04

Interface gráfica do NMap

Transcrição

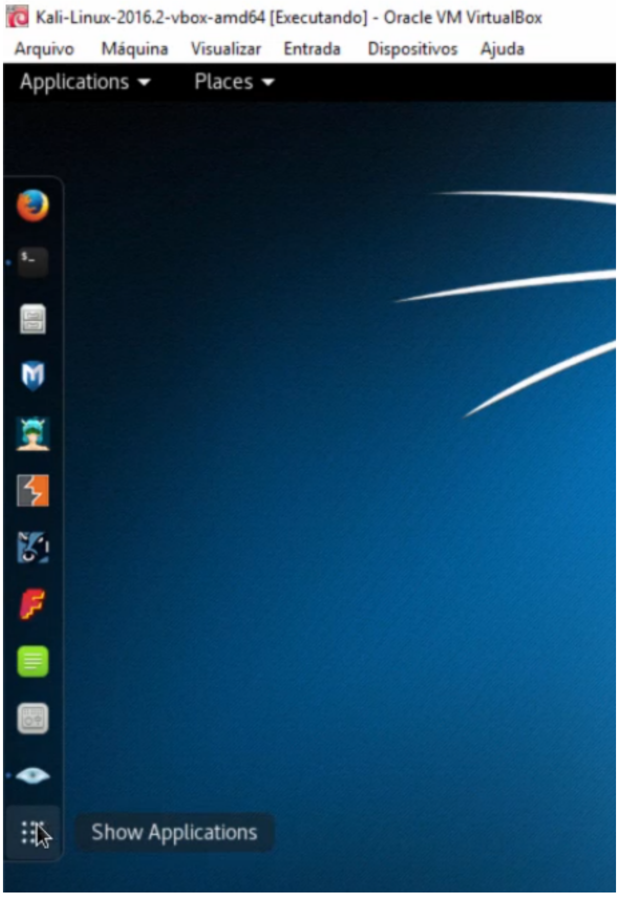
Conseguimos acessar o servidor pela porta `21`, porque sua versão tinha uma vulnerabilidade. Faremos o `nmap` novamente.

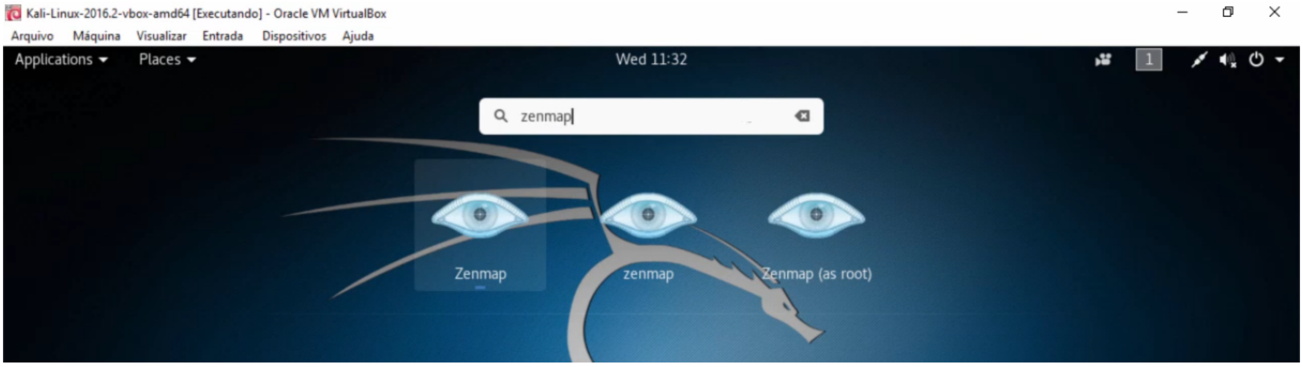
```
root@kali:~# nmap -A 192.168.121.174

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-07 09:48 EST
Nmap scan report for 192.168.121.174
Host is up (0,00053s latency).
Not shown: 978 closed ports
PORT       STATE SERVICE     VERSION
21/tcp      open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymus FTP login allowed (FTP code 230)
22/tcp      open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|   ssh-hostkey:
|       1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_      2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp      open  telnet       Linux telnetd
25/tcp      open  smtp         Postfix smtpd
|_smtp-commands: Metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, EI
| ssk-cert: Subject: commonNome=ubuntu804-base.localdomain/organizationNme=OCOSA/state0rProvinc
...
```

Fica um pouco ruim ver o mapeamento direto no terminal. A análise se torna difícil, pois as portas que estão abertas não são facilmente localizáveis, nem os serviços que estão rodando.

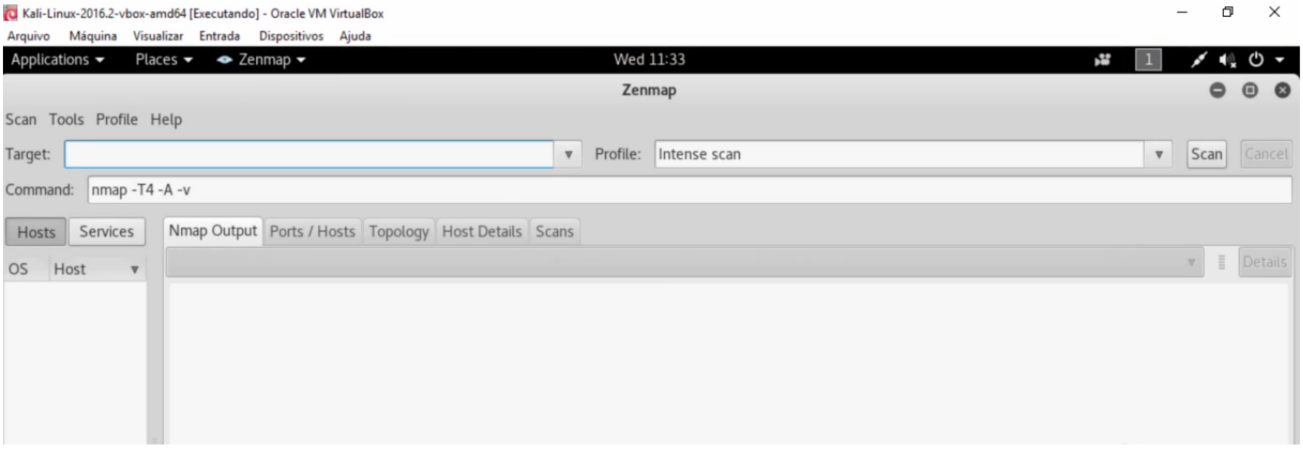
Existe uma interface gráfica do `nmap` chamada Zenmap. Caso você queira saber mais sobre a interface e o funcionamento do Zenmap, o que é recomendável, acesse o [site oficial (https://nmap.org/)](https://nmap.org/).

Clicaremos em `Show Applications` e buscaremos o Zenmap na barra de pesquisa.


Kali-Linux-2016.2-vbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Applications
Places
Show Applications


Kali-Linux-2016.2-vbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Applications
Places
Wed 11:32
zenmap
Zenmap
zenmap
Zenmap (as root)

Ao clicarmos no primeiro ícone, o programa se abrirá.

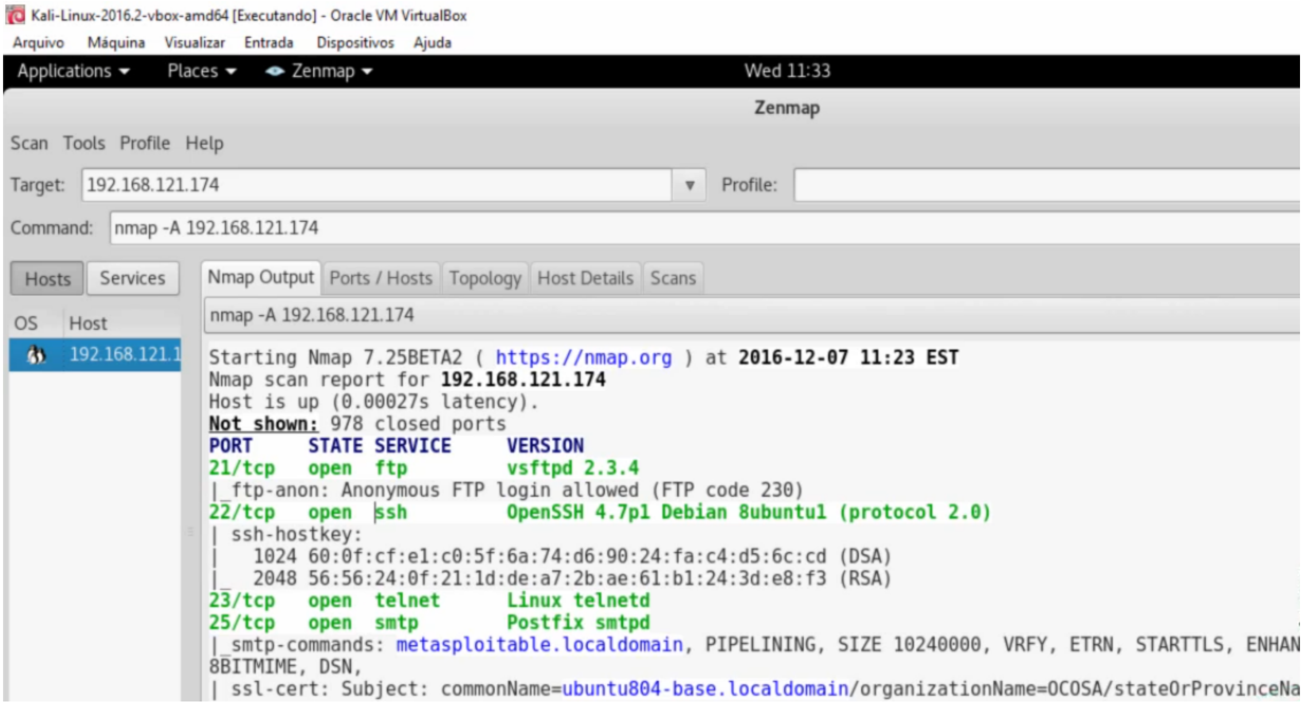


Target:

Profile: Intense scan

Command: nmap -T4 -A -v

No campo `Command`, digitaremos o mesmo comando que usaríamos no terminal: `nmap -A 192.168.121.174`. Assim:


Kali-Linux-2016.2-vbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Applications ▾ Places ▾ Zenmap ▾
Wed 11:33
Zenmap
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
192.168.121.1

Target: 192.168.121.174 Profile:

Command: nmap -A 192.168.121.174

```
nmap -A 192.168.121.174

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-07 11:23 EST
Nmap scan report for 192.168.121.174
Host is up (0.00027s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHAN
8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceNa
```

Agora ficou mais fácil de interpretar os resultados. Analisaremos a porta `22`, cuja linha correspondente diz:

```
22/tcp   open  ssh        OpenSSH 4.7p1   Debian  8ubuntu1  (protocol 2.0)
```

O protocolo `SSH` é utilizado para conexões remotas de equipamentos. Enquanto hackers, podemos pensar se o administrador da rede colocou algum tipo de autenticação para o acesso, ou se qualquer um consegue ter acesso ao servidor. Para descobrir, abriremos um novo terminal. Colocaremos `ssh` seguido do IP do servidor:

```
root@kali:~# ssh 192.168.121.174
```

Ao dar `Enter`, nos depararemos com o seguinte:

```
root@kali:~# ssh 192.168.121.174
root@192.168.121.174's password:
```

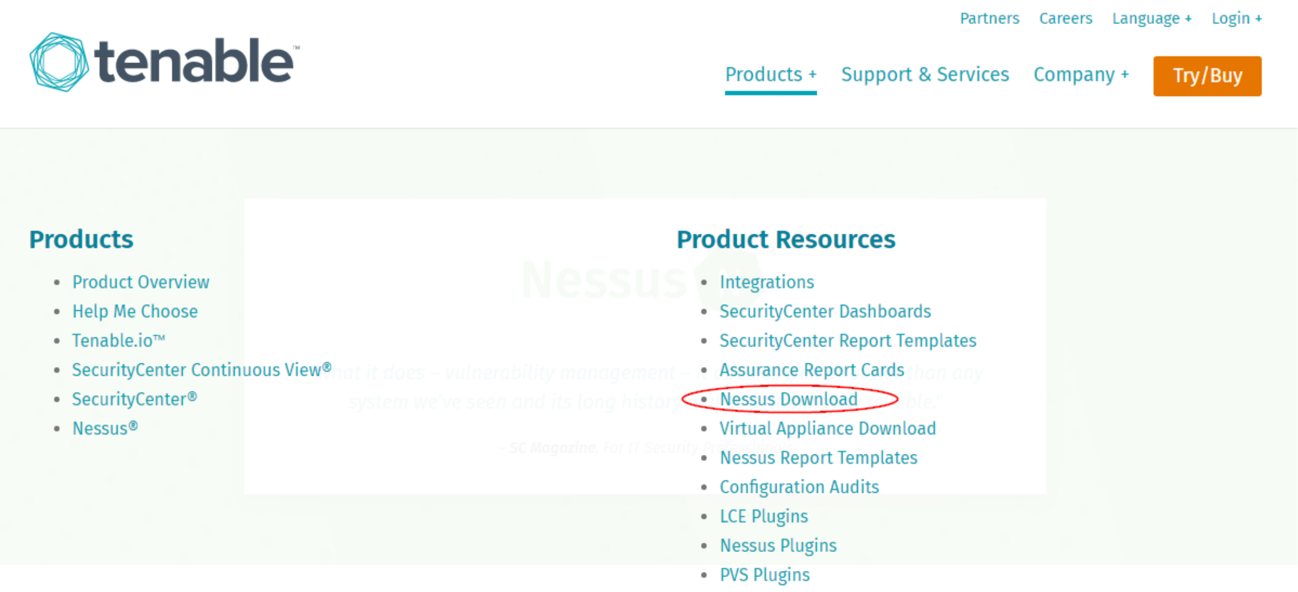
Ele nos pede uma senha. o administrador da rede se preocupou em proteger o acesso remoto ao servidor. É um pouco trabalho ficar conferindo manualmente se cada porta possui uma vulnerabilidade. Seria ótimo se houvesse alguma ferramenta que fizesse isso para nós. E adivinha só... Essa ferramenta existe, e se chama Nessus.

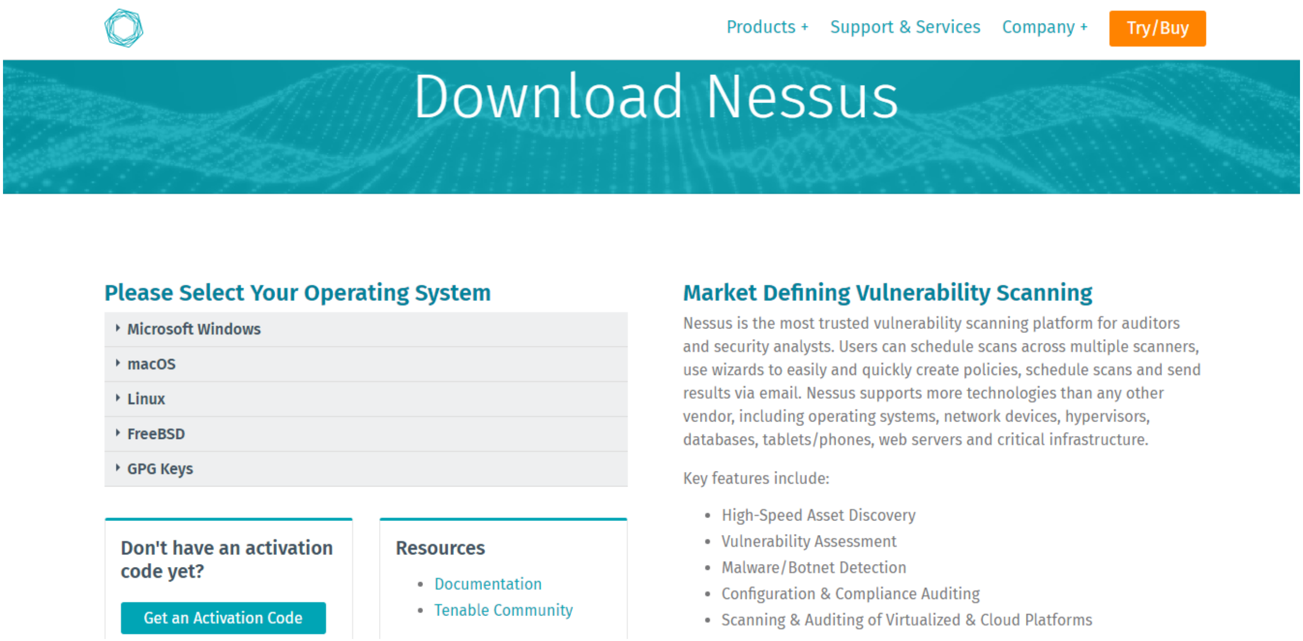
O programa pode ser baixado nesse site (https://www.tenable.com/products/nessus-vulnerability-scanner).

"What it does – vulnerability management – it does as well or better than any system we've seen and its long history makes it completely reliable."

– SC Magazine, For IT Security Professionals

Clicaremos em `Products > Nessus Download`, que nos levará à página de download no Nessus, no qual devemos escolher nosso sistema operacional e suas especificações. O Kali Linux é um Linux 64, portanto, escolheremos a opção correspondente.



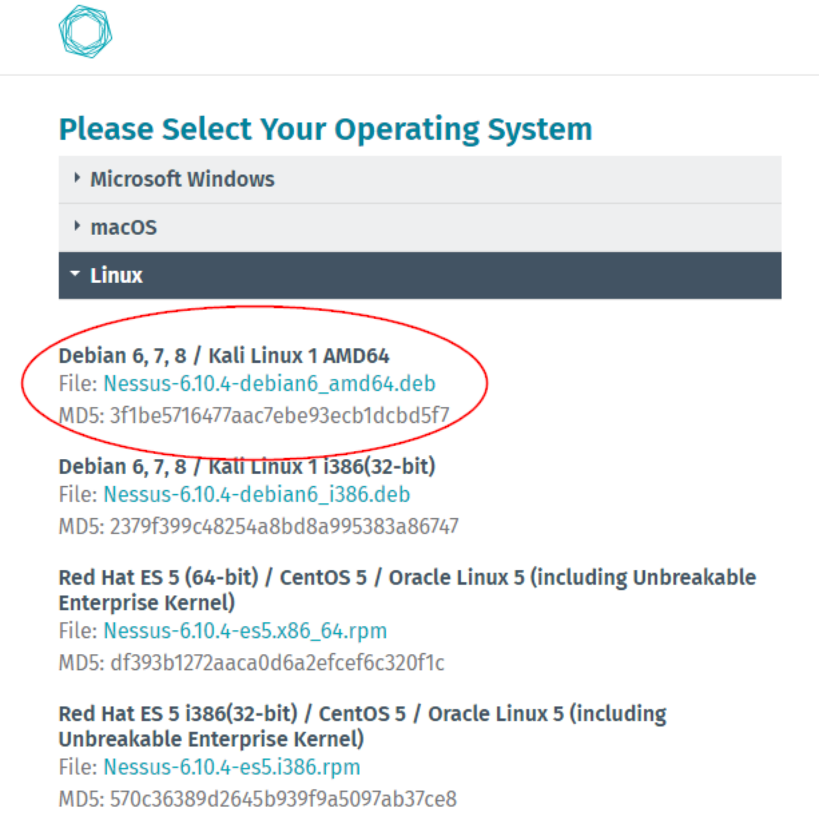


Market Defining Vulnerability Scanning

Nessus is the most trusted vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, use wizards to easily and quickly create policies, schedule scans and send results via email. Nessus supports more technologies than any other vendor, including operating systems, network devices, hypervisors, databases, tablets/phones, web servers and critical infrastructure.

Key features include:

- High-Speed Asset Discovery
- Vulnerability Assessment
- Malware/Botnet Detection
- Configuration & Compliance Auditing
- Scanning & Auditing of Virtualized & Cloud Platforms



Please Select Your Operating System

- Microsoft Windows
- macOS
- Linux

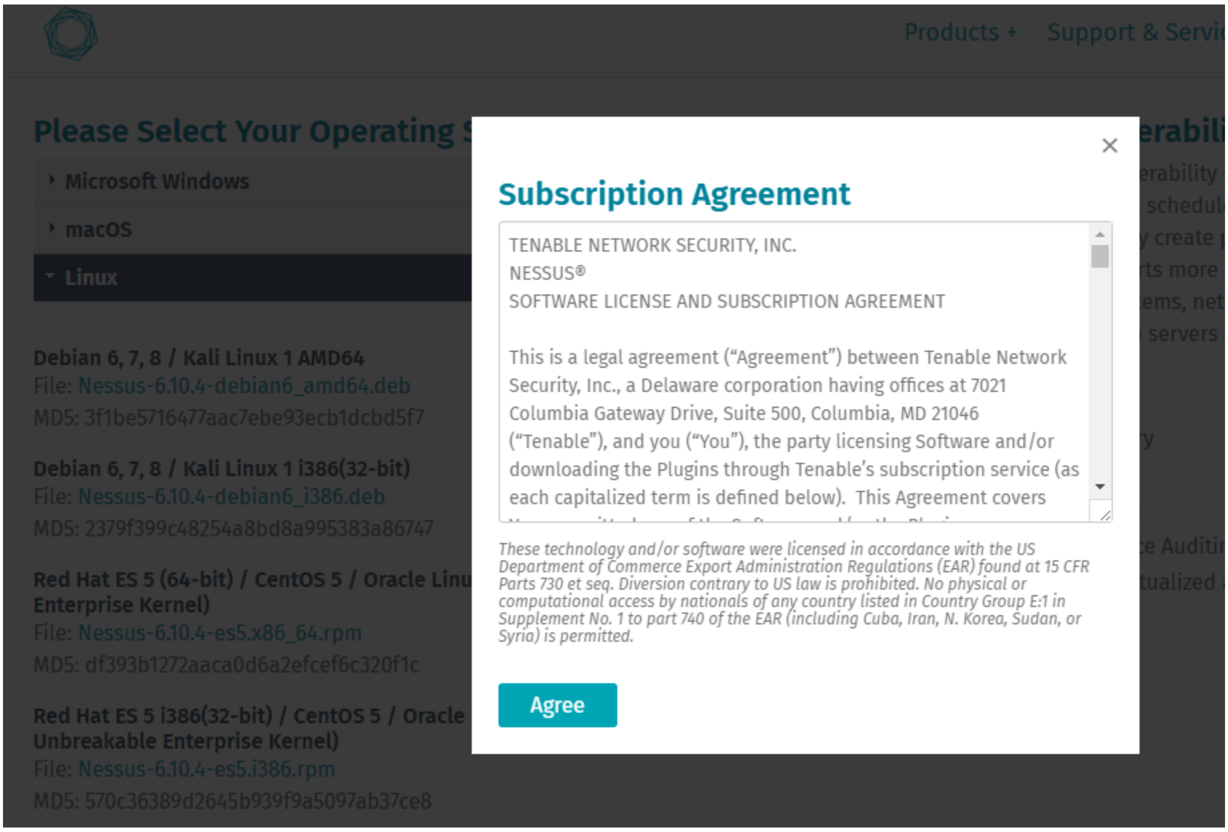
Debian 6, 7, 8 / Kali Linux 1 AMD64
File: Nessus-6.10.4-debian6_amd64.deb
MD5: 3f1be5716477aac7ebe93ecb1dcbd5f7

Debian 6, 7, 8 / Kali Linux 1 i386(32-bit)
File: Nessus-6.10.4-debian6_i386.deb
MD5: 2379f399c48254a8bd8a995383a86747

Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)
File: Nessus-6.10.4-es5.x86_64.rpm
MD5: df393b1272aaca0d6a2efcef6c320f1c

Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)
File: Nessus-6.10.4-es5.i386.rpm
MD5: 570c36389d2645b939f9a5097ab37ce8

Assim que clicarmos para fazer o download, ele pedirá para que você concorde com os termos de uso. O Nessus não deve ser utilizado caso você não tenha permissão para realizar os testes. Não se pode ficar testando a vulnerabilidade de um sistema sem a anuência de seu administrador. Como estamos testando apenas no nosso ambiente controlado, não haverá problema.



Please Select Your Operating S

- Microsoft Windows
- macOS
- Linux

Debian 6, 7, 8 / Kali Linux 1 AMD64
File: Nessus-6.10.4-debian6_amd64.deb
MD5: 3f1be5716477aac7ebe93ecb1dcbd5f7

Debian 6, 7, 8 / Kali Linux 1 i386(32-bit)
File: Nessus-6.10.4-debian6_i386.deb
MD5: 2379f399c48254a8bd8a995383a86747

Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linu
Enterprise Kernel)
File: Nessus-6.10.4-es5.x86_64.rpm
MD5: df393b1272aaca0d6a2efcef6c320f1c

Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle
Unbreakable Enterprise Kernel)
File: Nessus-6.10.4-es5.i386.rpm
MD5: 570c36389d2645b939f9a5097ab37ce8

Subscription Agreement

TENABLE NETWORK SECURITY, INC.
NESSUS®
SOFTWARE LICENSE AND SUBSCRIPTION AGREEMENT

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you ("You"), the party licensing Software and/or downloading the Plugins through Tenable's subscription service (as each capitalized term is defined below). This Agreement covers

These technology and/or software were licensed in accordance with the US Department of Commerce Export Administration Regulations (EAR) found at 15 CFR Parts 730 et seq. Diversion contrary to US law is prohibited. No physical or computational access by nationals of any country listed in Country Group E:1 in Supplement No. 1 to part 740 of the EAR (including Cuba, Iran, N. Korea, Sudan, or Syria) is permitted.

Basta concordar e iniciar o download. Quando ele for concluído, faremos a instalação no terminal. Abriremos o diretório de downloads com o `cd`, e a seguir daremos um `ls` para conferir se o arquivo do Nessus realmente está lá.

```
root@kali:~# Download/
root@kali:~/Downloads# ls
Nessus-6.9.1-debian6_amd64.deb  Nessus-6.9.1-Win32.msi
```

Para instalar, usaremos `dpkg` seguido de `-i` e do nome do arquivo.

```
root@kali:~# Download/
root@kali:~/Downloads# ls
Nessus-6.9.1-debian6_amd64.deb  Nessus-6.9.1-Win32.msi
root@kali:~/Downloads# dpkg -i Nessus-6.9.1-debian6_amd64.deb
Selecting preciouly unselected package nessus.
(Reading database ... 70%
```

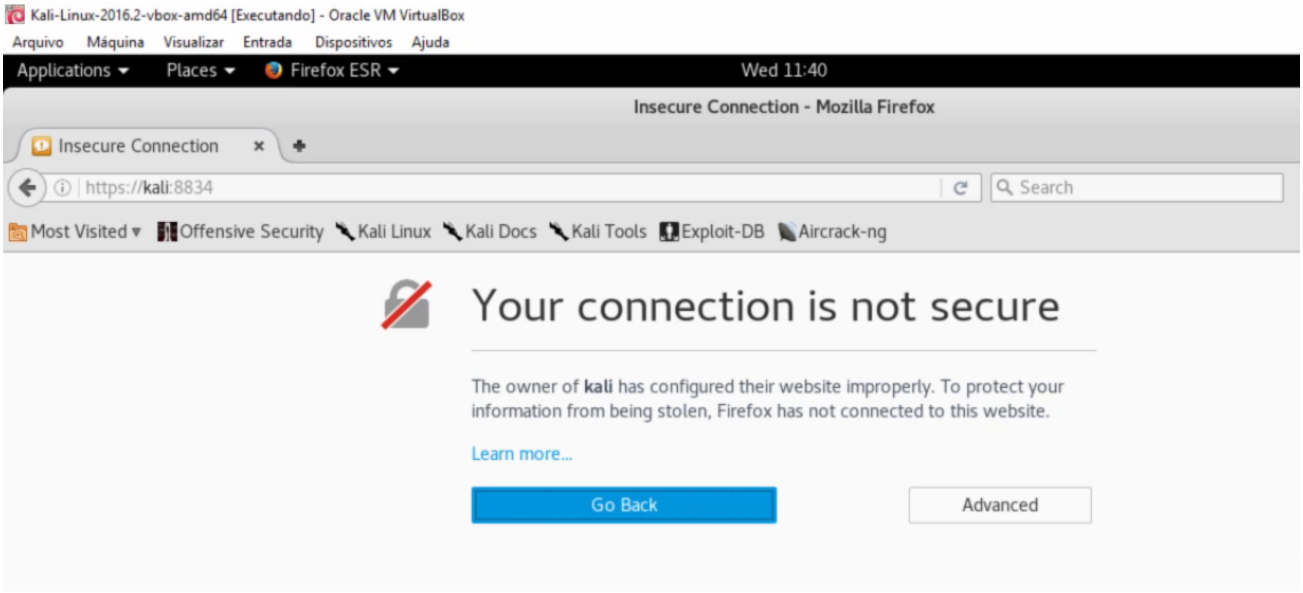
Esperaremos a instalação terminar.

```
root@kali:~# Download/
root@kali:~/Downloads# ls
Nessus-6.9.1-debian6_amd64.deb  Nessus-6.9.1-Win32.msi
root@kali:~/Downloads# dpkg -i Nessus-6.9.1-debian6_amd64.deb
Selecting preciouly unselected package nessus.
(Reading database ... 315154 files and directories currently installed.)
Preparing to unpack Nessus-6.9.1-debian6_amd64.deb ...
Unpacking nesses (6.9.1) ...
Setting up nessus (6.9.1) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.9.1 [build M20071] fo Linux
Copyright (C) 1998 - 2016 Tenable Network Security, Inc

Processing the Nessus plugins...
[##########################################]

All plugins loaded (2sec)

  - You can start Nessus by typing /etc/init.d/nessusd start
  - The go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (231-4) ...
```

Ele nos avisa que podemos iniciar o Nessus com o comando `/etc/init.d/nessusd start` .

```
...
All plugins loaded (2sec)

  - You can start Nessus by typing /etc/init.d/nessusd start
  - The go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (231-4) ...
root@kali:~/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
```

Para inicializar a parte gráfica do Nessus, devemos acessar a URL https://kali:8834/ (https://kali:8834/).

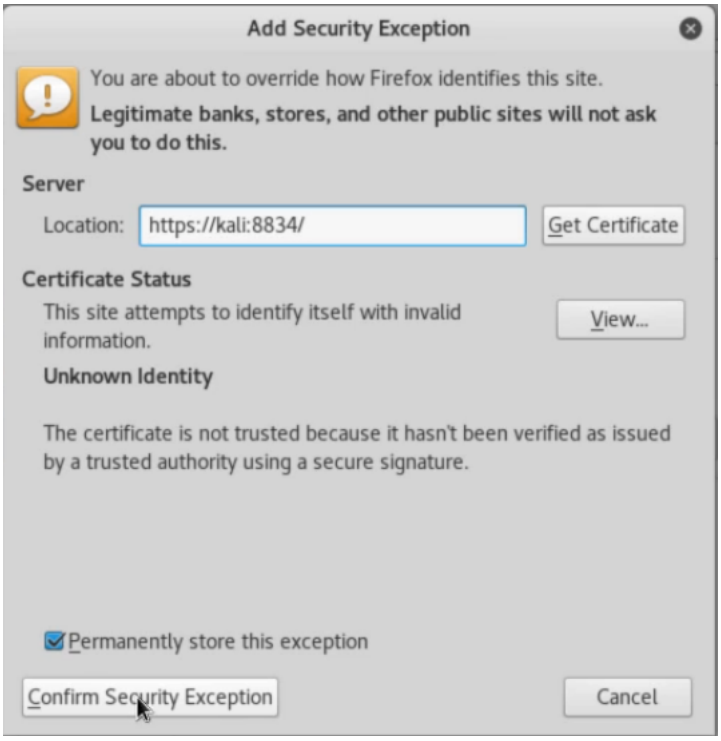

Kali-Linux-2016.2-vbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Applications Places Firefox ESR
Wed 11:40
Insecure Connection - Mozilla Firefox
Insecure Connection
https://kali:8834
Search
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Your connection is not secure

The owner of **kali** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

O navegador nos avisa que esse site não é considerado seguro. Clicaremos em `Add Exception` .



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://kali:8834/

Certificate Status

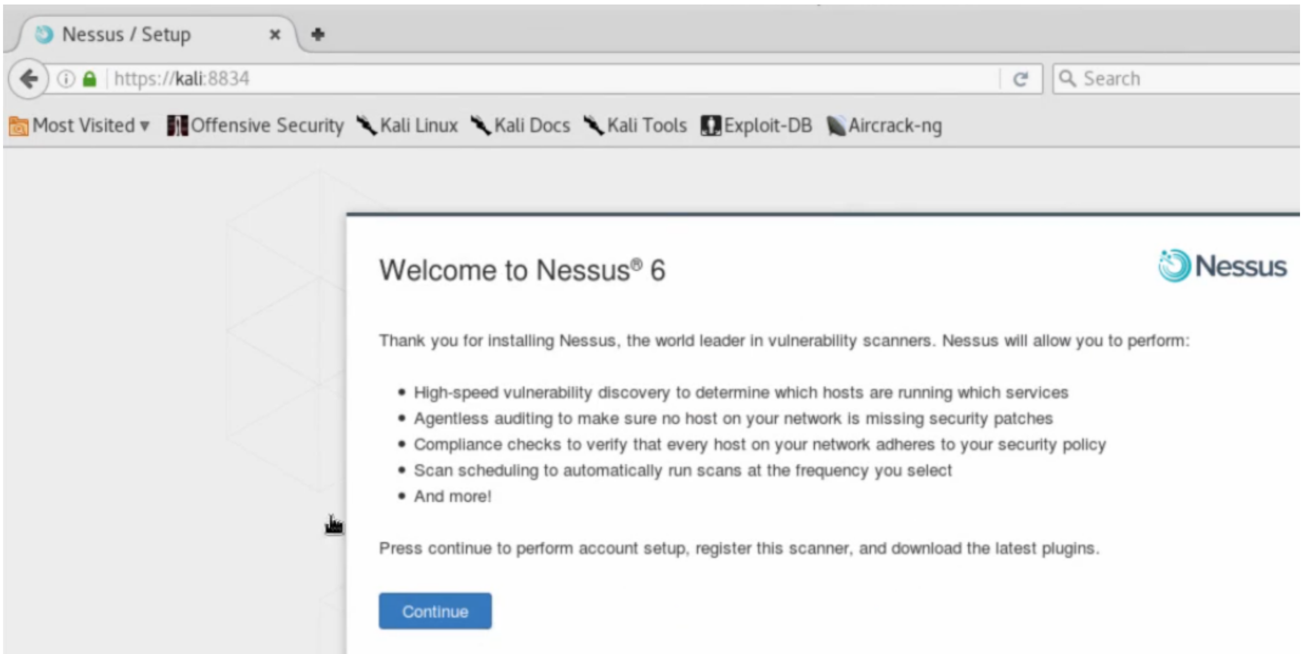
This site attempts to identify itself with invalid information.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

E depois em `Confirm Security Exception` .



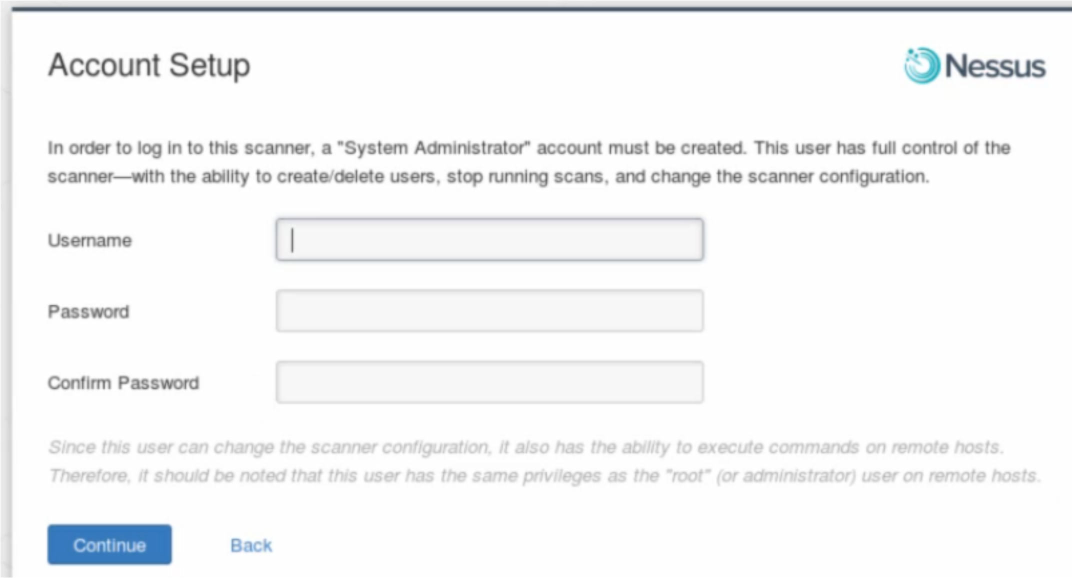
Welcome to Nessus® 6

Thank you for installing Nessus, the world leader in vulnerability scanners. Nessus will allow you to perform:

- High-speed vulnerability discovery to determine which hosts are running which services
- Agentless auditing to make sure no host on your network is missing security patches
- Compliance checks to verify that every host on your network adheres to your security policy
- Scan scheduling to automatically run scans at the frequency you select
- And more!

Press continue to perform account setup, register this scanner, and download the latest plugins.

Clicaremos em `Continue`, o que nos redirecionará para as configurações de conta, nas quais devemos escolher um nome de usuário e uma senha.



Account Setup

In order to log in to this scanner, a "System Administrator" account must be created. This user has full control of the scanner—with the ability to create/delete users, stop running scans, and change the scanner configuration.

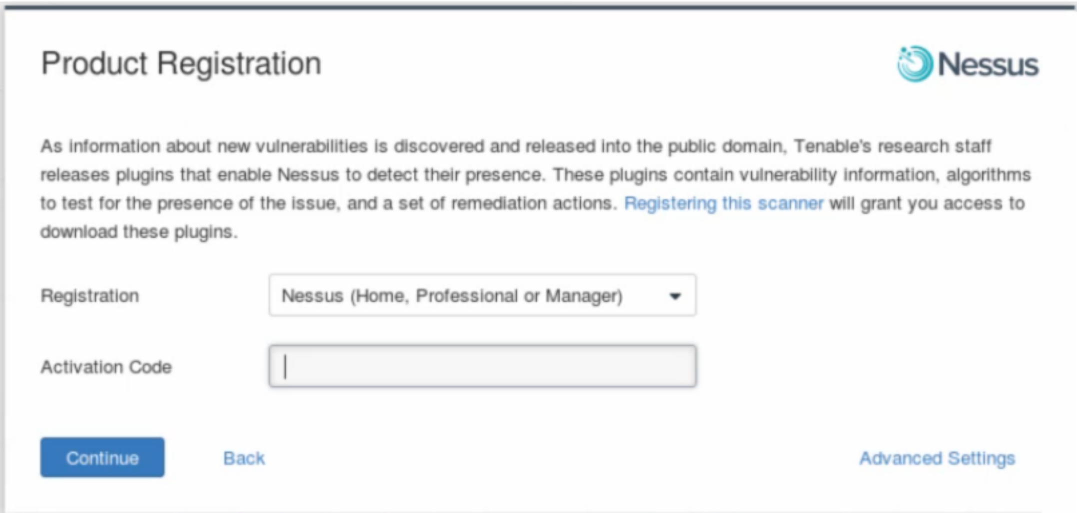
Username

Password

Confirm Password

Since this user can change the scanner configuration, it also has the ability to execute commands on remote hosts. Therefore, it should be noted that this user has the same privileges as the "root" (or administrator) user on remote hosts.

A seguir, devemos inserir o código de registro e selecionar qual tipo desejamos. Escolheremos o `Nessus (Home, Professional or Manager)`.



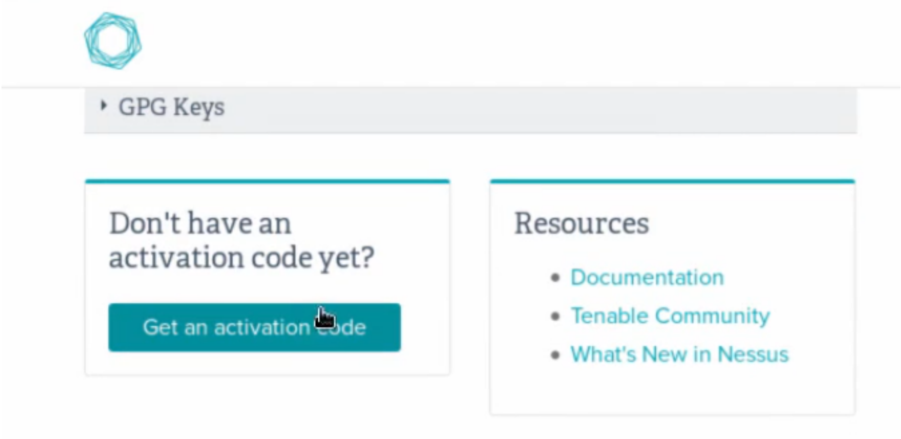
Product Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.

Registration: Nessus (Home, Professional or Manager)

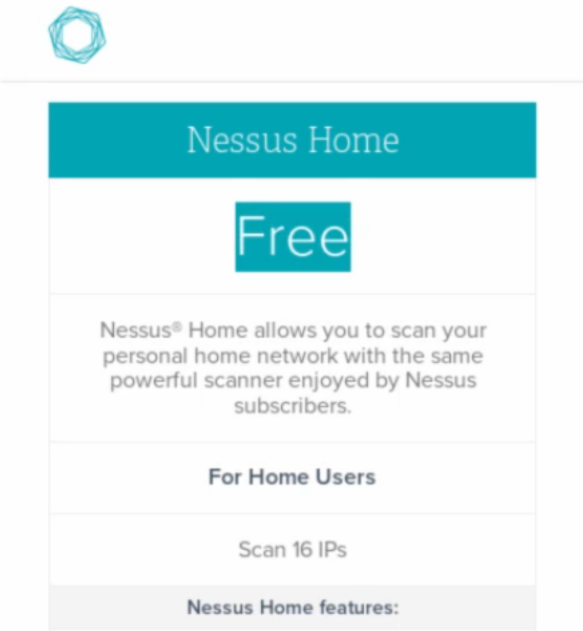
Activation Code

Para obter o código, devemos voltar ao site do Nesses, que possui uma sessão que oferece um código de ativação.



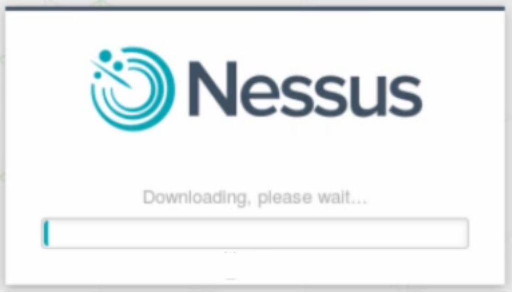
Don't have an activation code yet?

Ela nos direciona para uma página que nos permite escolher o tipo de licença. Escolheremos a versão trial, que é gratuita.



Nessus® Home allows you to scan your personal home network with the same powerful scanner enjoyed by Nessus subscribers.

A seguir, o site pedirá um registro rápido com dados que incluem nome, email e país. O código de ativação será enviado para o email cadastrado.



Downloading, please wait...

Assim que a instalação estiver concluída, continuaremos. Até breve!