistas da computação foi utilizar dois firewalls: um posicionado na fronteira entre a rede interna de uma organização e a internet – chamado **Firewall de Borda**; e outro posicionado dentro da rede interna – chamado **Firewall de Perímetro**[2].

Claro que se você encher a sua rede de firewalls, isso pode comprometer o desempenho da rede! *Sabe quando você vai a um show e é revistado pelo segurança?* É como se cada firewall fosse um segurança. Pois bem... a área entre o Firewall de Borda e o Firewall de Perímetro é conhecida como **Zona Desmilitarizada (DMZ)** – trata-se de uma área em que a segurança é bem mais tranquila, em contraste com a área dentro do perímetro, que é como se fosse uma área de segurança máxima.

[2] Em geral, é um Filtro de Pacotes ou um Proxy.

Galera, eu tenho um amigo que coleciona *Action Figures* (aqueles bonecos de personagens de filmes e desenhos). *Qualquer pessoa pode brincar com eles?* Não, apenas ele e os filhos! *E os filhos podem brincar com todos?* Não, apenas com os mais baratos! **Os mais caros custam uma fortuna (mais de R$5.000,00!!!!!!!!!!) e ele os deixa protegidos por uma redoma de vidro de modo que apenas ele tenha acesso.** *O que podemos concluir disso?*




A primeira conclusão é que ele é maluco de gastar tanto dinheiro assim com bonecos; a segunda é que todos os bonecos estão protegidos pelo muro de sua casa; e que os bonecos mais caros estão superprotegidos até mesmo de alguns moradores de sua casa. **Chama-se zona desmilitarizada porque nessa área a proteção é mais branda, isto é, seus filhos podem brincar à vontade; mas dentro dessa área, nós temos uma espécie de área de segurança máxima.** *Entendido?*

CURIOSIDADE

DMZ *(**De**Militarized **Z**one) é a sigla para Zona Desmilitarizada! Em termos miliares, trata-se de uma área, habitualmente a fronteira entre duas ou mais potências ou alianças militares, onde a atividade militar não é permitida devido – em geral – a um tratado de paz, um armistício ou outro acordo bilateral ou multilateral. Por exemplo: vocês sabiam que existe uma DMZ entre a Coréia do Norte e a Coréia do Sul com 250km de extensão conforme podemos visualizar na imagem apresentado ao lado.*

Bem, vamos trazer isso agora para o contexto de uma empresa ou órgão. Imaginem que um órgão possua uma intranet, isto é, uma rede interna/privada. *O que é isso mesmo, Diego?* **É uma rede corporativa – privada, restrita e exclusiva a um público específico – que se utiliza de tecnologias, padrões e serviços comuns à internet com o intuito de compartilhar informações e recursos computacionais, além de melhorar a comunicação interna entre membros de uma organização.**

Galera, o mundo pós-pandemia abriu a cabeça dos gestores tanto no serviço público quanto na iniciativa privada para o teletrabalho, logo se tornou muito comum que funcionários acessassem a intranet de suas organizações a partir de suas casas por meio da Internet. Esses funcionários – em

geral – precisam acessar serviços! *E onde eles estão localizados?* **Em diversos servidores (máquinas especializadas em prover algum serviço) geralmente localizados na rede interna/local do órgão.**

Professor, não entendi essa parte aí não! Galera, o que vocês precisam saber é que cada serviço precisa de um servidor específico! **O site da organização fica hospedado no Servidor Web; o serviço de e-mail fica hospedado no Servidor de E-Mail; o serviço de transferência de arquivos fica hospedado no Servidor FTP; e assim por diante.** Agora vamos utilizar como exemplo o Tribunal de Contas da União (TCU).

Esse órgão disponibiliza diversos serviços, como podemos visualizar na imagem seguinte retirada do seu portal. Como eles são serviços, devem ser disponibilizados por meio de algum servidor! E todos esses servidores estão localizados na rede privada desse órgão. Agora vejam que interessante: **alguns serviços são públicos e podem ser acessados por qualquer cidadão que deseje acessá-lo, mas outros serviços estão disponíveis apenas para os funcionários do órgão.**

Na imagem acima, nós podemos ver que há um serviço em que um cidadão pode pegar emprestado um livro da biblioteca do TCU. No entanto, há diversos outros serviços – relacionados à função de um tribunal de contas – que somente os funcionários desse órgão conseguirão acessar (Ex: sistema de controle de auditoria; sistema de julgamento de contas; sistema de controle de jurisprudências; sistema de folha de pagamento; serviço de e-mail; bancos de dados, entre outros).

Todos esses serviços são disponibilizados na rede privada do órgão! *Sabe outra coisa que nós temos nessa rede?* Os próprios computadores dos funcionários! Uma rede conecta diversos dispositivos, tanto servidores quanto estações de trabalho. *Onde você quer chegar, professor?* Eu quero que vocês entendam o seguinte: **dentro de uma mesma rede, nós temos alguns serviços que estão disponíveis externamente e outros serviços que não estão disponíveis externamente.**

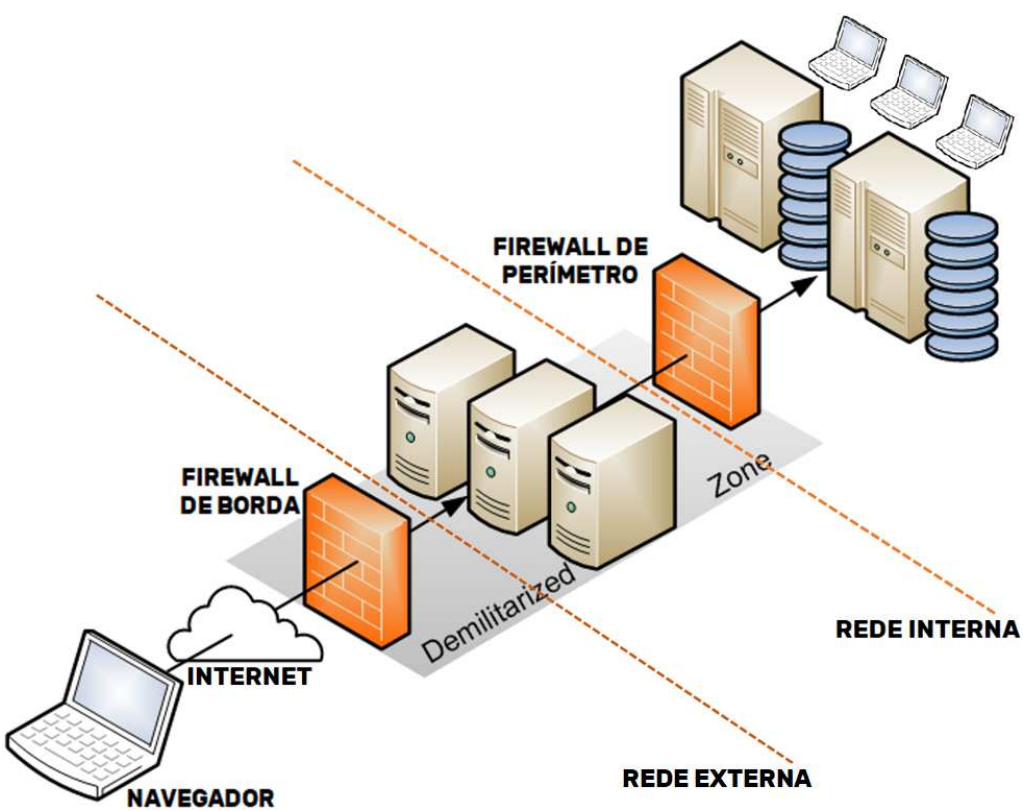
Além disso, alguns desses serviços que não estão disponíveis externamente podem ser bastante críticos e conter dados confidenciais, que não podem ser acessados pelo cidadão

comum. Dito isso, nós temos três alternativas: (1) não disponibilizar nenhum serviço externamente, porém ninguém conseguirá pegar um livro emprestado, pegar uma certidão negativa, verificar a agenda oficial de um ministro e, até mesmo, acessar a própria página do órgão.

(2) disponibilizar todos os serviços externamente, porém existe aplicações que são extremamente críticas e o que não falta no mundo são hackers habilidosos que conseguem encontrar falhas e vulnerabilidades que permitam seu acesso à rede; **(3) disponibilizar externamente aqueles serviços que podem ser acessados por cidadãos comuns e disponibilizar internamente aqueles serviços que podem ser acessados por funcionários do órgão.** *E como podemos fazer isso?*

Bem, uma sugestão seria termos um segmento de rede de computadores apenas para as aplicações que necessitam de mais segurança e outra região para as aplicações que devem ficar expostas na internet. **Dessa forma, se um hacker conseguir atravessar o Firewall de Borda, ele terá acesso apenas às aplicações da rede desmilitarizada, mas não àquelas que estão dentro da rede interna/local da organização.** *Qual o nome desse segmento de rede?* DMZ!

A DMZ é utilizada para disponibilizar serviços externamente! Na imagem a seguir, é possível visualizar a configuração padrão[3] de uma zona desmilitarizada:



Observem que a zona desmilitarizada – também chamada de rede de perímetro – é a forma mais clássica de segmentação de uma rede com objetivos de segurança. **Ela adiciona uma camada extra**

[3] Existe também uma configuração que permite utilizar apenas um firewall, no entanto não veremos essa configuração alternativa porque ela é mais rara em provas e mais insegura na prática.

de segurança para as redes corporativas, visto que – quando um atacante externo inicia uma tentativa de invasão – esta será direcionada para os recursos publicados na zona desmilitarizada em vez de diretamente atacar os recursos da rede local.

A DMZ é o segmento de rede que contém os servidores – também chamados de Bastion Hosts – que oferecerão os serviços tanto para usuários internos quanto para usuários externos (Ex: Servidor HTTP, Servidor FTP, Servidor SMTP, Servidor DNS, etc). **Por causa do alto risco potencial destes servidores serem comprometidos, eles são colocados em uma rede separada para que, caso um intruso seja bem-sucedido, este ataque não afete os servidores internos da rede.** Em suma:

ZONA DESMILITARIZADA (DMZ)	Trata-se de uma sub-rede física ou lógica – também chamada de rede de perímetro – utilizada para transmitir informações entre uma rede confiável e uma não confiável, mantendo os serviços que possuem acesso externo separados da rede interna/local.

(TRE/CE – 2012) Sobre DMZ é INCORRETO afirmar:

a) O desenho e implementação de uma DMZ estão intimamente ligados à utilização de sistemas de firewall.

b) Caso um invasor consiga ter acesso à DMZ por conta de uma vulnerabilidade de algum serviço, ele normalmente permanece sem acesso à rede interna, uma vez que um firewall pode estar configurado para proteger a rede interna.

c) A implementação padrão de DMZ utiliza normalmente dois firewalls, um separando a rede WAN da DMZ e outro separando a DMZ da rede interna.

d) Uma DMZ separa os serviços e os usuários da rede interna de um possível ataque vindo de uma rede insegura, como a Internet.

e) É recomendável colocar serviços como Exchange, DNS interno ou servidores de aplicativos que necessitam acessar um banco de dados e transitar informações sensíveis dentro da DMZ.

Comentários: essa é uma excelente questão para treinar tudo que nós aprendemos – (a) Correto, nós vimos que a implementação de uma zona desmilitarizada está intimamente ligada à utilização de sistemas de firewall; (b) Correto, é exatamente o que nós vimos insistentemente na aula – o invasor pode conseguir acessar a zona desmilitarizada, no entanto ele tem o firewall de perímetro que impede que ele acesse a rede interna; (c) Correto, em geral utiliza dois firewalls – um separa da Rede WAN (Internet) da DMZ e o outro separa a DMZ da rede interna; (d) Correto, a zona desmilitarizada realmente separa os serviços e os usuários da rede interna de um possível ataque vindo da rede externa como a internet; (e) Errado, independente do tipo de servidor tipicamente inserido na zona desmilitarizada, eles não podem transitar informações sensíveis – tudo que trafega informações sensíveis devem estar dentro da rede interna protegido pelo firewall de perímetro (Letra E).

UTM/NGFW

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Por fim, vamos falar rapidamente sobre alguns conceitos que muuuito raramente caem em prova: Unified Threat Management (UTM) e Next Generation Firewall (NGFW). **O UTM – em tradução livre: Gerenciamento Unificado de Ameaçadas – é uma abordagem de segurança da informação recomendada para pequenas e médias organizações em que um único sistema (hardware e/ou software) fornece múltiplas funções de segurança.** *Quais, Diego?*

O UTM deve integrar – ao menos – Firewall, IDS e IPS. No entanto, ele pode integrar também outras soluções como Antivírus, Antispam, Antispyware, VPN, NAT, etc. De acordo com a Kaspersky, o fascínio dessa solução baseia-se na simplicidade: organizações que têm fornecedores ou dispositivos para cada tarefa de segurança podem agora tê-los todos sob o controle do mesmo fornecedor, com o suporte de uma mesma equipe de TI e executados através de um console.

Outra grande vantagem é a melhoria de desempenho: como todas as soluções estão integradas, existe uma baixa latência (tempo em que dados levam de um ponto a outro) – permitindo que potenciais ameaças sejam identificadas com maior rapidez. *E desvantagens, professor?* **Notem que o UTM é um ponto único de falha, isto é, caso o sistema seja comprometido, todas as soluções de segurança serão comprometidas de uma só vez e a rede poderá ficar vulnerável.**

Já o NGFW ainda é muito pouco documentado em bibliografias consagradas, então vamos nos basear no Glossário do Gartner. **Trata-se de uma nova geração de firewall que utiliza o conceito de Deep Packet Inspection (DPI), que permite uma inspeção profunda na carga útil dos pacotes de dados que vão além da inspeção e bloqueio via porta/protocolo para adicionar uma inspeção em nível de camada de aplicação – esse conceito também existe no UTM!**

O NGFW também concentra em uma única ferramenta diversos mecanismos de proteção e segurança como IPS, IDS, Firewall, Filtro Web, Antispam, Antimalware[4], etc – trazendo uma inteligência externa aos firewalls. Como esse assunto ainda é muito recente, é possível encontrar muitas divergências em diversas fontes e também nas poucas questões que existem sobre esse tema, mas é o que temos para hoje...

> **(Polícia Federal – 2018)** Para a melhoria de desempenho, vários produtos de segurança (firewall e antispyware, por exemplo) podem ser substituídos por um sistema de gerenciamento unificado de ameaça (UTM – Unified Threat Management).
>
> _____
>
> **Comentários:** ele realmente ajuda a melhorar o desempenho, substituindo de forma unificada e integrada diversas soluções de segurança (Correto).

[4] Antimalware é polêmico – algumas fontes dizem que faz parte e outras, não.

(PRF – 2021) O firewall da próxima geração (NGFW) dispõe, em um mesmo equipamento, de recursos como IDS (Intrusion Detection System), IPS (Intrusion Prevention System) e antivírus.

_____

Comentários: ela realmente dispõe de vários recursos de segurança, mas antivírus/antimalware é polêmico (Anulada).

(BANRISUL – 2018) Sobre tecnologias de firewalls, considere as afirmações abaixo.

I - A Firewall de Nova Geração (NGFW) é assim chamada por concentrar todas as soluções de firewall em um único hardware (antivírus, proxy web, proteção contra malwares, etc.).

II - Em uma NGFW, é possível analisar se um download que está em andamento contém algum tipo de ameaça, como ransomware ou outro malware qualquer.

III - Firewalls do tipo Unified Threat Management (UTM) são o produto geralmente recomendado para grandes empresas. Quais estão corretas?

a) Apenas I.
b) Apenas II.
c) Apenas III.
d) Apenas I e II.
e) I, II e III.

_____

Comentários: (I) Errado, no entanto eu discordo do gabarito da banca – não vejo nenhum erro nessa questão; (II) Correto, ele permite analisar profundamente pacotes de downloads em andamento para detectar malwares; (III) Errado, ele é recomendado para pequenas e médias empresas. Meu gabarito seria Letra D! (Letra B).

Hardening

INCIDÊNCIA EM PROVA: BAIXA

Hardening (Endurecimento) é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e com o objetivo principal de torná-la preparada para enfrentar tentativas de ataque. De acordo com André Luiz Facina, trata-se de uma técnica usada para mapear ameaças e depois executar possíveis correções nos sistemas, preparando-os para determinadas tentativas de ataques ou violação na segurança da informação.

DEFINIÇÕES DE HARDENING
Trata-se de ajustes finos efetuados no sistema após uma instalação.
Trata-se de medidas e ações que visam proteger um determinado sistema de invasores.
Trata-se de um processo de proteger um sistema contra ameaças desconhecidas. Os administradores de sistema devem endurecer uma instalação contra o que eles acham que pode ser uma ameaça.
Trata-se de uma melhoria de segurança, ativando controles nativos ou implementando-os.
Trata-se do processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

Normalmente, o processo inclui remover ou desabilitar nomes ou logins de usuários que não estejam mais em uso, além de serviços desnecessários; limitar o software instalado àquele que se destina a função desejada do sistema; aplicar e manter patches atualizados – tanto de sistema operacional quanto de aplicações; revisar e modificar as permissões dos sistemas de arquivos – em especial de escrita/execução; reforçar a segurança do login, impondo uma política de senhas fortes.

Em outras palavras, o hardening consiste em fazer a remoção dos meios de acesso e parâmetros desatualizados, inutilizados e desnecessários que permitam o acesso de fora para dentro e de dentro para fora, reduzindo assim as chances de ataques bem sucedidos. **Com essa técnica, é possível remover completamente o acesso de usuários não autorizados, bem como a inserção de scripts maliciosos nos servidores da rede.**

Também pode ser feito o bloqueio do login, logout de usuários inativos há muito tempo, remoção de permissões, etc. Dessa forma, brechas de segurança e vulnerabilidades são descobertas, fazendo com que a empresa consiga não somente administrar melhor, mas também fazer mudanças necessárias em sua estrutura (Ex: se for notado que os softwares utilizados estão muito desatualizados, a organização pode imediatamente investir nesse setor e resolver o problema).

E como implementar o Hardening? Bem... um processo de proteção do sistema deve estar em vigor para todos os dispositivos conectados a uma rede. Isso inclui estações de trabalho, servidores, dispositivos de rede, impressoras, entre outros. Se a sua organização não possui atualmente um

processo de proteção do sistema, abaixo estão algumas recomendações gerais sobre o que deve incluir um forte processo de proteção do sistema.

RECOMENDAÇÕES DE HARDENING
Renomear ou desativar contas internas.
Determinar protocolos necessários.
Proteger os sistemas básicos de entrada / saída ("BIOS").
Identificar e remover aplicativos e serviços desnecessários.
Documentar o processo de proteção do sistema.

(TCE/PA – 2016) A técnica hardening é utilizada para mapear ameaças e executar, em nível lógico, possíveis correções nos sistemas, preparando-os para impedir tentativas de ataques ou de violação da segurança da informação.

_____

Comentários: não há como impedir tentativas, ela é utilizada para reagir a tentativas de ataque ou violação (Errado).

(CGU – 2012) É um mecanismo de Hardening do Servidor Linux:

a) minimizar software instalado.
b) instalar apenas softwares padronizados internacionalmente.
c) instalar versões antigas do sistema operacional e fazer logo em seguida o upgrade do sistema.
d) não fazer upgrades frequentes, o que pode comprometer a segurança do sistema.
e) manter instalados todos os serviços, mesmo os que sejam aparentemente desnecessários.

_____

Comentários: (a) Correto, quanto menos softwares instalados e mais softwares em nuvem, por exemplo, maior a proteção; (b) Errado, padronização internacional não é garantia de proteção; (c) Errado, o ideal é instalar o que há de mais atualizado; (d) Errado, upgrades devem ocorrer com frequência para ajudar na segurança dos sistemas; (e) Errado, serviços desnecessários devem ser desabilitados (Letra A).

(TCE/PA – 2012) Em segurança da informação, entende-se por Hardening:

a) as medidas e ações que visam proteger um sistema de invasores.
b) um software para a detecção de invasão a servidores de redes.
c) os processos para a auditoria de segurança de servidores.
d) a tolerância a falhas e o bom desempenho de sistemas.
e) os controles implantados no tráfego das redes.

_____

Comentários: (a) Correto; (b) Errado, isso seria um IDS (Intrusion Detection System); (c) Errado, não há nenhuma relação com hardening; (d) Errado, não há nenhuma relação com hardening; (e) Errado, não há nenhuma relação com hardening (Letra A).

(TCE/PA – 2012) O Hardening possui algumas ações típicas, uma delas é a:

a) configuração de memória e espaço em disco dos servidores de aplicação e banco de dados.
b) aplicação de patches nos programas e no kernel do sistema operacional.
c) instalação e configuração de servidores de redes com fontes redundantes.
d) criação de logins para usuários autenticados no sistema operacional.
e) definição dos perfis de usuários para o acesso à rede da organização.

Comentários: (a) Errado, isso não tem nenhuma relação com hardening; (b) Correto, patches são pacotes com atualizações ou correções de um software com o intuito de melhorar sua usabilidade, segurança ou performance; (c) Errado, isso não tem nenhuma relação com hardening; (d) Errado, a desativação de logins não utilizados é um exemplo de hardening – sua criação, não; (e) Errado, isso não tem nenhuma relação com hardening (Letra B).

(TCE/PA – 2016) Hardening é um processo de alteração na infraestrutura física dos recursos dos computadores em rede cujo objetivo principal consiste em preparar a infraestrutura para enfrentar erros. Esse processo inclui habilitar o acesso de todos os usuários aos recursos de todos os servidores, de forma a garantir que qualquer recurso de hardware esteja disponível aos usuários existentes.

Comentários: a ideia é reduzir ao máximo a superfície de vulnerabilidade, logo esse processo inclui habilitar o acesso de usuários específicos a recursos específicos e, não, habilitar todos os usuários a todos os recursos (Errado).

(BACEN – 2013) Entre as ações que integram o processo de hardening incluem-se desinstalar softwares desnecessários para o cotidiano do usuário na estação de trabalho e instalar antispyware.

Comentários: perfeito... ao desinstalar softwares desnecessários, reduz-se a superfície de vulnerabilidade (Correto).

(ANTAQ – 2014) Entre as atividades corretivas definidas para a hardening, técnica utilizada para tornar o sistema completamente seguro, destaca-se a de manter atualizados tanto os softwares do sistema operacional quanto os das aplicações.

Comentários: não é para tornar o completamente seguro e as atividades são preventivas (Errado).

(TCU – 2007) Algumas providências que um processo de hardening deve incluir são: limitar o software instalado àquele que se destina à função desejada do sistema; aplicar e manter os patches atualizados, tanto de sistema operacional quanto de aplicações; revisar e modificar as permissões dos sistemas de arquivos, em especial no que diz respeito a escrita e execução; reforçar a segurança do login, impondo uma política de senhas fortes; habilitar apenas os serviços necessários.

Comentários: perfeito, perfeito, perfeito – tudo impecável (Correto).

(IBGE – 2019) Atualização do sistema operacional e instalação de patches de segurança, remoção de serviços desnecessários e contas de usuário não utilizadas, instalação de controles de segurança adicionais e testes de segurança são medidas para reforçar a segurança de um computador. O conjunto desses procedimentos é conhecido como:

a) hardening.
b) varredura.
c) análise de vulnerabilidades.
d) privilégio mínimo.
e) pentest.

Comentários: esse conjunto de procedimentos de segurança é chamado de hardening (Letra A).

Controles de Dispositivos USB

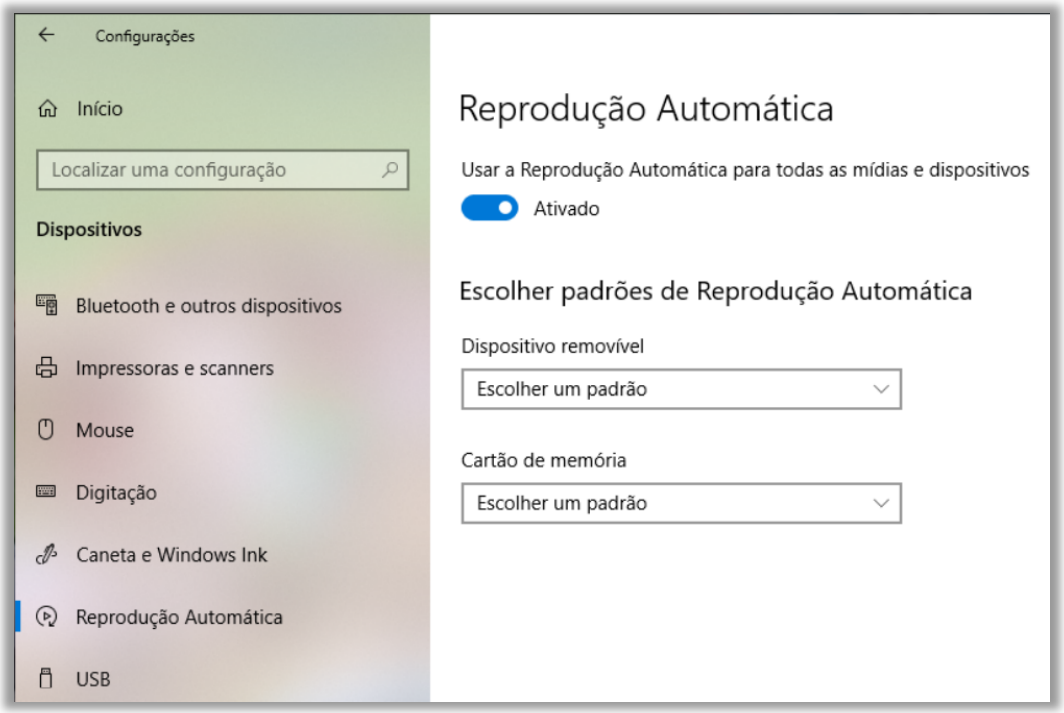
A grande vantagem de dispositivos USB é que, por se comportarem como uma partição do computador, eles permitem que você os use da maneira que bem entender, transferindo dados e executando aplicativos. **O problema é que isso nem sempre é vantajoso: é possível instalar softwares maliciosos (malwares) no dispositivo, danificando o sistema em que ele se conectar enquanto informações importantes podem ser roubadas com extrema facilidade.**

Logo, embora inofensivos à primeira vista, esses dispositivos são uma das principais causas de incidentes de segurança que podem causar grandes danos a computadores de pessoas físicas ou de organizações. **Os danos variam de dados confidenciais sendo roubados a grandes multas devido a violações das regras e regulamentos de conformidade.** Dito isso, é importante – em determinadas ocasiões – controlar os dispositivos conectados.

Algumas recomendações comuns são: (1) defina políticas de segurança e monitores portas e dispositivos USB em todos os terminais; (2) identifique todos os dispositivos conectados via USB; (3) bloqueie o uso não autorizado de dispositivos e imponha, se possível, a criptografia dos dados; (4) obtenha relatórios e alertas sobre atividades de dispositivos USB sobre os terminais. A tabela seguinte apresenta algumas maneiras de permitir ou bloquear dispositivos removíveis:

CONTROLE	DESCRIÇÃO
RESTRINGIR UNIDADES USB E OUTROS PERIFÉRICOS	Você pode permitir/impedir que os usuários instalem apenas as unidades USB e outros periféricos incluídos em uma lista de dispositivos autorizados/não autorizados ou tipos de dispositivos.
BLOQUEAR A INSTALAÇÃO E O USO DO ARMAZENAMENTO REMOVÍVEL	Não é possível instalar ou usar armazenamento removível.
PERMITIR A INSTALAÇÃO E O USO DE PERIFÉRICOS ESPECIFICAMENTE APROVADOS	Você só pode instalar e usar periféricos aprovados que relatam propriedades específicas em seu firmware.
IMPEDIR A INSTALAÇÃO DE PERIFÉRICOS ESPECIFICAMENTE PROIBIDOS	Não é possível instalar ou usar periféricos proibidos que relatam propriedades específicas em seu firmware.
PERMITIR A INSTALAÇÃO E O USO DE PERIFÉRICOS ESPECIFICAMENTE APROVADOS COM IDS DE INSTÂNCIA DE DISPOSITIVO CORRESPONDENTES	Você só pode instalar e usar periféricos aprovados que corresponderem a qualquer uma dessas IDs de instância de dispositivo.

No Windows 10, é possível realizar algumas configurações de reprodução automática de dispositivos removíveis em: **Configurações** > **Dispositivos** > **Reprodução Automática**.


Configurações
Início
Localizar uma configuração
Dispositivos
Bluetooth e outros dispositivos
Impressoras e scanners
Mouse
Digitação
Caneta e Windows Ink
Reprodução Automática
USB
Reprodução Automática
Usar a Reprodução Automática para todas as mídias e dispositivos
Ativado
Escolher padrões de Reprodução Automática
Dispositivo removível
Escolher um padrão
Cartão de memória
Escolher um padrão

MAPA MENTAL

Segurança da Informação

Mecanismos Avançados

IDS/IPS

- Monitoram a rede inspecionando profundamente cada pacote.
- Intrusion Detection System.
  = Sistema de Detecção de Intrusão.
  Dispositivo passivo (não reage!).

- Intrusion Prevention System.
  = Sistema de Prevenção de Intrusão.
  Dispositivo reativo ou proativo (esse reage!).

Atenção!

- IDS e IPS analisam o tráfego de rede em busca de assinaturas ou de um conjunto de regras que possibilitem a identificação dos ataques.
- IDS = só detecta e alerta. Não reage!
- IPS = detecta e bloqueia. Reage!

- OBS: antivírus baseado em assinatura monitora um computador. IDS e IPS monitoram a rede!
- Desvantagens dos IDS e dos IPS baseados em assinatura:
  - São cegos para novos ataques.
  - Podem apresentar muitos falsos-positivos.
    - A consequência é pior no IPS (ele bloqueia).

UTM

- Unified Threat Management.
  = Gerenciamento Unificado de Ameaças.
- Um único sistema que fornece múltiplas funções de segurança.
  Pelo menos Firewall, IDS e IPS.
- Vantagem: potenciais ameaças são identificadas com + rapidez).
- Desvantagem: o UTM é um ponto único de falha.

Honeypot

= armadilha p/ atrair invasores.

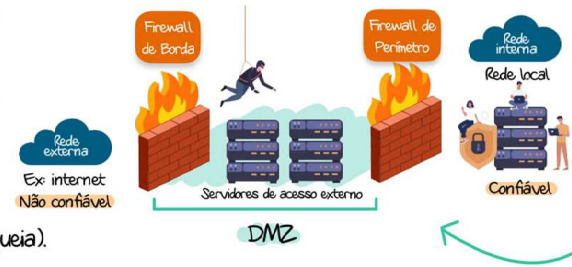
- Ferramenta que simula falhas de segurança em um sistema p/ atrair invasores e colher informações sobre os ataques.

- Não realiza ações!
- O invasor é atraído p/ um sistema não crítico (geralmente isolado e monitorado) e incentivado a ficar nele por tempo suficiente p/ que haja uma monitoração pelos administradores.

DMZ

= Zona Desmilitarizada (ou rede de perímetro).

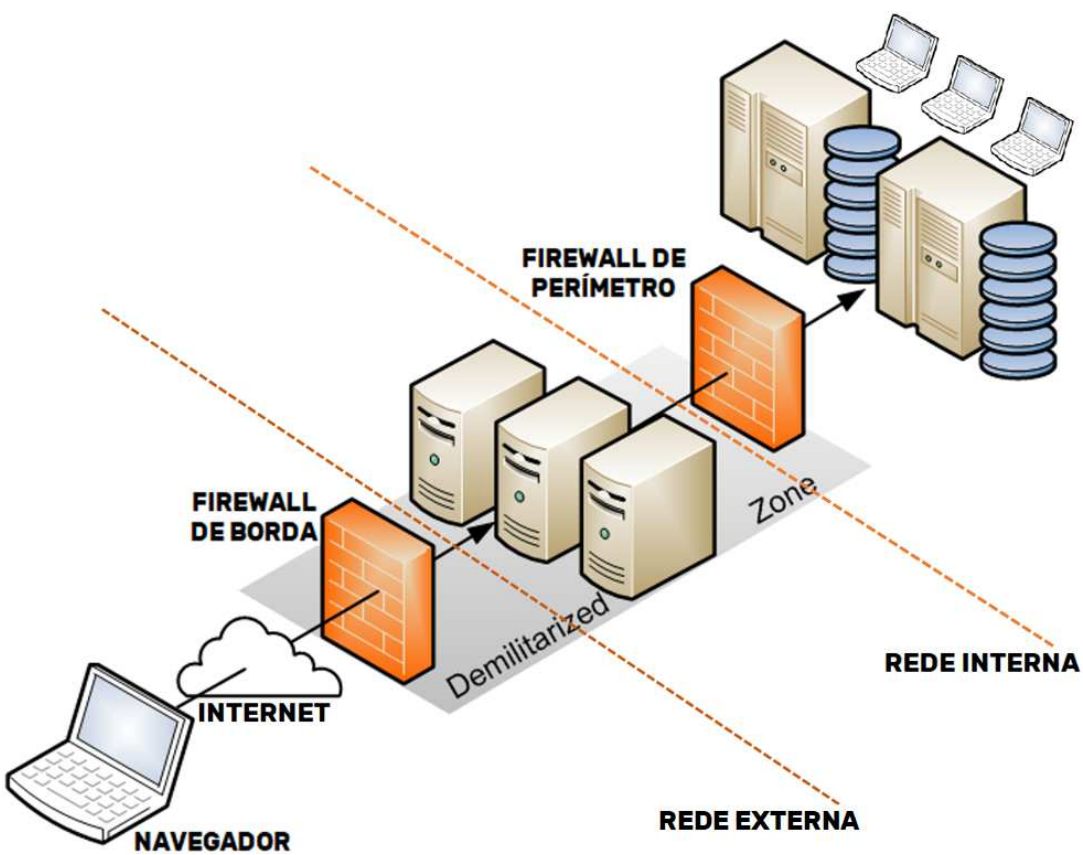
- Sub-rede (segmento de rede) física ou lógica entre o Firewall de Borda e o Firewall de Perímetro em que a proteção é mais branda.
- Nela ficam os servidores de acesso externo da organização.
- Utilizada p/ transmitir informações entre uma rede confiável e uma não confiável.
- Mantém os serviços que possuem acesso externo separados da rede local (interna).
  - O invasor pode conseguir acessar a DMZ, mas haverá o Firewall de Perímetro p/ impedir seu acesso à rede interna.



@mapasdathai

RESUMO

IDS (INTRUSION DETECTION SYSTEM)	Em português, Sistema de Detecção de Intrusão – trata-se de um dispositivo passivo que monitora a rede, detecta e alerta quando observa tráfegos potencialmente mal-intencionados, mas não o bloqueia
IPS (INTRUSION PREVENTION SYTEM)	Em português, Sistema de Prevenção de Intrusão – trata-se de um dispositivo reativo ou proativo que monitora a rede, detecta e bloqueia quando observa tráfegos potencialmente mal intencionados.
HONEYPOT	Trata-se de um mecanismo de segurança que tem a função de propositalmente simular falhas ou vulnerabilidades em um sistema para colher informações sobre um invasor. Em outras palavras, é uma armadilha para atrair invasores! Ele não oferece proteção ou reage contra ataques, podendo eventualmente ser considerado como uma espécie de sistema de detecção de intrusão.
ZONA DESMILITARIZADA (DMZ)	Trata-se de uma sub-rede física ou lógica – também chamada de rede de perímetro – utilizada para transmitir informações entre uma rede confiável e uma não confiável, mantendo os serviços que possuem acesso externo separados da rede interna/local.



QUESTÕES COMENTADAS – CESPE

1. **(CESPE / DPDF - 2022)** Um IDS (Intrusion Detection System), quando disponibilizado para oferecer detecção somente no servidor da rede onde ele está instalado, é denominado NIDS (Network Intrusion Detection System).

Comentários:

Quando o IDS é utilizado para fornecer segurança em apenas um dispositivo específico, trata-se de um Host IDS (HIDS). Quando a função do IDS é fornecer segurança para uma rede, trata-se do Network IDS (NIDS).

Gabarito: Errado

---

2. **(CESPE / DPDF - 2022)** O registro de logs e a desinstalação de software desnecessário para o funcionamento do servidor são considerados ações do processo de hardening do sistema operacional.

Comentários:

Hardening, no contexto de computação, é o processo de proteger um sistema contra ataques. Dessa forma, o registro de logs e a desinstalação de softwares desnecessários são atividades que dificultam o comprometimento de um sistema operacional.

Gabarito: Correto

---

3. **(CESPE / TELEBRÁS - 2021)** Em uma organização, será considerado como um sistema de prevenção de intrusão baseado em hospedeiro um aplicativo que, instalado em uma das máquinas da infraestrutura de rede, capture pacotes nessa rede, compare esses pacotes com uma base de assinaturas (padrões de ataques específicos), gere eventos que possam ser ações ou alertas e envie esses eventos para o próprio administrador.

Comentários:

Pessoal, a questão trata de um IPS baseado em hospedeiro (HIPS). Esses sistemas funcionam integrados ao kernel do host, ou seja, eles têm acesso ao sistema operacional. Em suma, todas as chamadas passam pelo HIPS antes de serem executadas. Além disso, eles identificam comportamentos suspeitos no sistema, ao invés de comparar assinaturas.

Gabarito: Errado

---

4. **(CESPE / TELEBRÁS - 2021)** Capaz de analisar qual a parcela de risco de uma intrusão e bloqueá-la antes que ela ocorra, um IPS permite criar regras com o objetivo de monitorar aumentos anormais de tráfego de rede; além dessa funcionalidade, ele ainda pode alertar o responsável pela segurança, caso ocorram tais anomalias.

Comentários:

É o IDS que alerta o administrador da rede, caso ocorram anomalias, entretanto, isso – por si só – não torna a questão errada. Um IPS pode executar tudo que um IDS executa, ou seja, ele pode não só agir para evitar o ataque, como pode também enviar alertas para o administrador da rede.

Gabarito: Correto

---

5. **(CESPE / CODEVASF – 2021)** Um dispositivo configurado como IPS (Intrusion Prevention System) analisa tráfegos na rede de computadores, em busca de assinaturas de ataques, e notifica os administradores, porém não possui autonomia para bloquear o tráfego de rede.

Comentários:

IPS realmente analisa tráfego em uma rede de computadores em busca de uma assinatura de ataque que corresponda àquelas armazenadas em seu banco de dados e notifica os administradores da rede – eles podem, sim, bloquear o tráfego de forma autônoma, visto que são proativos. Lembrem-se que IPS é um dispositivo reativo ou proativo que monitora a rede, detecta e bloqueia quando observa tráfegos potencialmente mal intencionados.

Gabarito: Errado

---

6. **(CESPE / Polícia Federal – 2021)** Caso o usuário tenha recebido um conjunto de arquivos com *trojan* em seu conteúdo e esses arquivos estejam em uma mídia de armazenamento local em sua estação de trabalho, recomenda-se a utilização de IDS (*intrusion detection system*) para a realização da limpeza dos arquivos.

Comentários:

Um IDS (Intrusion Detection System) tem a função de monitorar uma rede ou sistema em busca de atividades maliciosas – ele nada poderá fazer para limpar os arquivos infectados.

Gabarito: Errado

---

7. **(CESPE / PRF – 2021)** O firewall da próxima geração (NGFW) dispõe, em um mesmo equipamento, de recursos como IDS (Intrusion Detection System), IPS (Intrusion Prevention System) e antivírus.

Comentários:

sabem quantas vezes já caiu NGFW em provas anteriores? Duas! E pior: esse é um tipo de firewall pouquíssimo documentado em bibliografias consagradas, logo nós temos que nos basear no que existe de informação na internet. NGFW é uma tecnologia extremamente parecida com UTM (Unified Threat Management) no sentido que de congrega em uma única ferramenta diversos mecanismos de proteção e segurança. Ele se baseia no conceito de Deep Packet Inspection (DPI), que permite inspecionar a carga útil dos pacotes de dados até a camada de aplicação.

Na prática, ambas as tecnologias são idênticas – elas reúnem recursos como IPS, IDS, Firewall, Filtro Web, Antispam, Antimalware, etc. O lance é que há fontes que afirmam que NGFW oferece recursos de antimalware/antivírus e há fontes que afirmam o contrário. Como não temos uma bibliografia consagrada para consultar, adivinhem só: o que a banca afirmar virará nossa jurisprudência daqui em diante.

Sendo bem honesto: eu acho que erraria essa questão na hora da prova. Por que? Porque eu acho que antimalware/antivírus faz parte do NGFW, mas eu acredito que o gabarito preliminar da banca poderá vir como errado. Veremos assim que sair, mas pode ter certeza que vai chover recursos independente do gabarito.

Gabarito: Correto

---

8. **(CESPE / TJ-AM – 2019)** Uma desvantagem de utilizar um IDS para proteger a rede contra ataques externos é que ele não pode ser configurado para realizar a atualização automática de suas definições de assinatura, pois a atualização é um procedimento cauteloso que deve ocorrer sob a supervisão do administrador de rede.

Comentários:

É claro que ele pode ser configurado para realizar a atualização automática de suas definições de assinatura – não é necessária nenhuma supervisão do administrador da rede.

Gabarito: Errado

---

9. **(CESPE / TJ-AM – 2019)** Um IDS permite criar regras com o objetivo de monitorar aumentos anormais de tráfego de rede; além dessa funcionalidade, ele ainda pode alertar o responsável pela segurança, caso ocorram tais anomalias.

Comentários:

Perfeito! IDS tem o objetivo de monitorar a rede, detectar e alertar quando observa tráfegos potencialmente mal-intencionados, mas não os bloqueia – apenas alerta o administrador da rede.

Gabarito: Correto

---

10. (CESPE / EMAP- 2018) O dispositivo de IPS (do inglês Intrusion Prevention System) utilizado em redes corporativas tem como objetivo bloquear ataques a partir da identificação de assinaturas e(ou) anomalias.

Comentários:

Perfeito, perfeito, perfeito! Ele realmente bloqueia ataques e pode ser baseado em identificação de assinatura e/ou anomalias.

Gabarito: Correto

---

11. (CESPE / ABIN – 2018) Os honeypots (potes de mel), enquanto tecnologia de detecção de intrusão, podem ser utilizados para atingir os objetivos de atrair um atacante potencial e afastá-lo de sistemas críticos e de incentivar o atacante a ficar no sistema por período de tempo suficiente para que haja resposta dos administradores, mas não para coletar informações sobre a atividade do atacante, uma vez que não foram projetados para esse fim.

Comentários:

Opa... também para coletar informações sobre a atividade do atacante, uma vez que eles foram projetados justamente para esse fim.

Gabarito: Errado

---

12. (CESPE / FUB – 2018) Em uma comunicação de rede, um IPS instalado em linha (no caminho de comunicação entre a origem e o destino) analisa ativamente o tráfego e pode disparar ações automatizadas em tempo real, como, por exemplo, bloquear o tráfego de uma origem identificada como maliciosa.

Comentários:

Perfeito! IPS opera de forma proativa, disparando ações automatizadas em tempo real.

Gabarito: Correto

---

13. (CESPE / IFF – 2018) A fim de descobrir, em tempo real, as tentativas de acessos não autorizados a recursos de sistema, utiliza-se o serviço de segurança que monitora, analisa e informa os eventos ocorridos no próprio sistema denominado:

a) antispam.
b) antivírus.
c) firewall de aplicação.
d) firewall de estado.
e) IDS.

Comentários:

Monitora, analisa e informa sobre eventos ocorridos? Trata-se de um IDS!

Gabarito: Letra E

---

14. (CESPE / CGM de João Pessoa - PB – 2018) Um Sistema de Detecção de Intrusão (Intrusion Detection System – IDS) consegue detectar comportamentos maliciosos tanto em computadores individuais quanto em redes de computadores.

Comentários:

Perfeito! Eles são utilizados geralmente para detectar comportamentos maliciosos em redes de computadores, mas também podem ser utilizados para detecção em computadores individuais.

Gabarito: Correto

---

15. (CESPE / FUB – 2016) Ferramentas IDS podem trabalhar simplesmente emitindo alertas de tentativa de invasão ou aplicando ações com a finalidade de contra-atacar a tentativa de invasão.

Comentários:

Discordo do gabarito dessa questão! Ferramentas IDS não aplicam ações com a finalidade de contra-atacar a tentativa de invasão. Não sei dizer se não houve recurso na época, mas isso não está de acordo com a bibliografia consagrada.

Gabarito: Correto

---

16. (CESPE / TC-DF - 2014) Uma DMZ destinada a proteger um segmento de rede contra ataques externos deve ser colocada preferencialmente entre o roteador externo e a Internet.

Comentários:

Na verdade, deve ser colocada entre o roteador externo (internet) e a rede interna.

Gabarito: Errado

---

17. (CESPE / TJ-SE – 2014) A detecção de intrusão abrange formas de resposta, tais como a geração de alertas e a interrupção dos fluxos de dados maliciosos.

Comentários:

Considerando que tanto IDS quanto IPS detectam intrusão, essa detecção realmente abrange formas de resposta como a geração de alertas (IDS) e a interrupção dos fluxos de dados maliciosos (IPS).

Gabarito: Correto

---

18. (CESPE / TJ-ES – 2014) A detecção de intrusão compreende medidas proativas na proteção de sistemas computacionais.

Comentários:

Lembrem-se que tanto IDS quanto IPS detectam intrusão, logo a questão não está falando de IDS – ela está falando de forma genérica. *Nesse caso, a detecção de intrusão compreende medidas proativas na proteção de sistemas computacionais?* Sim, por meio do IPS! Logo, discordo do gabarito definitivo da questão.

Gabarito: Errado

---

19. (CESPE / CNJ – 2013) Ferramentas de IDS (Intrusion Detect System) são capazes de detectar anomalias no tráfego de rede, gerar logs e reações, como regras de bloqueio do tráfego.

Comentários:

Opa... ele não gera reações como regras de bloqueio do tráfego.

Gabarito: Errado

---

20. (CESPE / Polícia Federal - 2012) Os sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) utilizam metodologias similares na identificação de ataques, visto que ambos analisam o tráfego de rede em busca de assinaturas ou de conjunto de regras que possibilitem a identificação dos ataques.

Comentários:

Na identificação de ataques, a metodologia é realmente similar! De fato, ambos analisam o tráfego da rede em busca de assinaturas ou de um conjunto de regras que possibilitem a identificação dos

ataques. A diferença entre eles é que o IDS apenas monitora e alerta; o IPS monitora e reagem contra a invasão.

Gabarito: Correto

---

21. (CESPE / TJ-AC - 2012) O IPS (Intrusion Prevention System) e o IDS (Intrusion Detection System) são ferramentas de rede que, respectivamente, protegem a rede interna de ataques externos e antivírus em cloud para Internet.

Comentários:

O IDS não tem nenhuma relação com antivírus em cloud para Internet! Que viagem... ele é apenas um mecanismo de segurança que monitora uma rede, detecta possíveis invasões e gera alertas e/ou logs (registros de eventos).

Gabarito: Errado

---

22. (CESPE / TJ-AC – 2012) Sistemas de prevenção à intrusão (IPS) e sistemas de detecção de intrusão (IDS) são sistemas concebidos com os mesmos propósitos. A diferença entre eles encontra-se no público-alvo. Enquanto os IPS são sistemas voltados para os usuários domésticos, os IDS focam as grandes redes corporativas.

Comentários:

Eles não possuem o mesmo propósito – um apenas monitora e gera alertas; o outro monitora e impede a invasão. Não há nenhuma relação com o público-alvo!

Gabarito: Errado

---

23. (CESPE / TRE-ES - 2011) Com a instalação do software DMZ, cria-se uma barreira de proteção entre a intranet e a Internet.

Comentários:

DMZ não é um software, é uma sub-rede física ou lógica.

Gabarito: Errado

---

24. (CESPE / STM - 2011) IDS e IPS detectam intrusões com alta precisão, porém diferem pelo fato de o segundo atuar bloqueando o tráfego, quando algum evento relevante é detectado.

Comentários:

Alta precisão? Não! Há muitas ocorrências de falsos-positivos e falsos-negativos.

Gabarito: Errado

---

25. (CESPE / BRB – 2011) Honeypots são mecanismos de segurança, geralmente isolados e monitorados, que aparentam conter informação útil e valiosa para a organização. São armadilhas para enganar agentes nvasores como spammers ou crackers.

Comentários:

Galera, para mim não há erro dessa questão! A questão foi anulada e eu não consegui encontrar a justificativa, mas eu imagino que seja por conta do "*nvasores*".

Gabarito: Anulada

---

26. (CESPE / BRB - 2011) O posicionamento correto de um firewall é dentro da DMZ.

Comentários:

Na verdade, o posicionamento correto de um firewall é entre duas redes e, não, dentro da DMZ!

Gabarito: Errado

---

27. (CESPE / TJ-ES - 2011) Uma DMZ, ou rede de perímetro, representa um perímetro físico de isolamento de uma rede, geralmente protegendo uma rede externa por meio de uma VPN, sem necessidade de uso de firewalls, pois estes referem-se a perímetros lógicos.

Comentários:

DMZ realmente representa um perímetro físico de isolamento de uma rede (o fato de poder ser lógico não invalida a questão), no entanto ela serve para proteger uma rede interna e, não, externa. Além disso, não é por meio de uma VPN, mas – sim – por meio do uso de firewalls.

Gabarito: Errado

---

28. (CESPE / TJ-ES – 2011) IDS (Intrusion Detection System) pode ser utilizado para incrementar o trabalho do firewall e permitir que o tráfego de dados de uma rede seja monitorado para correção imediata de problemas ou falhas.

Comentários:

IDS realmente pode ser utilizado para incrementar o trabalho de um firewall. *Ele permite que o tráfego de dados de uma rede seja monitorado para correção imediata de problemas ou falhas?* Sim,

note que ele não fala que é o próprio IDS que fará essa correção, mas o monitoramento e detecção do tráfego permitirá que outros agentes possam fazer a correção imediata dos problemas/falhas.

Gabarito: Correto

---

29. **(CESPE / BANCO DA AMAZÔNIA - 2010)** A ocorrência de falsos positivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.

Comentários:

Falsos-positivos são eventos que normais que são identificados como anormais! O IDS apenas detectará, mas não reagirá contra esse evento normal, logo as consequências são mais brandas; já o IPS detectará e reagirá contra esse evento normal, logo as consequências são mais graves.

Gabarito: Errado

---

30. **(CESPE / BANCO DA AMAZÔNIA - 2010)** Uma zona desmilitarizada (DMZ) é uma porção da rede onde encontram-se, geralmente, os servidores de acesso externo da organização, como por exemplo, WWW e FTP. A DMZ é criada com o intuito de isolar e proteger a rede interna da organização contra acessos externos. Nesse caso, o firewall deixa passar os acessos destinados à DMZ e bloqueia os acessos destinados à rede interna.

Comentários:

Na DMZ, realmente estão localizados os servidores de acesso externo (Ex: WWW e FTP). Ela realmente cria um perímetro que isola e protege a rede interna da organização contra acessos externos. Por fim, um firewall realmente deixa passar os acessos destinados à DMZ e outro bloqueia os acessos destinados à rede interna.

Gabarito: Correto

---

31. **(CESPE / TRE-BA - 2010)** DMZ (Demilitarized Zone Network) é uma solução de segurança para redes na qual é criada uma rede intermediária entre a rede externa e a rede interna. Assim, não é possível implementar uma DMZ utilizando um único firewall.

Comentários:

É possível, sim! Nós vimos que existe a implementação com dois firewalls e a implementação com apenas um, porém essa última é mais rara e mais insegura.

Gabarito: Errado

QUESTÕES COMENTADAS – FCC

32. (FCC / TJ-MA – 2019) Um sistema que monitora pacotes de rede em busca de tráfego potencialmente prejudicial, respondendo a esse tipo de tráfego com a rejeição dos pacotes potencialmente mal-intencionados, corresponde a:

a) uma DMZ.
b) um switch de camada 3.
c) um IPS.
d) um Honeypot.
e) um Proxy SPS.

Comentários:

Se ele rejeita os pacotes potencialmente mal-intencionados, então ele possui uma função passiva (monitorar) e uma função ativa (rejeitar). Logo, trata-se de um IPS!

Gabarito: Letra C

---

33. (FCC / ARTESP - 2017) IDS e IPS são recursos de segurança que podem ser posicionados estrategicamente dentro da rede para detectar tráfego malicioso que por ventura tenha passado pelas regras do firewall. O IDS, por exemplo, ao detectar tráfego malicioso,

a) reagirá ao tráfego malicioso isolando os pacotes recebidos em uma área virtual da rede.
b) interromperá o tráfego automaticamente e negará novos pacotes da mesma origem.
c) gerará alarmes e/ou logs.
d) bloqueará a porta de origem do tráfego na rede automaticamente.
e) revidará automaticamente o ataque utilizando DoS.

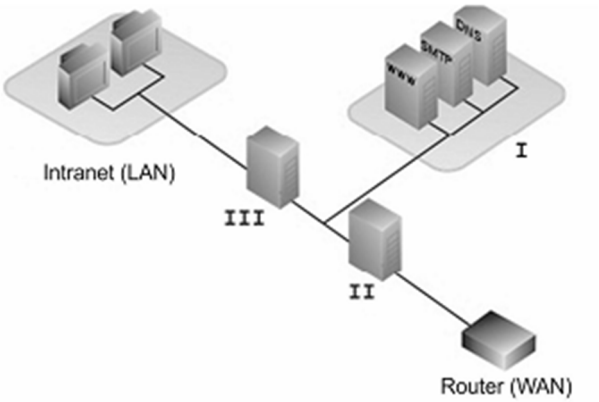
Comentários:

(a) Errado, ele não reagirá – apenas gerará alertas e/ou logs; (b) Errado, ele não reagirá, portanto não interromperá tráfego algum; (c) Correto; (d) Errado, ele não reagirá, portanto não bloqueará nada; (e) Errado, ele não reagirá, portanto não revidará nada.

Gabarito: Letra C

---

34. (FCC / ARTESP - 2017) A imagem abaixo mostra a utilização de uma arquitetura com mecanismos apropriados para proteger a rede interna de uma organização.



Na arquitetura mostrada na figura, I é:

a) um cluster, II é um firewall e III é uma DMZ.
b) uma DMZ e II e III são firewalls.
c) um Data Center, II é uma DMZ e III é um firewall.
d) um cluster de servidores e II e III são DMZs.
e) um firewall, II é um IPS e III é um IDS.

Comentários:

A figura apresenta um sinal de internet chegando ao Roteador (Rede WAN). Em II, há um Firewall de Borda; em I, há uma DMZ (vejam que estão presentes o Servidor WWW, SMTP e DNS); em III há um Firewall de Perímetro, que protege a rede interna da organização.

Gabarito: Letra B

---

35. (FCC / TRF-1ª Região - 2014) *Criminosos virtuais costumam varrer a Internet procurando computadores vulneráveis, sem ter alvos específicos para atacar. Aproveitando-se disso, especialistas em segurança criam sistemas que se mostram vulneráveis, atraindo invasores que, quando conectados ao sistema, serão monitorados. Com isso, técnicas, vulnerabilidades e ferramentas são obtidas para análise e proteção dos sistemas.*

(http://g1.globo.com)

O texto trata de uma técnica utilizada para detectar intrusões em uma rede, em que um computador é usado como isca para intrusos. Muitas vezes é colocado na rede de forma que se torna atraente, como estar configurado com um software com vulnerabilidades conhecidas e com seu disco rígido repleto de documentos que aparentam conter segredos da empresa ou outra informação aparentemente valiosa. A técnica descrita é conhecida como:

a) honeybox.
b) mousetrap.
c) honeypot.
d) fakecall.

e) goldenbox.

Comentários:

Detectar intrusões? Computador como isca para intrusos? De forma atraente? Configurado com vulnerabilidades conhecidas? São todas características de Honeypot!

Gabarito: Letra C

---

36. (FCC / TRT-SP - 2015) Com respeito à DMZ, do termo em inglês "DeMilitarized Zone", ou seja, "Zona Desmilitarizada" considere:

I. Tem como função manter os serviços que possuem acesso externo separados da rede local, restringindo ao máximo um potencial dano causado por algum invasor, tanto interno como externo.

II. Permite o acesso de usuários externos aos servidores específicos localizados na rede de perímetro e também o acesso deles à rede corporativa interna.

III. Tem como papel principal ser uma rede "tampão" entre as redes externa e interna.

IV. A configuração é realizada através do uso de equipamentos de Firewall, que vão realizar o controle de acesso entre ela, a rede local e a Internet.

Está correto o que consta APENAS em:

a) II.
b) I, III e IV.
c) II, III e IV.
d) I e II.
e) I e III.

Comentários:

(I) Correto, é uma característica típica de uma DMZ; (II) Errado, não permite acesso à rede corporativa interna; (III) Correto, serve realmente como um "tampão"; (IV) Correto, firewalls são essenciais para a implementação de uma zona desmilitarizada.

Gabarito: Letra B

---

37. (FCC / TJ-AP - 2014) Um dos dispositivos utilizados em rede de computadores para aumentar a segurança é o Firewall, que é instalado na fronteira da rede local com a rede ampla. Na estrutura de um Firewall que possui a DMZ, pode ser encontrado, dentro da DMZ, um servidor:

a) LDAP.
b) de páginas Web públicas.
c) Proxy.
d) de backup de arquivos privados.
e) DHCP.

Comentários:

(a) Errado, esse servidor geralmente é encontrado em redes internas; (b) Correto; (c) Errado, esse servidor não deve estar dentro DMZ; (d) Errado, esse servidor geralmente é encontrado em redes internas; (e) Errado, esse servidor geralmente é encontrado em redes internas.

Gabarito: Letra B

---

38. (FCC / TRE-CE - 2012) A sub-rede, também conhecida como rede de perímetro, utilizada para transmitir informações entre uma rede confiável e uma não confiável, mantendo os serviços que possuem acesso externo separados da rede local, é chamada de:

a) proxy.
b) VPN.
c) firewall.
d) DMZ.
e) intranet.

Comentários:

Sub-rede? Rede de perímetro? Transmitir informações entre uma rede confiável e uma não confiável? Mantém os serviços que possuem acesso externo separados da rede local? São todas características de uma DMZ!

Gabarito: Letra D

---

39. (FCC / TRT-RO e AC - 2011) No ambiente de rede da empresa, é uma região que pode ser acessada tanto por uma rede interna quanto pela pública (internet) e que servidores nela presentes não podem acessar os computadores internos da empresa por questões de segurança. Trata-se de:

a) FTP.
b) DMZ.
c) DNS.
d) DTD.
e) SMS.

Comentários:

Região que pode ser acessada tanto por uma rede interna quanto pela rede pública (internet) em que servidores nela presentes não podem acessar os computadores internos da empresa por questões de segurança. Esses são conceitos de uma DMZ!

Gabarito: Letra B

40.(FCC / TRT-MS - 2011) É uma pequena rede situada entre uma rede confiável e uma não confiável, ou seja, mantém a rede local separada de todos os serviços que possuem acesso externo:

a) VPN (Virtual Private Network).
b) DMZ (DeMilitarized Zone).
c) VNC (Virtual Network Computing).
d) CSG (Citrix Secure Gateway).
e) SWG (Secure Web Gateway).

Comentários:

Pequena rede? Entre uma rede confiável e uma não confiável? Mantém a rede local separada de serviços externos? São todas características de uma DMZ!

Gabarito: Letra B

41.(FCC / TRE-AM - 2010) A segurança de perímetro reside na separação do tráfego entre servidores de redes internas e externas e é reforçada por um firewall, que inspeciona os pacotes e as sessões para determinar o que deve ser transmitido para a rede protegida e/ou a partir dela ou ser descartado. É uma característica:

a) DMZ.
b) CSG.
c) IPsec.
d) ATM.
e) VPN.

Comentários:

Vejam as palavras-chave: segurança de perímetro; separa tráfego entre redes internas e externas; reforçada por firewall; determina o que deve ser transmitido para a rede protegida e/ou a partir dela ou ser descartado. Todas são características de uma DMZ!

Gabarito: Letra A

---

42. (FCC / TER-MS - 2007) Uma DMZ - Zona Desmilitarizada - é um segmento de rede parcialmente protegido que para possibilitar maior segurança na Internet deve estar associada ao mecanismo de proteção:

a) Plano de contingência.
b) Proxy.
c) Criptografia.
d) Firewall.
e) Sistema de detecção de intrusão.

Comentários:

DMZ está sempre associada intimamente a um Firewall.

Gabarito: Letra D

QUESTÕES COMENTADAS – FGV

43. (FGV / BANESTES - 2018) Um ataque de negação de serviço a uma instituição foi detectado pelo sistema de proteção instalado, que colocou automaticamente regras de proteção para evitá-lo. Pode-se concluir que o sistema de proteção usado é do tipo:

a) IDS
b) IPS
c) EPP
d) DLP
e) DNSSEC

Comentários:

Note que o enunciado afirma que o ataque foi detectado pelo sistema de proteção, que colocou automaticamente regras de proteção para evitá-lo, portanto reagiu ao ataque. Dessa forma, só pode ser um IPS.

Gabarito: Letra B

---

44. (FGV / MPOG - 2013) Um analista de segurança precisa detectar preventivamente ataques a uma determinada subrede, realizando contramedidas de forma automática. O instrumento mais adequado a realizar essa função é um:

a) IDS;
b) Firewall;
c) IPS;
d) Proxy;
e) Filtro de pacotes.

Comentários:

Detectar preventivamente ataques a uma determinada sub-rede é uma característica que pode ser do IDS ou IPS. No entanto, realizar contramedidas de forma automática é uma característica apenas do IPS.

Gabarito: Letra C

QUESTÕES COMENTADAS – VUNESP

45. (VUNESP / EMPLASA – 2014) Existem diversos recursos que podem ser utilizados para aumentar a segurança em sistemas de informação. Para detectar as invasões nesses sistemas, pode-se utilizar um IDS (Sistema de Detecção de Intrusão) ou o recurso denominado:

a) trap.
b) bridge.
c) switch.
d) gateway.
e) honeypot.

Comentários:

A única opção que apresenta um sistema de detecção de intrusão é o Honeypot.

Gabarito: Letra E

---

46. (VUNESP / COREN-SP - 2013) No contexto de sistemas de detecção de intrusão, um honeypot é:

a) uma aplicação que facilita o acesso não autorizado aos servidores de produção.
b) o nome dado ao servidor principal de uma empresa, isto é, aquele que atacantes procurarão invadir.
c) o canal de comunicação com a rede interna de uma empresa.
d) um servidor falso que expõe vulnerabilidades conhecidas para os atacantes.
e) o banco de dados de uma aplicação.

Comentários:

Nenhum dos itens faz qualquer sentido, exceto o honeypot como um servidor falso que expõe vulnerabilidades conhecidas para os atacantes.

Gabarito: Letra D

QUESTÕES COMENTADAS – CESGRANRIO

47. (CESGRANRIO / PETROBRAS - 2004) As chamadas zonas desmilitarizadas (DMZ) podem ser implementadas a partir de firewalls. Quais dos componentes abaixo, são normalmente encontrados em uma DMZ?

a) Servidores de bancos de dados.
b) Servidores Web para Internet.
c) Servidores DHCP da rede interna.
d) Estações de trabalho de usuários.
e) Sistemas legados.

Comentários:

(a) Errado, são normalmente encontrados na rede interna; (b) Correto; (c) Errado, são normalmente encontrados na rede interna; (d) Errado, são normalmente encontrados na rede interna; (e) Errado, são normalmente encontrados na rede interna.

Gabarito: Letra B

---

48. (CESGRANRIO / PETROBRAS – 2012) No contexto de rotinas de proteção e segurança, HoneyPot é um(a):

a) antivírus especializado na detecção e remoção de cavalos de Troia.

b) dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

c) programa que recolhe informações sobre um usuário e as transmite pela Internet, sem o conhecimento e o consentimento desse usuário.

d) mecanismo para proteção de informações sigilosas que usa técnicas de criptografia.

e) ferramenta que simula falhas de segurança em um sistema e colhe informações sobre eventuais invasores.

Comentários:

(a) Errado, isso seria um antimalware; (b) Errado, ele não aplica nenhuma política de segurança – isso seria um firewall; (c) Errado, isso seria um botnet ou spyware; (d) Errado, isso seria a própria criptografia; (e) Correto.

Gabarito: Letra E

49.(CESGRANRIO / LIQUIGAS – 2012) Os mecanismos de segurança da informação proporcionam a implantação de diferentes tipos de controle. Honeypot é exemplo de um recurso que pode implantar segurança por meio de controle:

a) interno
b) lógico
c) restrito
d) biométrico
e) de assinatura digital

Comentários:

Honeypot pode implantar segurança por meio de controle lógico.

Gabarito: Letra B

QUESTÕES COMENTADAS – DIVERSAS BANCAS

50. (CPCON / PREF CUIATÉ-PB - 2019) Em segurança da informação, um IDS pode ser:

a) um sistema de detecção de imagem, que permite recuperar as principais imagens do ataque recebido, permitindo detectar o invasor pela análise das imagens.

b) um software de interrupção de disco, que, mediante algum tipo de ataque, trava completamente o sistema até que o invasor seja detectado, evitando perda de dados.

c) um sistema de detecção de intrusão, que possibilita a coleta e o uso de informações dos diversos tipos de ataques, ajudando na defesa de toda uma infraestrutura de rede.

d) um sistema de detecção de IP, através do qual o servidor de DNS consegue identificar o exato momento em que o ataque ocorreu e o IP do computador do atacante.

e) um software de apoio aos hackers, que permite instalar aplicativos maliciosos no computador da vítima, roubando senhas e informações pessoais.

Comentários:

(a) Errado, não tem nenhuma relação com imagem; (b) Errado, não tem nenhuma relação com interrupção de disco; (c) Correto, ele é um sistema de detecção de instrução, que realmente possibilita a coleta e o uso de informações dos diversos tipos de ataques, ajudando na defesa de toda uma infraestrutura de rede; (d) Errado, não tem nenhuma relação com detecção de IP; (e) Errado, não tem nenhuma relação com apoio aos hackers.

Gabarito: Letra C

---

51. (QUADRIX / CRESS-GO - 2019) O IDS (Intrusion Detection System) é capaz de monitorar os arquivos de configuração do Windows.

Comentários:

O IDS é capaz de monitorar quaisquer arquivos que trafegam em uma rede.

Gabarito: Correto

---

52. (IADES / AL-GO - 2019) Entre esses dois tipos de firewalls, estão um ou mais dispositivos conectados em uma região chamada de rede DMZ (zona desmilitarizada).

STALLINGS, W. Cryptography and network security: principles and practice. Londres: Pearson, 2017. Tradução Livre.

Com relação à rede DMZ, é correto afirmar que geralmente os dispositivos que ficam nela são acessíveis:

a) pela rede externa, mas precisam de algumas proteções.
b) somente pela rede interna, mas precisam de algumas proteções.
c) pela rede externa e não precisam de proteções.
d) somente pela rede interna e não precisam de proteções.
e) somente pela rede DMZ e não precisam de proteções.

Comentários:

Os dispositivos dentro da DMZ são acessíveis pela rede interna e externa, mas é claro que precisam de algumas proteções (firewall) para a rede externa – que fica exposta.

Gabarito: Letra A

---

53. (IDIB / Prefeitura de Planaltina – GO - 2018) Assinale o dispositivo capaz de prevenir ataques a rede de computador:

a) IDS
b) IPS
c) HIDS
d) NIDS.

Comentários:

Capaz de prevenir ataques a rede de computador? Trata-se do IPS!

Gabarito: Letra B

---

54. (COPESE / Câmara de Palmas-TO – 2018) Os Potes de Mel (Honeypots) são sistemas projetados para auxiliar no processo de detecção de intrusão em redes e sistemas computacionais. Marque a alternativa que NÃO apresenta uma função desses sistemas:

a) Desviar um atacante do acesso a sistemas críticos.
b) Coletar informações sobre a atividade do atacante.
c) Incentivar o atacante a ficar no sistema por tempo suficiente para que os administradores respondam.
d) Tentar todas as chaves possíveis em uma amostra de texto cifrado até obter tradução que leve a um texto às claras inteligível.

Comentários:

(a) Correto, essa é uma possível comum de honeypots; (b) Correto, essa é uma função comum de honeypots; (c) Correto, essa é uma função comum de honeypots; (d) Errado, essa não é uma função comum de um honeypot – esse é um ataque de força bruta.

Gabarito: Letra D

---

55. **(IBFC / TJ-PE - 2017)** Questionou-se entre a equipe, a diferença básica entre um IPS (Intrusion Prevention System) e um IDS (Intrusion Detection System). Assinale a alternativa que identifica corretamente essa diferença:

a) o IDS possui um papel estritamente passivo, ou seja, não toma ação, enquanto o IPS, por sua vez, possui um papel ativo tomando algum tipo de ação em caso de detecção de algum intruso.

b) o IPS possui um papel estritamente passivo, ou seja, não toma ação, enquanto o IDS, por sua vez, possui um papel ativo tomando algum tipo de ação em caso de detecção de algum intruso.

c) tanto o IPS como o IDS possuem o papel ativo sempre tomando algum tipo de ação em caso de detecção de algum intruso.

d) tanto o IPS como o IDS possuem o papel passivo, com a única diferença principal que o IDS fica conectado junto a um firewall.

e) não se pode dizer que o IPS e o IDS sejam ativos ou passivos pois os mesmos são considerados como equipamentos de rede com a responsabilidade de criar uma conexão segura e criptografada por meio de tunelamento.

Comentários:

(a) Correto; (b) Errado, a questão inverteu os conceitos; (c) Errado, IDS não possui papel ativo; (d) Errado, IPS não possui papel passivo; (e) Errado, não tem nenhuma relação com conexão segura e criptografada por meio de tunelamento.

Gabarito: Letra A

---

56. **(FAU / E-PARANÁ COMUNICAÇÃO - 2017)** Analise as assertivas e assinale a alternativa que aponta as corretas:

I - A DMZ é uma rede que fica entre a rede interna, que deve ser protegida, e a rede externa.

II - Os proxies são sistemas que atuam como um gateway entre duas redes, permitindo as requisições dos usuários internos e as respostas dessas requisições, de acordo com a política de segurança definida.

III - O Firewall é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego.

a) Apenas a afirmativa I.
b) Apenas a afirmativa II.
c) Apenas as afirmativas II e III.
d) Apenas as afirmativas I e III.
e) Todas as afirmativas estão corretas.

Comentários:

(I) Correto, tudo perfeito; (II) Correto, tudo perfeito também; (III) Correto, perfeito mais uma vez. Essa questão resume tudo que estudamos :)

Gabarito: Letra E

---

57. (COSEAC / UFF - 2017) O ambiente criado para proteger a rede interna por meio de um perímetro de segurança, localizado entre a Internet e a rede interna e normalmente acoplado a um firewall, é:

a) Network Address Translation (NAT).
b) Sistema de Detecção de Intrusos (IDS).
c) Zona Desmilitarizada (DMZ).
d) Sistema de Prevenção de Intrusos (IPS).
e) Pote de Mel (Honeypot).

Comentários:

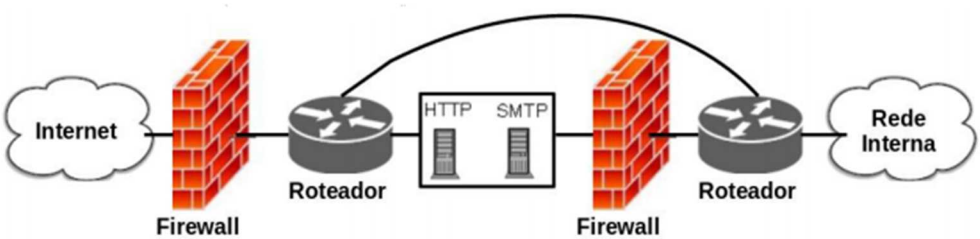
Proteger a rede interna? Perímetro de segurança? Localizado entre a Internet e a rede interna? Acoplado a um firewall? Todas são características de uma Zona Desmilitarizada (DMZ).

Gabarito: Letra C

---

58. (IF-PE / IF-PE - 2016) Os profissionais de tecnologia da informação encarregados de administrar os serviços Web e de rede do IFPE necessitam manter-se atualizados e atentos para implantar estratégias com o objetivo de aumentar a segurança da rede Institucional. Considerando esse contexto, analise o projeto de rede apresentado na FIGURA 02, assinalando a única alternativa CORRETA.

FIGURA 02 (exemplo de um projeto de rede)



a) Os servidores de HTTP e SMTP estão implantados em uma DMZ com o objetivo de oferecer maior segurança à LAN em caso de comprometimento de um desses serviços por um invasor.

b) Esse projeto de rede é ideal para empresas que precisem garantir máxima segurança para sua rede interna, uma vez que os dispositivos dela não possuem conexão com a Internet.

c) Um dos pontos negativos dessa solução é que o servidor HTTP não pode ser acessado pelos dispositivos alocados na rede interna.

d) Estão contemplados nesse projeto de rede um servidor Web e um sistema de gerenciamento de banco de dados.

e) Os servidores de HTTP e SMTP estão oferecendo serviços de DNS com o objetivo de oferecer maior segurança à rede local ao converter os endereços IP externos em internos para a rede local.

Comentários:

(a) Correto. Servidor HTTP e SMTP comumente ficam localizados em uma DMZ com o objetivo de oferecer maior segurança à LAN em caso de comprometimento de um desses serviços por um invasor; (b) Errado. Dispositivos da rede interna possuem – sim – conexão com a internet, mas são protegidos por dois firewalls; (c) Errado. Todos os dispositivos localizados na zona desmilitarizada são acessíveis na rede externa e interna; (d) Errado. Nada indica que há um sistema de gerenciamento de banco de dados; (e) Errado. Serviços de DNS são oferecidos por um Servidor DNS. Além disso, ele não tem função de converter endereços IP externos em internos – eles convertem endereços IP em nomes de domínio e vice-versa.

Gabarito: Letra A

---

59. (IESES / BAHIAGÁS - 2016) Escolha a melhor alternativa que defina o que é uma DMZ (Demilitarized Zone ou Zona Desmilitarizada):

a) É um local físico da empresa que é utilizado para o armazenamento de todos os equipamentos de informática.

b) É uma área lógica da rede na qual, geralmente, são colocados os servidores e serviços que estarão publicamente disponíveis na internet. Geralmente é protegida por algum mecanismo de segurança, como firewall.

c) É a área mais segura do datacenter, onde somente o administrador da empresa tem acesso.

d) É uma área física ou lógica da rede onde devem sempre ser colocados os serviços acessíveis somente internamente na empresa. Usualmente não é protegida por mecanismos de segurança, como firewalls.

e) O principal objetivo de uma DMZ é aumentar a velocidade de acesso às páginas WEB hospedadas na nuvem.

Comentários:

(a) Errado, não é um local físico da empresa (é uma sub-rede) e não é utilizado para o armazenamento de todos os equipamentos de informática; (b) Correto, ela pode ser física ou lógica – não há erro no item; (c) Errado, não é a área mais segura e qualquer um pode acessar; (d) Errado, são acessíveis internamente ou externamente – é, sim, protegida por mecanismos de segurança como firewalls; (e) Errado, não tem nenhuma relação com aumentar a velocidade de acesso às páginas web hospedadas na nuvem.

Gabarito: Letra B

60.(FAUEL / CISMEPAR-PR - 2016) No contexto de segurança de redes de computadores, o que é um falso-positivo?

a) Um evento real não detectado pelo IDS.
b) Um evento real detectado pelo IDS.
c) Um evento não real detectado pelo IDS como real.
d) Um evento não real não detectado pelo IDS.

Comentários:

Um falso-positivo é um evento não real (normal) detectado como real (anormal) pelo IDS; já um falso-negativo é um evento real (anormal) detectado como não real (normal) pelo IDS.

Gabarito: Letra C

61.(IBFC / EBSERH – 2016) Ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o(s) invasor(es):

a) Ahwatukee

b) CalaBash
c) BeggingBbowl
d) HoneyPot
e) CucurBit

Comentários:

Essa questão é uma viagem – nenhuma dessas opções faz qualquer sentido, exceto o Honeypot! Ele realmente tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre invasores.

Gabarito: Letra D

---

62. (OBJETIVA / SESCOOP - 2015) Dentre os conceitos de firewall, a zona desmilitarizada (DMZ) corresponde a:

a) Uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável.
b) Um tipo de firewall do tipo stateful.
c) Uma área insegura que permite a incidência de ataques.
d) Uma área composta de serviços de filtragem do mais alto nível.

Comentários:

(a) Correto, trata-se realmente de uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável (internet); (b) Errado, DMZ não é um tipo de firewall; (c) Errado, não é uma área insegura, mas com um nível de segurança mais bairro; (d) Errado, não possui serviços de filtragem, mas serviços públicos.

Gabarito: Letra A

---

63. (UNIRIO / UNIRIO - 2014) Os serviços indicados para serem abrigados na rede DMZ de uma instituição são:

a) serviços internos que só podem ser acessados por usuários externos via VPN.
b) serviços internos que nunca devem ser acessados por usuários externos à instituição.
c) serviços que só podem ser acessados por usuários externos à instituição.
d) serviços internos que só podem ser acessados por usuários externos que estejam cadastrados na DMZ.
e) serviços que podem ser publicamente acessados por usuários externos à instituição.

Comentários:

(a) Errado, não são serviços internos; (b) Errado, não são serviços internos; (c) Errado, são serviços que podem ser acessados por usuários internos ou externos; (d) Errado, não são serviços internos; (e) Correto, são serviços que podem ser publicamente acessados por usuários externos à instituição.

Gabarito: Letra E

64.(QUADRIX / COREN-BA - 2014) Assinale a alternativa que exibe como a zona desmilitarizada também é conhecida:

a) Firewall.
b) Rede de Contato.
c) Rede de Perímetro.
d) Área de Conflito.
e) Área de Contato.

Comentários:

A Zona Desmilitarizada é também conhecida como uma Rede de Perímetro.

Gabarito: Letra C

65.(FUNCAB / MDA – 2014) Uma empresa instalou um sistema de detecção de intrusão baseado em honeypots. Isso significa que nesse sistema:

a) um computador qualquer simula importância, atraindo intrusos para ele, sendo que os atacantes são monitorados ao invadirem.

b) foram instalados pelo menos dois firewalls para realizar varreduras das portas TCP, procurando sinais ICMP externos.

c) um computador monitora todos os e-mails de saídas realizados por funcionários da empresa, tentando identificar e-mail suspeitos.

d) vasculha-se a rede interna, procurando servidores web que estejam instalados em máquinas comuns que não servidores originais.

e) um servidor especial testa as saídas UDPs procurando falhas; se as encontra, informa um firewall para bloqueá-las.

Comentários:

Mais uma questão que apresenta diversas opções que não têm qualquer relação com Honeypot! Ele é um computador qualquer simula importância, atraindo intrusos para ele, sendo que os atacantes são monitorados ao invadirem.

Gabarito: Letra A

---

66. (FUNRIO / MPOG - 2013) Qual dispositivo usado na segurança de rede que investiga todo pacote que passa por ele, abrindo seu conteúdo e filtrando se necessário?

a) Sistema de exploração de vulnerabilidade.
b) Sistema Firewall.
c) Sistema de detecção de intrusão.
d) Sistema de eliminação de intrusão.
e) Sistema de prevenção de intrusão.

Comentários:

É maluquice, mas – para mim – essa questão possui três respostas corretas: (b), (c) e (e). Firewall, IDS e IPS são capazes de investigar pacotes, abrindo seu conteúdo e filtrando, se necessário.

Gabarito: Letra E

---

67. (FMP CONCURSOS / PROCEMPA - 2012) Em um IDPS, Sistemas de Detecção e Prevenção de Intrusão, as técnicas que são baseadas em comparação de uma atividade (pacote ou entrada em um log de eventos) com uma lista previamente estabelecida, são classificadas como:

a) análise statefull de protocolos.
b) análise de anomalias.
c) análise de assinatura.
d) inspeção profunda de pacotes.
e) inspeção de proxy.

Comentários:

Eles podem funcionar baseado em assinaturas ou anomalias. Aquele que se baseia em uma comparação com listas estabelecidas são classificadas como Análise de Assinatura.

Gabarito: Letra C

---

68. (COMPROV / UFCG – 2012) O honeypot não é necessariamente um tipo de IDS, porém ele pode ser utilizado para que o administrador de segurança aprenda sobre os ataques realizados contra sua organização, detectando e armazenando todos os tipos de ataques.

Comentários:

Ele – de fato – não é necessariamente um tipo de IDS e realmente pode ser utilizado para que o administrador de segurança aprenda sobre os ataques realizados contra sua organização, detectando e armazenando todos os tipos de ataques (em logs/registros).

Gabarito: Correto

---

69. (IADES / PG-DF - 2012) Em situação hipotética, um órgão de segurança do governo está sofrendo um ataque ao seu servidor web. O perito em segurança, responsável por analisar o incidente, tomou a decisão de investigar a ação criminosa em andamento, com o objetivo de estudar o seu comportamento e obter informações sobre as técnicas de ataques utilizadas. Assinale a alternativa adequada a esse tipo de análise:

a) Firewall.
b) Botnet.
c) DMZ.
d) Hijacking.
e) Honeypot.

Comentários:

Investigar a ação criminosa em andamento com o objetivo de estudar comportamento e obter informações sobre as técnicas de ataques é uma característica de um Honeypot.

Gabarito: Letra E

---

70. (AOCP / TCE-PA - 2012) Em segurança da informação uma DMZ é a sigla para de "DeMilitarized Zone". A função de uma DMZ é:

a) proteger os servidores que acessam a internet contra ataques de serviços invasores.
b) determinar um perímetro de segurança para o acesso a redes militares de computadores por civis.
c) manter todos os serviços que possuem acesso externo separados da rede local.
d) manter todo o funcionamento da rede de computadores, mesmo após uma invasão.
e) assegurar que as redes militares não sejam invadidas por crackers.

Comentários:

(a) Errado, isso é a função de um IPS; (b) Errado, não tem nenhuma relação com redes militares; (c) Correto, ela realmente mantém todos os serviços que possuem acesso externo separados da rede local/interna; (d) Errado, esse item sequer faz sentido; (e) Errado, não tem nenhuma relação com redes militares.

Gabarito: Letra C

---

71. (FUNIVERSA / SEPLAG-DF - 2010) Um IPS (Intrusion Prevention System), de forma geral, é um equipamento auxiliar no gerenciamento e segurança da rede, instalado em determinado ponto de passagem de tráfego de uma rede de computadores. Assinale a alternativa que apresenta apenas funções que podem ser realizadas por um IPS:

a) Autenticação de usuários e acesso a serviço de mensagens eletrônicas (e-mail).
b) Cadastro de usuários da rede e controle de acesso a recursos locais.
c) Detecção de ataque DDoS e controle de uso de banda por aplicação.
d) Armazenamento de backups e controle de acesso a banco de dados.
e) Filtro de pacotes, por aplicação, e hospedagem de sites Web.

Comentários:

O IPS é um sistema de prevenção de invasão, logo nenhuma das opções apresenta funções que podem ser realizadas por ele; exceto a detecção de ataques de DDoS (Negação de Serviço Distribuída) e controle de uso de banda por aplicação. Nesses casos, ele é capaz de monitorar, identificar e reagir contra esse tipo de ataque.

Gabarito: Letra C

---

72. (IDIB / TRE-AL - 2004) Um dos mecanismos utilizados pelos sistemas detectores de intrusão (IDS - Intrusion Detection System) é a detecção por assinatura, em que a assinatura típica de um tráfego malicioso permite identificá-lo como um ataque a computador.

Comentários:

Perfeito! Na detecção por assinatura, o tráfego malicioso é comparado com uma base de dados de ataques conhecidos a fim de identifica-lo.

Gabarito: Correto

Lista de Questões – CESPE

1. **(CESPE / DPDF - 2022)** Um IDS (Intrusion Detection System), quando disponibilizado para oferecer detecção somente no servidor da rede onde ele está instalado, é denominado NIDS (Network Intrusion Detection System).

2. **(CESPE / DPDF - 2022)** O registro de logs e a desinstalação de software desnecessário para o funcionamento do servidor são considerados ações do processo de hardening do sistema operacional.

3. **(CESPE / TELEBRÁS - 2021)** Em uma organização, será considerado como um sistema de prevenção de intrusão baseado em hospedeiro um aplicativo que, instalado em uma das máquinas da infraestrutura de rede, capture pacotes nessa rede, compare esses pacotes com uma base de assinaturas (padrões de ataques específicos), gere eventos que possam ser ações ou alertas e envie esses eventos para o próprio administrador.

4. **(CESPE / TELEBRÁS - 2021)** Capaz de analisar qual a parcela de risco de uma intrusão e bloqueá-la antes que ela ocorra, um IPS permite criar regras com o objetivo de monitorar aumentos anormais de tráfego de rede; além dessa funcionalidade, ele ainda pode alertar o responsável pela segurança, caso ocorram tais anomalias.

5. **(CESPE / CODEVASF – 2021)** Um dispositivo configurado como IPS (Intrusion Prevention System) analisa tráfegos na rede de computadores, em busca de assinaturas de ataques, e notifica os administradores, porém não possui autonomia para bloquear o tráfego de rede.

6. **(CESPE / Polícia Federal – 2021)** Caso o usuário tenha recebido um conjunto de arquivos com *trojan* em seu conteúdo e esses arquivos estejam em uma mídia de armazenamento local em sua estação de trabalho, recomenda-se a utilização de IDS (*intrusion detection system*) para a realização da limpeza dos arquivos.

7. **(CESPE / PRF – 2021)** O firewall da próxima geração (NGFW) dispõe, em um mesmo equipamento, de recursos como IDS (Intrusion Detection System), IPS (Intrusion Prevention System) e antivírus.

8. **(CESPE / TJ-AM – 2019)** Uma desvantagem de utilizar um IDS para proteger a rede contra ataques externos é que ele não pode ser configurado para realizar a atualização automática de suas definições de assinatura, pois a atualização é um procedimento cauteloso que deve ocorrer sob a supervisão do administrador de rede.

9. **(CESPE / TJ-AM – 2019)** Um IDS permite criar regras com o objetivo de monitorar aumentos anormais de tráfego de rede; além dessa funcionalidade, ele ainda pode alertar o responsável pela segurança, caso ocorram tais anomalias.

10. **(CESPE / EMAP- 2018)** O dispositivo de IPS (do inglês Intrusion Prevention System) utilizado em redes corporativas tem como objetivo bloquear ataques a partir da identificação de assinaturas e(ou) anomalias.

11. **(CESPE / ABIN – 2018)** Os honeypots (potes de mel), enquanto tecnologia de detecção de intrusão, podem ser utilizados para atingir os objetivos de atrair um atacante potencial e afastá-lo de sistemas críticos e de incentivar o atacante a ficar no sistema por período de tempo suficiente para que haja resposta dos administradores, mas não para coletar informações sobre a atividade do atacante, uma vez que não foram projetados para esse fim.

12. **(CESPE / FUB – 2018)** Em uma comunicação de rede, um IPS instalado em linha (no caminho de comunicação entre a origem e o destino) analisa ativamente o tráfego e pode disparar ações automatizadas em tempo real, como, por exemplo, bloquear o tráfego de uma origem identificada como maliciosa.

13. **(CESPE / IFF – 2018)** A fim de descobrir, em tempo real, as tentativas de acessos não autorizados a recursos de sistema, utiliza-se o serviço de segurança que monitora, analisa e informa os eventos ocorridos no próprio sistema denominado:

    a) antispam.
    b) antivírus.
    c) firewall de aplicação.
    d) firewall de estado.
    e) IDS.

14. **(CESPE / CGM de João Pessoa - PB – 2018)** Um Sistema de Detecção de Intrusão (Intrusion Detection System – IDS) consegue detectar comportamentos maliciosos tanto em computadores individuais quanto em redes de computadores.

15. **(CESPE / FUB – 2016)** Ferramentas IDS podem trabalhar simplesmente emitindo alertas de tentativa de invasão ou aplicando ações com a finalidade de contra-atacar a tentativa de invasão.

16. **(CESPE / TC-DF - 2014)** Uma DMZ destinada a proteger um segmento de rede contra ataques externos deve ser colocada preferencialmente entre o roteador externo e a Internet.

17. **(CESPE / TJ-SE – 2014)** A detecção de intrusão abrange formas de resposta, tais como a geração de alertas e a interrupção dos fluxos de dados maliciosos.

18. **(CESPE / TJ-ES – 2014)** A detecção de intrusão compreende medidas proativas na proteção de sistemas computacionais.

19. **(CESPE / CNJ – 2013)** Ferramentas de IDS (Intrusion Detect System) são capazes de detectar anomalias no tráfego de rede, gerar logs e reações, como regras de bloqueio do tráfego.

20. **(CESPE / Polícia Federal - 2012)** Os sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) utilizam metodologias similares na identificação de ataques, visto que ambos analisam o tráfego de rede em busca de assinaturas ou de conjunto de regras que possibilitem a identificação dos ataques.

21. **(CESPE / TJ-AC - 2012)** O IPS (Intrusion Prevention System) e o IDS (Intrusion Detection System) são ferramentas de rede que, respectivamente, protegem a rede interna de ataques externos e antivírus em cloud para Internet.

22. **(CESPE / TJ-AC – 2012)** Sistemas de prevenção à intrusão (IPS) e sistemas de detecção de intrusão (IDS) são sistemas concebidos com os mesmos propósitos. A diferença entre eles encontra-se no público-alvo. Enquanto os IPS são sistemas voltados para os usuários domésticos, os IDS focam as grandes redes corporativas.

23. **(CESPE / TRE-ES - 2011)** Com a instalação do software DMZ, cria-se uma barreira de proteção entre a intranet e a Internet.

24. **(CESPE / STM - 2011)** IDS e IPS detectam intrusões com alta precisão, porém diferem pelo fato de o segundo atuar bloqueando o tráfego, quando algum evento relevante é detectado.

25. **(CESPE / BRB – 2011)** Honeypots são mecanismos de segurança, geralmente isolados e monitorados, que aparentam conter informação útil e valiosa para a organização. São armadilhas para enganar agentes nvasores como spammers ou crackers.

26. **(CESPE / BRB - 2011)** O posicionamento correto de um firewall é dentro da DMZ.

27. **(CESPE / TJ-ES - 2011)** Uma DMZ, ou rede de perímetro, representa um perímetro físico de isolamento de uma rede, geralmente protegendo uma rede externa por meio de uma VPN, sem necessidade de uso de firewalls, pois estes referem-se a perímetros lógicos.

28. **(CESPE / TJ-ES – 2011)** IDS (Intrusion Detection System) pode ser utilizado para incrementar o trabalho do firewall e permitir que o tráfego de dados de uma rede seja monitorado para correção imediata de problemas ou falhas.

29. **(CESPE / BANCO DA AMAZÔNIA - 2010)** A ocorrência de falsos positivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.

30. **(CESPE / BANCO DA AMAZÔNIA - 2010)** Uma zona desmilitarizada (DMZ) é uma porção da rede onde encontram-se, geralmente, os servidores de acesso externo da organização, como por exemplo, WWW e FTP. A DMZ é criada com o intuito de isolar e proteger a rede interna da organização contra acessos externos. Nesse caso, o firewall deixa passar os acessos destinados à DMZ e bloqueia os acessos destinados à rede interna.

31. **(CESPE / TRE-BA - 2010)** DMZ (Demilitarized Zone Network) é uma solução de segurança para redes na qual é criada uma rede intermediária entre a rede externa e a rede interna. Assim, não é possível implementar uma DMZ utilizando um único firewall.

LISTA DE QUESTÕES – FCC

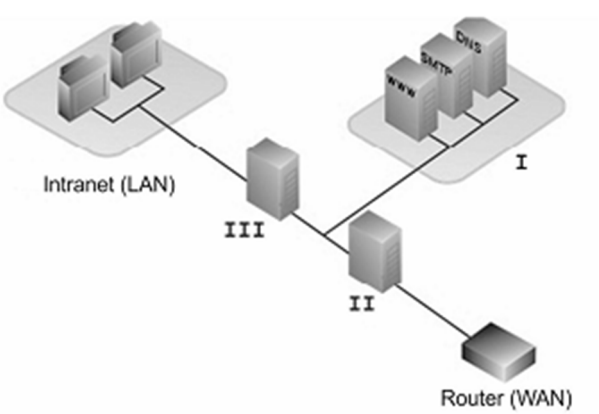
32. (FCC / TJ-MA – 2019) Um sistema que monitora pacotes de rede em busca de tráfego potencialmente prejudicial, respondendo a esse tipo de tráfego com a rejeição dos pacotes potencialmente mal-intencionados, corresponde a:

a) uma DMZ.
b) um switch de camada 3.
c) um IPS.
d) um Honeypot.
e) um Proxy SPS.

33. (FCC / ARTESP - 2017) IDS e IPS são recursos de segurança que podem ser posicionados estrategicamente dentro da rede para detectar tráfego malicioso que por ventura tenha passado pelas regras do firewall. O IDS, por exemplo, ao detectar tráfego malicioso,

a) reagirá ao tráfego malicioso isolando os pacotes recebidos em uma área virtual da rede.
b) interromperá o tráfego automaticamente e negará novos pacotes da mesma origem.
c) gerará alarmes e/ou logs.
d) bloqueará a porta de origem do tráfego na rede automaticamente.
e) revidará automaticamente o ataque utilizando DoS.

34. (FCC / ARTESP - 2017) A imagem abaixo mostra a utilização de uma arquitetura com mecanismos apropriados para proteger a rede interna de uma organização.



Na arquitetura mostrada na figura, I é:

a) um cluster, II é um firewall e III é uma DMZ.
b) uma DMZ e II e III são firewalls.
c) um Data Center, II é uma DMZ e III é um firewall.
d) um cluster de servidores e II e III são DMZs.
e) um firewall, II é um IPS e III é um IDS.

35. **(FCC / TRF-1ª Região - 2014)** *Criminosos virtuais costumam varrer a Internet procurando computadores vulneráveis, sem ter alvos específicos para atacar. Aproveitando-se disso, especialistas em segurança criam sistemas que se mostram vulneráveis, atraindo invasores que, quando conectados ao sistema, serão monitorados. Com isso, técnicas, vulnerabilidades e ferramentas são obtidas para análise e proteção dos sistemas.*

(http://g1.globo.com)

O texto trata de uma técnica utilizada para detectar intrusões em uma rede, em que um computador é usado como isca para intrusos. Muitas vezes é colocado na rede de forma que se torna atraente, como estar configurado com um software com vulnerabilidades conhecidas e com seu disco rígido repleto de documentos que aparentam conter segredos da empresa ou outra informação aparentemente valiosa. A técnica descrita é conhecida como:

a) honeybox.
b) mousetrap.
c) honeypot.
d) fakecall.
e) goldenbox.

36. **(FCC / TRT-SP - 2015)** Com respeito à DMZ, do termo em inglês "DeMilitarized Zone", ou seja, "Zona Desmilitarizada" considere:

I. Tem como função manter os serviços que possuem acesso externo separados da rede local, restringindo ao máximo um potencial dano causado por algum invasor, tanto interno como externo.

II. Permite o acesso de usuários externos aos servidores específicos localizados na rede de perímetro e também o acesso deles à rede corporativa interna.

III. Tem como papel principal ser uma rede "tampão" entre as redes externa e interna.

IV. A configuração é realizada através do uso de equipamentos de Firewall, que vão realizar o controle de acesso entre ela, a rede local e a Internet.

Está correto o que consta APENAS em:

a) II.
b) I, III e IV.
c) II, III e IV.
d) I e II.
e) I e III.

37. **(FCC / TJ-AP - 2014)** Um dos dispositivos utilizados em rede de computadores para aumentar a segurança é o Firewall, que é instalado na fronteira da rede local com a rede ampla. Na estrutura de um Firewall que possui a DMZ, pode ser encontrado, dentro da DMZ, um servidor:

a) LDAP.
b) de páginas Web públicas.
c) Proxy.
d) de backup de arquivos privados.
e) DHCP.

38. **(FCC / TRE-CE - 2012)** A sub-rede, também conhecida como rede de perímetro, utilizada para transmitir informações entre uma rede confiável e uma não confiável, mantendo os serviços que possuem acesso externo separados da rede local, é chamada de:

a) proxy.
b) VPN.
c) firewall.
d) DMZ.
e) intranet.

39. **(FCC / TRT-RO e AC - 2011)** No ambiente de rede da empresa, é uma região que pode ser acessada tanto por uma rede interna quanto pela pública (internet) e que servidores nela presentes não podem acessar os computadores internos da empresa por questões de segurança. Trata-se de:

a) FTP.
b) DMZ.
c) DNS.
d) DTD.
e) SMS.

40. **(FCC / TRT-MS - 2011)** É uma pequena rede situada entre uma rede confiável e uma não confiável, ou seja, mantém a rede local separada de todos os serviços que possuem acesso externo:

a) VPN (Virtual Private Network).
b) DMZ (DeMilitarized Zone).
c) VNC (Virtual Network Computing).
d) CSG (Citrix Secure Gateway).
e) SWG (Secure Web Gateway).

41. **(FCC / TRE-AM - 2010)** A segurança de perímetro reside na separação do tráfego entre servidores de redes internas e externas e é reforçada por um firewall, que inspeciona os pacotes

e as sessões para determinar o que deve ser transmitido para a rede protegida e/ou a partir dela ou ser descartado. É uma característica:

a) DMZ.
b) CSG.
c) IPsec.
d) ATM.
e) VPN.

42. (FCC / TER-MS - 2007) Uma DMZ - Zona Desmilitarizada - é um segmento de rede parcialmente protegido que para possibilitar maior segurança na Internet deve estar associada ao mecanismo de proteção:

a) Plano de contingência.
b) Proxy.
c) Criptografia.
d) Firewall.
e) Sistema de detecção de intrusão.

LISTA DE QUESTÕES – FGV

43. **(FGV / BANESTES - 2018)** Um ataque de negação de serviço a uma instituição foi detectado pelo sistema de proteção instalado, que colocou automaticamente regras de proteção para evitá-lo. Pode-se concluir que o sistema de proteção usado é do tipo:

a) IDS
b) IPS
c) EPP
d) DLP
e) DNSSEC

44. **(FGV / MPOG - 2013)** Um analista de segurança precisa detectar preventivamente ataques a uma determinada subrede, realizando contramedidas de forma automática. O instrumento mais adequado a realizar essa função é um:

a) IDS;
b) Firewall;
c) IPS;
d) Proxy;
e) Filtro de pacotes.

LISTA DE QUESTÕES – VUNESP

45. **(VUNESP / EMPLASA – 2014)** Existem diversos recursos que podem ser utilizados para aumentar a segurança em sistemas de informação. Para detectar as invasões nesses sistemas, pode-se utilizar um IDS (Sistema de Detecção de Intrusão) ou o recurso denominado:

a) trap.
b) bridge.
c) switch.
d) gateway.
e) honeypot.

46. **(VUNESP / CORENSP - 2013)** No contexto de sistemas de detecção de intrusão, um honeypot é:

a) uma aplicação que facilita o acesso não autorizado aos servidores de produção.
b) o nome dado ao servidor principal de uma empresa, isto é, aquele que atacantes procurarão invadir.
c) o canal de comunicação com a rede interna de uma empresa.
d) um servidor falso que expõe vulnerabilidades conhecidas para os atacantes.
e) o banco de dados de uma aplicação.

LISTA DE QUESTÕES – CESGRANRIO

47. **(CESGRANRIO / PETROBRAS - 2004)** As chamadas zonas desmilitarizadas (DMZ) podem ser implementadas a partir de firewalls. Quais dos componentes abaixo, são normalmente encontrados em uma DMZ?

a) Servidores de bancos de dados.
b) Servidores Web para Internet.
c) Servidores DHCP da rede interna.
d) Estações de trabalho de usuários.
e) Sistemas legados.

48. **(CESGRANRIO / PETROBRAS – 2012)** No contexto de rotinas de proteção e segurança, HoneyPot é um(a):

a) antivírus especializado na detecção e remoção de cavalos de Troia.

b) dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

c) programa que recolhe informações sobre um usuário e as transmite pela Internet, sem o conhecimento e o consentimento desse usuário.

d) mecanismo para proteção de informações sigilosas que usa técnicas de criptografia.

e) ferramenta que simula falhas de segurança em um sistema e colhe informações sobre eventuais invasores.

49. **(CESGRANRIO / LIQUIGAS – 2012)** Os mecanismos de segurança da informação proporcionam a implantação de diferentes tipos de controle. Honeypot é exemplo de um recurso que pode implantar segurança por meio de controle:

a) interno
b) lógico
c) restrito
d) biométrico
e) de assinatura digital

LISTA DE QUESTÕES – DIVERSAS BANCAS

50. (CPCON / PREF CUIATÉ-PB - 2019) Em segurança da informação, um IDS pode ser:

a) um sistema de detecção de imagem, que permite recuperar as principais imagens do ataque recebido, permitindo detectar o invasor pela análise das imagens.

b) um software de interrupção de disco, que, mediante algum tipo de ataque, trava completamente o sistema até que o invasor seja detectado, evitando perda de dados.

c) um sistema de detecção de intrusão, que possibilita a coleta e o uso de informações dos diversos tipos de ataques, ajudando na defesa de toda uma infraestrutura de rede.

d) um sistema de detecção de IP, através do qual o servidor de DNS consegue identificar o exato momento em que o ataque ocorreu e o IP do computador do atacante.

e) um software de apoio aos hackers, que permite instalar aplicativos maliciosos no computador da vítima, roubando senhas e informações pessoais.

51. (QUADRIX / CRESS-GO - 2019) O IDS (Intrusion Detection System) é capaz de monitorar os arquivos de configuração do Windows.

52. (IADES / AL-GO - 2019) Entre esses dois tipos de firewalls, estão um ou mais dispositivos conectados em uma região chamada de rede DMZ (zona desmilitarizada).

STALLINGS, W. Cryptography and network security: principles and practice. Londres: Pearson, 2017. Tradução Livre.

Com relação à rede DMZ, é correto afirmar que geralmente os dispositivos que ficam nela são acessíveis:

a) pela rede externa, mas precisam de algumas proteções.
b) somente pela rede interna, mas precisam de algumas proteções.
c) pela rede externa e não precisam de proteções.
d) somente pela rede interna e não precisam de proteções.
e) somente pela rede DMZ e não precisam de proteções.

53. (IDIB / Prefeitura de Planaltina – GO - 2018) Assinale o dispositivo capaz de prevenir ataques a rede de computador:

a) IDS
b) IPS
c) HIDS

d) NIDS.

54. **(COPESE / Câmara de Palmas-TO – 2018)** Os Potes de Mel (Honeypots) são sistemas projetados para auxiliar no processo de detecção de intrusão em redes e sistemas computacionais. Marque a alternativa que NÃO apresenta uma função desses sistemas:

a) Desviar um atacante do acesso a sistemas críticos.
b) Coletar informações sobre a atividade do atacante.
c) Incentivar o atacante a ficar no sistema por tempo suficiente para que os administradores respondam.
d) Tentar todas as chaves possíveis em uma amostra de texto cifrado até obter tradução que leve a um texto às claras inteligível.

55. **(IBFC / TJ-PE - 2017)** Questionou-se entre a equipe, a diferença básica entre um IPS (Intrusion Prevention System) e um IDS (Intrusion Detection System). Assinale a alternativa que identifica corretamente essa diferença:

a) o IDS possui um papel estritamente passivo, ou seja, não toma ação, enquanto o IPS, por sua vez, possui um papel ativo tomando algum tipo de ação em caso de detecção de algum intruso.

b) o IPS possui um papel estritamente passivo, ou seja, não toma ação, enquanto o IDS, por sua vez, possui um papel ativo tomando algum tipo de ação em caso de detecção de algum intruso.

c) tanto o IPS como o IDS possuem o papel ativo sempre tomando algum tipo de ação em caso de detecção de algum intruso.

d) tanto o IPS como o IDS possuem o papel passivo, com a única diferença principal que o IDS fica conectado junto a um firewall.

e) não se pode dizer que o IPS e o IDS sejam ativos ou passivos pois os mesmos são considerados como equipamentos de rede com a responsabilidade de criar uma conexão segura e criptografada por meio de tunelamento.

56. **(FAU / E-PARANÁ COMUNICAÇÃO - 2017)** Analise as assertivas e assinale a alternativa que aponta as corretas:

I - A DMZ é uma rede que fica entre a rede interna, que deve ser protegida, e a rede externa.

II - Os proxies são sistemas que atuam como um gateway entre duas redes, permitindo as requisições dos usuários internos e as respostas dessas requisições, de acordo com a política de segurança definida.

III - O Firewall é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego.

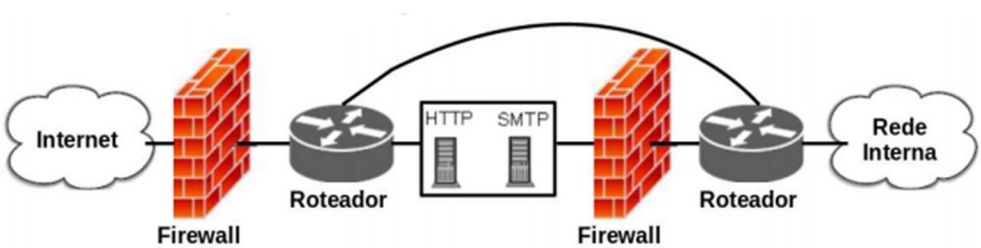
a) Apenas a afirmativa I.
b) Apenas a afirmativa II.
c) Apenas as afirmativas II e III.
d) Apenas as afirmativas I e III.
e) Todas as afirmativas estão corretas.

57. (COSEAC / UFF - 2017) O ambiente criado para proteger a rede interna por meio de um perímetro de segurança, localizado entre a Internet e a rede interna e normalmente acoplado a um firewall, é:

a) Network Address Translation (NAT).
b) Sistema de Detecção de Intrusos (IDS).
c) Zona Desmilitarizada (DMZ).
d) Sistema de Prevenção de Intrusos (IPS).
e) Pote de Mel (Honeypot).

58. (IF-PE / IF-PE - 2016) Os profissionais de tecnologia da informação encarregados de administrar os serviços Web e de rede do IFPE necessitam manter-se atualizados e atentos para implantar estratégias com o objetivo de aumentar a segurança da rede Institucional. Considerando esse contexto, analise o projeto de rede apresentado na FIGURA 02, assinalando a única alternativa CORRETA.

FIGURA 02 (exemplo de um projeto de rede)



a) Os servidores de HTTP e SMTP estão implantados em uma DMZ com o objetivo de oferecer maior segurança à LAN em caso de comprometimento de um desses serviços por um invasor.

b) Esse projeto de rede é ideal para empresas que precisem garantir máxima segurança para sua rede interna, uma vez que os dispositivos dela não possuem conexão com a Internet.

c) Um dos pontos negativos dessa solução é que o servidor HTTP não pode ser acessado pelos dispositivos alocados na rede interna.

d) Estão contemplados nesse projeto de rede um servidor Web e um sistema de gerenciamento de banco de dados.

e) Os servidores de HTTP e SMTP estão oferecendo serviços de DNS com o objetivo de oferecer maior segurança à rede local ao converter os endereços IP externos em internos para a rede local.

59. **(IESES / BAHIAGÁS - 2016)** Escolha a melhor alternativa que defina o que é uma DMZ (Demilitarized Zone ou Zona Desmilitarizada):

a) É um local físico da empresa que é utilizado para o armazenamento de todos os equipamentos de informática.

b) É uma área lógica da rede na qual, geralmente, são colocados os servidores e serviços que estarão publicamente disponíveis na internet. Geralmente é protegida por algum mecanismo de segurança, como firewall.

c) É a área mais segura do datacenter, onde somente o administrador da empresa tem acesso.

d) É uma área física ou lógica da rede onde devem sempre ser colocados os serviços acessíveis somente internamente na empresa. Usualmente não é protegida por mecanismos de segurança, como firewalls.

e) O principal objetivo de uma DMZ é aumentar a velocidade de acesso às páginas WEB hospedadas na nuvem.

60. **(FAUEL / CISMEPAR-PR - 2016)** No contexto de segurança de redes de computadores, o que é um falso-positivo?

a) Um evento real não detectado pelo IDS.
b) Um evento real detectado pelo IDS.
c) Um evento não real detectado pelo IDS como real.
d) Um evento não real não detectado pelo IDS.

61. **(IBFC / EBSERH – 2016)** Ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o(s) invasor(es):

a) Ahwatukee
b) CalaBash
c) BeggingBbowl
d) HoneyPot
e) CucurBit

62. **(OBJETIVA / SESCOOP - 2015)** Dentre os conceitos de firewall, a zona desmilitarizada (DMZ) corresponde a:

a) Uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável.
b) Um tipo de firewall do tipo stateful.
c) Uma área insegura que permite a incidência de ataques.
d) Uma área composta de serviços de filtragem do mais alto nível.

63. (UNIRIO / UNIRIO - 2014) Os serviços indicados para serem abrigados na rede DMZ de uma instituição são:

a) serviços internos que só podem ser acessados por usuários externos via VPN.
b) serviços internos que nunca devem ser acessados por usuários externos à instituição.
c) serviços que só podem ser acessados por usuários externos à instituição.
d) serviços internos que só podem ser acessados por usuários externos que estejam cadastrados na DMZ.
e) serviços que podem ser publicamente acessados por usuários externos à instituição.

64. (QUADRIX / COREN-BA - 2014) Assinale a alternativa que exibe como a zona desmilitarizada também é conhecida:

a) Firewall.
b) Rede de Contato.
c) Rede de Perímetro.
d) Área de Conflito.
e) Área de Contato.

65. (FUNCAB / MDA – 2014) Uma empresa instalou um sistema de detecção de intrusão baseado em honeypots. Isso significa que nesse sistema:

a) um computador qualquer simula importância, atraindo intrusos para ele, sendo que os atacantes são monitorados ao invadirem.

b) foram instalados pelo menos dois firewalls para realizar varreduras das portas TCP, procurando sinais ICMP externos.

c) um computador monitora todos os e-mails de saídas realizados por funcionários da empresa, tentando identificar e-mail suspeitos.

d) vasculha-se a rede interna, procurando servidores web que estejam instalados em máquinas comuns que não servidores originais.

e) um servidor especial testa as saídas UDPs procurando falhas; se as encontra, informa um firewall para bloqueá-las.

66. **(FUNRIO / MPOG - 2013)** Qual dispositivo usado na segurança de rede que investiga todo pacote que passa por ele, abrindo seu conteúdo e filtrando se necessário?

a) Sistema de exploração de vulnerabilidade.
b) Sistema Firewall.
c) Sistema de detecção de intrusão.
d) Sistema de eliminação de intrusão.
e) Sistema de prevenção de intrusão.

67. **(FMP CONCURSOS / PROCEMPA - 2012)** Em um IDPS, Sistemas de Detecção e Prevenção de Intrusão, as técnicas que são baseadas em comparação de uma atividade (pacote ou entrada em um log de eventos) com uma lista previamente estabelecida, são classificadas como:

a) análise statefull de protocolos.
b) análise de anomalias.
c) análise de assinatura.
d) inspeção profunda de pacotes.
e) inspeção de proxy.

68. **(COMPROV / UFCG – 2012)** O honeypot não é necessariamente um tipo de IDS, porém ele pode ser utilizado para que o administrador de segurança aprenda sobre os ataques realizados contra sua organização, detectando e armazenando todos os tipos de ataques.

69. **(IADES / PG-DF - 2012)** Em situação hipotética, um órgão de segurança do governo está sofrendo um ataque ao seu servidor web. O perito em segurança, responsável por analisar o incidente, tomou a decisão de investigar a ação criminosa em andamento, com o objetivo de estudar o seu comportamento e obter informações sobre as técnicas de ataques utilizadas. Assinale a alternativa adequada a esse tipo de análise:

a) Firewall.
b) Botnet.
c) DMZ.
d) Hijacking.
e) Honeypot.

70. **(AOCP / TCE-PA - 2012)** Em segurança da informação uma DMZ é a sigla para de "DeMilitarized Zone". A função de uma DMZ é:

a) proteger os servidores que acessam a internet contra ataques de serviços invasores.
b) determinar um perímetro de segurança para o acesso a redes militares de computadores por civis.
c) manter todos os serviços que possuem acesso externo separados da rede local.
d) manter todo o funcionamento da rede de computadores, mesmo após uma invasão.
e) assegurar que as redes militares não sejam invadidas por crackers.

71. **(FUNIVERSA / SEPLAG-DF - 2010)** Um IPS (Intrusion Prevention System), de forma geral, é um equipamento auxiliar no gerenciamento e segurança da rede, instalado em determinado ponto de passagem de tráfego de uma rede de computadores. Assinale a alternativa que apresenta apenas funções que podem ser realizadas por um IPS:

a) Autenticação de usuários e acesso a serviço de mensagens eletrônicas (e-mail).
b) Cadastro de usuários da rede e controle de acesso a recursos locais.
c) Detecção de ataque DDoS e controle de uso de banda por aplicação.
d) Armazenamento de backups e controle de acesso a banco de dados.
e) Filtro de pacotes, por aplicação, e hospedagem de sites Web.

72. **(IDIB / TRE-AL - 2004)** Um dos mecanismos utilizados pelos sistemas detectores de intrusão (IDS - Intrusion Detection System) é a detecção por assinatura, em que a assinatura típica de um tráfego malicioso permite identificá-lo como um ataque a computador.

GABARITO

1. ERRADO
2. CORRETO
3. ERRADO
4. CORRETO
5. ERRADO
6. ERRADO
7. CORRETO
8. ERRADO
9. CORRETO
10. CORRETO
11. ERRADO
12. CORRETO
13. LETRA E
14. CORRETO
15. CORRETO
16. ERRADO
17. CORRETO
18. ERRADO
19. ERRADO
20. CORRETO
21. ERRADO
22. ERRADO
23. ERRADO
24. ERRADO
25. ANULADA
26. ERRADO
27. ERRADO
28. CORRETO
29. ERRADO
30. CORRETO
31. ERRADO
32. LETRA C
33. LETRA C
34. LETRA B
35. LETRA C
36. LETRA B
37. LETRA B
38. LETRA D
39. LETRA B
40. LETRA B
41. LETRA A
42. LETRA D
43. LETRA B
44. LETRA C
45. LETRA E
46. LETRA D
47. LETRA B
48. LETRA E
49. LETRA B
50. LETRA C
51. CORRETO
52. LETRA A
53. LETRA B
54. LETRA D
55. LETRA A
56. LETRA E
57. LETRA C
58. LETRA A
59. LETRA B
60. LETRA C
61. LETRA D
62. LETRA A
63. LETRA E
64. LETRA C
65. LETRA A
66. LETRA E
67. LETRA C
68. CORRETO
69. LETRA E
70. LETRA C
71. LETRA C
72. CORRETO

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.