Comando nmap no Linux (scan de rede)

O Comando nmap no Linux é uma ferramenta poderosa para descobrir as portas abertas em hosts locais ou remotos.

Ele pode ser instalado com qualquer gerenciador de pacotes. Ao contrário das ferramentas netstat, ss e lsof que verificam os sockets ou arquivos em aberto, o nmap faz uma busca por portas em aberto pelo método “tentativa e erro”, tentando se conectar nas portas conhecidas, e se encontra uma aberta, ele verifica qual o tipo de serviço a porta serve.

Usando NMAP para Encontrar Portas Abertas em uma Rede

Para verificar as portas abertas de 1 até 1000:

```
$ nmap localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-23 06:01 -03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000098s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Um pequeno script pode ser escrito para comparar as portas em aberto em relação a um arquivo prévio:

Primeiro deve-se criar o arquivo prévio para servir de comparação no futuro:

```
$ nmap localhost | grep open > original
```

O script abaixo executa o nmap, e compara o resultado com o arquivo “original”. Se houver diferença, um e-mail será enviado:

```
#!/bin/bash
nmap localhost | grep open > atual
diff original atual
if [ $? -eq 0 ]; then
    echo “nada mudou”
else
    mail diego@xyz.com.br < atual
fi
```

Verificar portas reservadas com nmap

A opção “-v” verifica todas as portas TCP reservadas na máquina scanme.nmap.org em modo detalhado:

```
$ nmap -v  scanme.nmap.org

Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:01 -03
Initiating Ping Scan at 22:01
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 22:01, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:01
Completed Parallel DNS resolution of 1 host. at 22:01, 0.02s elapsed
Initiating Connect Scan at 22:01
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 22:01, 1.07s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

Varredura SYN com nmap

A opção “-sS” inicia uma varredura SYN furtiva em cada máquina na rede de tamanho /24 onde o endereço scanme.nmap.org reside.

A opção “-O” determinará qual sistema operacional está sendo executado em cada host que está funcionando. Isso requer privilégios de root devido à varredura SYN e à detecção do sistema operacional:

```
$ sudo nmap -sS -O scanme.nmap.org/24
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:04 -03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.070s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Device type: general purpose|WAP|webcam|firewall|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (91%), Tandberg embedded (86%),
Fortinet Linux 2.6.X (86%), IPFire Linux 2.6.X (85%), Check Point Linux 2.6.X (85%),
Axcient embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:2.4 cpe:/h:tandberg:vcs cpe:/o:fortinet:linux_kernel:2.6
cpe:/o:ipfire:linux:2.6.32 cpe:/o:linux:linux_kernel:2.6.18
Aggressive OS guesses: Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%),
Linux 2.6.32 - 3.0 (90%), Linux 2.6.18 (89%), Linux 3.2 - 3.6 (89%), Linux 2.6.32
(88%), Linux 3.1.9 (88%), Linux 2.6.39 (88%), Linux 2.6.32 - 2.6.33 (88%), Linux 2.6.9
- 2.6.27 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops
(...)
```

Verificar portas específicas com nmap

A opção “-sV” a enumeração do host e uma varredura TCP na primeira metade da subnet 198.116.0.0/16. Isso testa se os sistemas executam SSH (22), DNS (53), POP3 (110) ou IMAP (143) em suas portas padrão ou qualquer coisa na porta 4564. Para qualquer uma dessas portas encontradas abertas, a detecção de versão é usada para determinar qual aplicativo está sendo executado:

```
$ nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:08 -03
Nmap scan report for ip-172-30-0-191.ec2.internal (172.30.0.191)
Host is up (0.00016s latency).
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 7.4 (protocol 2.0)
53/tcp   closed domain
110/tcp  closed pop3
143/tcp  closed imap
4564/tcp closed unknown
(...)
```

Varredura de hosts aleatórios com nmap

Neste exemplo nmap escolhe 100 hosts aleatoriamente e verificar se há servidores web (porta 80). A enumeração do host é desativada com -Pn :

```
$ nmap -v -iR 100 -Pn -p 80
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:11 -03
Initiating Parallel DNS resolution of 10 hosts. at 22:11
Completed Parallel DNS resolution of 10 hosts. at 22:11, 1.20s elapsed
(...)
```

Salvar dados do nmap em XML

Neste exemplo o nmap verifica 4096 IPs para qualquer servidor web (porta 80 – sem fazer ping) e salva a saída no formato XML:

```
$ nmap -Pn -p80 -oX pb-port80scan.xml  216.163.128.20/20
```

Descobre se o alvo usa algum firewall

A opção “-sA” faz a varredura se o host usa algum firewall linux para filtrar pacotes:

```
$ sudo nmap -sA facebook.com
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:29 -03
Nmap scan report for facebook.com (157.240.229.35)
Host is up (0.00055s latency).
rDNS record for 157.240.229.35: edge-star-mini-shv-02-iad3.facebook.com
All 1000 scanned ports on facebook.com (157.240.229.35) are filtered
```

Descobre hosts ligados com varredura de ping

A opção “-sP” faz uma varredura do tipo ping em uma rede:

```
$ nmap -sP 172.30.0.0/24
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:31 -03
Nmap scan report for go.universobh.com.br (172.30.0.30)
Host is up (0.00037s latency).
Nmap scan report for ip-172-30-0-191.ec2.internal (172.30.0.191)
Host is up (0.00035s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 5.04 seconds
```

Essa categoria de varredura nem sempre é eficaz, pois a maioria das redes protege seus hosts de ping.

Varre as possíveis portas abertas

A opção “–open” do nmap mostra as possíveis portas abertas de um host:

```
$ nmap --open google.pt
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:33 -03
Nmap scan report for google.pt (172.217.15.99)
Host is up (0.015s latency).
rDNS record for 172.217.15.99: iad30s21-in-f3.1e100.net
Not shown: 998 filtered ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
```

Teste rápido de portas abertas com nmap

A opção “-T5” faz uma varredura rápida de possíveis portas abertas:

```
$ nmap -T5 facebook.com
Starting Nmap 6.40 ( http://nmap.org ) at 2021-12-08 22:35 -03
Nmap scan report for facebook.com (157.240.229.35)
Host is up (0.00068s latency).
rDNS record for 157.240.229.35: edge-star-mini-shv-02-iad3.facebook.com
Not shown: 996 filtered ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
843/tcp closed unknown
5222/tcp closed xmpp-client
```

Cuidado ao usar o nmap

Cuidado ao executar o nmap em hosts hospedados na Amazon AWS, Google Cloud ou Microsoft Azure, pois eles verificam os logs em seus firewalls de borda para verificar que não há atividade suspeita de “PenTest” em suas redes.