05

Porta de segurança com endereço MAC

Transcrição

[00:00] Tínhamos falado pro nosso funcionário que essa porta fastEthernet 0/1 aceita somente um único dispositivo. Explicamos pra ele e ele entendeu tudo. Na semana seguinte, ele está estudando também pra prova do CCNA de segurança, tem uma curiosidade sobre essa área e decidiu instalar uns softwares pra fazer os testes de vulnerabilidades em um sistema.

[00:25] Ele vai instalar esses softwares no notebook dele e ele vai tentar conectar o notebook dele nesse nosso switch que está na nossa rede de produção. Ele vem aqui e tenta conectar esse notebook dele em uma porta do switch.

[00:40] Mas nós, como administradores de rede, já havíamos previsto que como uma boa prática de segurança, sempre desabilitar as portas que não estão sendo utilizadas. Então ao tentar conectar esse notebook em uma das portas do switch, essa porta vai estar desabilitada e o nosso usuário não teria sucesso.

[01:01] Mas ele vai lembrar do que explicamos pra ele. Tínhamos falado que essa porta fastEthernet 0/1 aceita somente um dispositivo. Ele vai vir aqui, simplesmente desconectar esse cabo que está indo pro PC 0, e vai o quê? Ele vai conectar o notebook nessa porta fastEthernet 0/1. Porque, nós como administradores de rede, tínhamos falado pra ele que essa porta fastEthernet 0/1 só aceita um dispositivo.

[01:32] Então, teoricamente nesse nosso cenário nós temos somente um dispositivo, um computador conectado nessa porta fastEthernet 0/1. Não estamos tendo, na teoria, nenhuma violação de segurança com o que tínhamos configurado nessa porta fastEthernet 0/1.

[01:50] Vamos só ver como é que essa porta vai se comportar nesse caso? Vou vir aqui nesse notebook e vamos inicialmente configurar um endereço IP pra ele. Eu vou colocar 192.168.0.3 e vamos tentar estabelecer a comunicação desse notebook com esse computador PC 1, pra ver como é que essa porta desse switch vai se comportar.

[02:12] Vou vir no Command Prompt e eu vou digitar o comando "ping 192.168.0.2" e veja lá a comunicação entre esse notebook do nosso funcionário, que tem esses softwares pra fazer teste de vulnerabilidade, ele conseguiu se comunicar com o chamado computador PC 1. Então não estamos tendo nenhuma violação da segurança que tínhamos configurado. Nós havíamos configurado pra essa porta fastEthernet 0/1 aceitar um dispositivo e aqui somente temos um dispositivo, então está tudo ok.

[02:46] Mas, pensando nisso temos que ter um pouco mais de cuidado, porque eu não quero que essa porta fastEthernet 0/1 aceite qualquer dispositivo, queremos que ela aceite somente o PC 0. Então, como que um switch consegue diferenciar um equipamento de outro equipamento? É através dos endereços físicos, os endereços MAC de cada equipamento, de cada dispositivo.

[03:13] Quando um equipamento de rede vem do fabricante, ele vai ter esse endereço MAC e esse endereço MAC é o endereço único do dispositivo. Não tem dois dispositivos com o mesmo endereço MAC. Então, vamos colocar que essa porta desse meu switch, a fastEthernet 0/1, deve estar vinculada com somente o endereço MAC desse meu PC 0, porque a partir daí vamos vincular que essa porta só vai aceitar os dados que vierem desse meu PC 0. Então, vamos fazer isso. Vou só apagar aqui o que eu tinha feito.

[03:46] Temos que vir no nosso switch e novamente temos que subir até o nível de configuração dessa interface fastEthernet 0/1. Colocamos o comando "enable" pra entrar no modo privilegiado. E colocamos o comando "configure terminal" pra ele entrar no modo de configuração global. E entramos na interface fastEthernet 0/1.

[04:13] Só que não podemos esquecer que essa porta fastEthernet 0/1 nós já configuramos com uma política de segurança, que era aquele modo pra no máximo um dispositivo. Então, eu tenho que retirar esse comando, eu tenho que remover esse comando, essa política de segurança que tínhamos criado, porque eu quero alterar essa política de segurança pra outra política, pra ela aceitar somente o endereço MAC do PC 0.

[04:38] Como eu quero remover aquela configuração de segurança que tínhamos feito antes, sempre quando quisermos remover algum comando nos equipamentos da Cisco, vamos vir aqui e colocar o comando "no", que seria não, uma negação. Vamos negar o comando que queremos remover. Eu quero remover aquele comando "switchport port-security". Eu quero remover a segurança da porta desse meu switch, pra que eu possa fazer uma nova configuração.

[05:04] Eu coloco o comando "no" e eu coloco o comando "switchport port-security". E agora quando eu pressiono enter, eu removi toda aquela configuração de segurança da porta que tínhamos feito. Agora, eu tenho que fazer o quê? Eu tenho que habilitar novamente essa segurança da porta pra fazer essa configuração. Então, eu tenho que vir aqui e digitar novamente "switchport port-security".

[05:35] Agora eu habilitei novamente essa porta pra que ela trabalhe com modo de segurança. E agora eu quero mudar aquela forma que tínhamos trabalhado. Antes tínhamos colocado que eu só queria um dispositivo conectado nessa porta, mas agora vamos ser mais específico, eu vou colocar que o switchport port-security, nessa porta fastEthernet 0/1, vai aceitar somente um endereço MAC. Então, eu venho aqui e coloco "mac-address" e o endereço MAC que ela vai aceitar vai ser desse meu computador PC 0.

[06:03] Então, eu clico no PC 0, venho na aba "Config" e eu coloco na aba "FastEthernet", e ela vai aceitar somente o endereço MAC desse meu dispositivo. Então eu venho, copio o endereço MAC desse meu computador, venho pra cá e eu falo que essa porta desse meu switch vai aceitar somente esse endereço MAC. Agora habilitamos essa porta pra só aceitar o endereço MAC do PC 0.

[06:30] Vamos comparar os endereços MAC dos dois. Vou colocar do PC 0 aqui na direita, e esse é o endereço MAC do meu laptop, que está conectado na porta. Eu só configurei pra aquela porta fastEthernet 0/1 aceitar esse endereço MAC, eu não a configurei pra aceitar esse endereço MAC da direita.

[06:55] Esperamos que essa porta tenha alguma forma de proteção, porque eu configurei pra ela aceitar um endereço MAC, mas o que está conectado agora é um dispositivo com outro endereço MAC.

[07:07] Vamos ver se essa porta vai atuar como imaginamos? Vamos tentar fazer o teste de conectividade de novo. Temos que o teste anterior tinha sido estabelecido com sucesso. E ele vai vir aqui e digitar "ping 192.168.0.2" e vamos ver o que nós temos: "Request timed out". Olha a nossa porta. A nossa porta desabilitou, por quê? Porque agora estamos transmitindo um dado que não pertence ao endereço MAC que tínhamos configurado nessa porta.

[07:42] Estamos sendo bem mais criterioso agora. Eu não estou aceitando qualquer dispositivo de ser conectado nessa porta fastEthernet 0/1, eu só aceito que essa porta fastEthernet 0/1 tenha conectado o computador PC 0. Então, por padrão, quando eu faço essa conexão com outro dispositivo que não o que eu configurei, a porta da Cisco do switch, por padrão, vai desabilitar essa porta e não vai deixar com que ela siga adiante.

[08:09] O funcionário de novo vai entrar em contato conosco, vai falar que a porta não está funcionando e vamos explicar pra ele que ele não pode conectar outro dispositivo nessa porta, que não o equipamento que estava previamente configurado que, nesse caso aqui, era o PC 0. Então vamos o quê? Vamos habilitar a porta novamente. Vamos aqui habilitar essa porta.

[08:31] Lembrando, como essa porta teve uma violação de segurança, eu tenho primeiro desabilitá-la administrativamente pra que depois eu possa habilitá-la. Eu tenho que desabilitar administrativamente colocando o

comando "shutdown". Perceba que ela coloca aqui administrativamente down. E eu tenho que agora habilitar essa porta colocando o comandinho "no shutdown", e a porta voltou para o status "up".

[08:57] Se eu verificar agora a porta voltou a operar normalmente. E já que explicamos para o funcionário que ele não pode usar outro computador que não o PC 0, ele entendeu e se desculpa e desconecta o notebook dele e ele volta a conexão pro computador do PC 0, na porta fastEthernet 0/1. E vamos ver se a comunicação ainda está sendo feita com sucesso, porque o PC 0 foi o endereço MAC que tínhamos configurado no switch pra que fosse aceito.

[09:32] Vamos ver se a política de segurança está sendo feita e está deixando com que esse computador realmente transmita os dados. Testamos com outro computador, o Laptop 4 aqui e não tivemos sucesso. Vamos ver se temos sucesso com esse PC 0. Vamos só esperar alguns segundos pra porta carregar, ela carregou.

[09:51] Vamos na aba "Desktop", Command Prompt e vamos fazer o teste. Eu só vou ver se ele está com o endereço IP, está sim. Eu tinha esquecido se tinha colocado endereço IP nele, ele está com endereço IP. Então é "ping 192.168.0.2" e olha lá: essa porta, a fastEthernet 0/1, está aceitando somente os dados desse meu computador do PC 0.

[10:19] Conseguimos ser mais criteriosos nessa nossa proteção das portas. Não estamos permitindo que nessa porta fastEthernet 0/1 seja conectado qualquer dispositivo, eu quero que ela esteja conectada somente com esse dispositivo PC 0. Se algum outro dispositivo conectar, o que a porta vai fazer? Ela vai detectar que teve uma violação de segurança. E, por padrão, quando tem uma violação de segurança, a porta do switch da Cisco vai desabilitar. Vamos seguir.