

## Tecnologias Hacker

Prof. Dr. Rodolfo Avelino e João Eduardo

### NMAP

Pode ser considerada uma das ferramentas mais completas para realizar varredura em redes, pois disponibiliza um grande número de opções, possibilitando realizarmos diversas varreduras em busca de vulnerabilidades e características do alvo. Essa ferramenta possui, inclusive, opções que permitem burlar sistemas de proteção, como IDS/IPS e Firewall, cujas regras poderiam bloquear ou detectar varreduras não permitidas.

Ela localiza e identifica todas as portas TCP e UDP disponíveis em um host, tentando determinar qual o serviço que está “escutando” em cada porta e é capaz de identificar o tipo de sistema operacional em execução. O nmap é visto como uma ferramenta de segurança, usada para descobrir “brechas” em sistemas, ajudando na tarefa de monitoração e gerenciamento da rede e identificação de serviços rodando em servidores.

Sintaxe:

nmap [Scan Type(s)] [Options] {target specification}

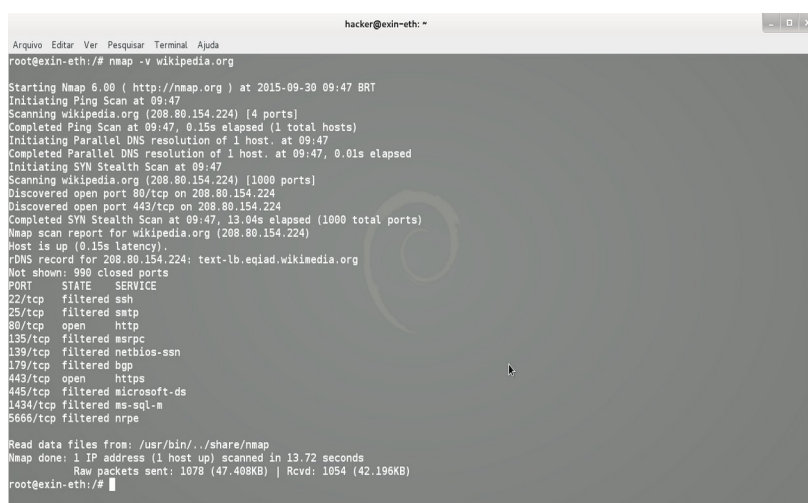
```
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@xin-eth:/# nmap 192.168.0.1

Starting Nmap 6.00 ( http://nmap.org ) at 2015-09-30 10:20 BRT
Nmap scan report for 192.168.0.1
Host is up (0.0020s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
23/tcp    closed telnet
80/tcp    open  http
1900/tcp  open  upnp
8080/tcp  open  http-proxy
MAC Address: CC:00:EC:ED:3F:9D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds
root@xin-eth:/#
```

No exemplo da Figura, ele foi executado de forma simples apenas indicando o IP do alvo. Como resposta é exibido as portas e serviços disponíveis no host.

Usando o modo “verbose” “-v” para exibir mais informações do alvo. Utilize “-vv” para ter uma saída de informações mais detalhadas.



```
hacker@exin-eth:~$ nmap -v wikipedia.org
Starting Nmap 5.00 ( http://nmap.org ) at 2015-09-30 09:47 BRT
Initiating Ping Scan at 09:47
Scanning wikipedia.org (208.80.154.224) [4 ports]
Completed Ping Scan at 09:47, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:47
Completed Parallel DNS resolution of 1 host. at 09:47, 0.01s elapsed
Initiating SYN Stealth Scan at 09:47
Scanning wikipedia.org (208.80.154.224) [1000 ports]
Discovered open port 80/tcp on 208.80.154.224
Discovered open port 443/tcp on 208.80.154.224
Completed SYN Stealth Scan at 09:47, 13.04s elapsed (1000 total ports)
Nmap scan report for wikipedia.org (208.80.154.224)
Host is up (0.15s latency).
rDNS record for 208.80.154.224: text-lb.eqiad.wikimedia.org
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    filtered ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
179/tcp   filtered bgp
443/tcp   open  https
445/tcp   filtered microsoft-ds
1434/tcp  filtered ms-sql-m
5668/tcp  filtered nrpe

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds
Raw packets sent: 1078 (47.408KB) | Rcvd: 1054 (42.196KB)
root@exin-eth:~$
```

Alguns exemplos de comandos nmap:

## Reconhecendo o alvo com o nmap

Primeiramente anote o número IP da máquina alvo fornecido em aula.

Para efeitos de exemplo, vou assumir que o IP da máquina alvo seja **192.168.68.109**. Lembre de alterá-lo para o número de sua máquina quando for executar algum comando.

## Exemplo 1: Descobrindo as portas abertas de um host

Vamos descobrir quais portas de comunicação TCP estão abertas no alvo.

`nmap -sT 192.168.68.109`

```
root@avelino-XPS-13-9350:/# nmap -sT 192.168.68.120
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-29 11:21 -03
Nmap scan report for 192.168.68.120
Host is up (0.00034s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:F1:A5:DE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

A opção “-s” no script é o comando para o escaneamento. Já a opção “T”, indica o escaneamento de portas TCP. Caso for necessário escanear as portas UDP, é alterar o T pelo U.

A saída do comando apresentada na figura apresenta 3 colunas: o número da porta aberta, seu estado e o possível serviço que está sendo executado nesta porta.

## Estado das portas

**Aberta (open)** - está ativamente aceitando conexões TCP ou pacotes UDP nesta porta;

**Fechado (closed)** - Uma porta fechada está acessível (ela recebe e responde a pacotes de sondagens do Nmap), mas não há nenhuma aplicação ouvindo nela.

**Filtrado (filtered)** - O Nmap não consegue determinar se a porta está aberta porque uma filtragem de pacotes impede que as sondagens alcancem a porta.

## Exemplo 2: Descobrindo as versões dos serviços em execução

Comando:

`nmap -sV 192.168.68.109`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-29 11:32 -03
Nmap scan report for 192.168.68.120
Host is up (0.00044s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F1:A5:DE (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds
```

Observe que na saída do comando é acrescentada uma quarta coluna, onde a versão do serviço em execução é apresentado.

## Exemplo 3: Descobrindo o Sistema Operacional

`nmap -O 192.168.68.109`

```
MAC Address: 08:00:27:F1:A5:DE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

A opção “-O” tenta descobrir qual a versão do sistema operacional do host alvo.

## Exemplo 4: selecionando as portas a serem escaneadas

É possível você uma porta ou várias portas a serem escaneadas. Para isso usamos a opção “-p”. No primeiro exemplo vamos escanear apenas a porta 80. Já no segundo exemplo iremos escanear as portas 445 e 22.

```
nmap -sV -p 80 192.168.68.109
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-29 16:32 -03
Nmap scan report for 192.168.68.120
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:F1:A5:DE (Oracle VirtualBox virtual NIC)
```

```
nmap -sV -p 445,22 192.168.68.109
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:F1:A5:DE (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## Nmap Scripting Engine (NSE)

Oferece um conjunto totalmente novo de recursos e confere uma nova dimensão para o Nmap. Permite que o Nmap conclua uma série de tarefas, incluindo scanning de vulnerabilidades, detecção de backdoors e em alguns casos a exploração de vulnerabilidades.

A seguir serão apresentados alguns exemplos e exercícios para a prática do nmap.

### Para descoberta de vulnerabilidades

```
nmap -sV - --script vuln 192.168.68.109
```

### Encontrar malware ou backdoor

```
nmap -v --script malware 192.168.68.109
```