

Tópicos Especiais em Segurança da Informação

TP4 - Varredura (scanning)

Arthur do Prado Labaki

31-05, 2022

GBC 235

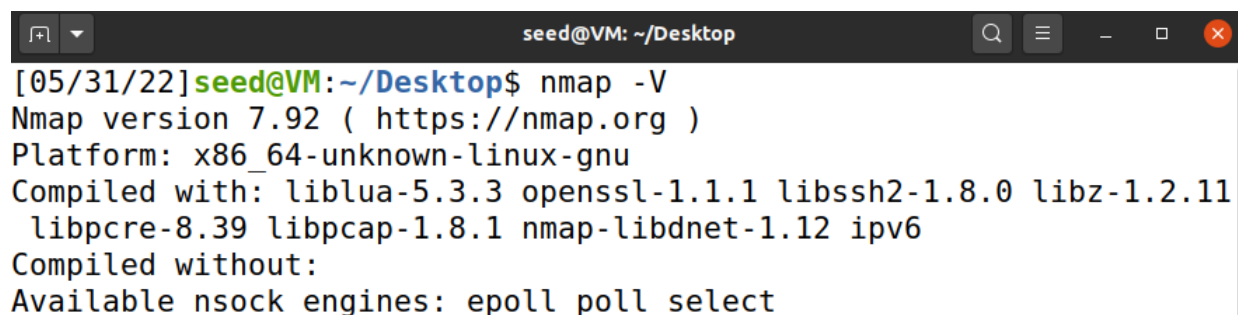
Informações adicionais

Nem todos os exercícios estão com imagem aqui no relatório, mas todas as imagens integradas nesse relatório, quanto códigos, planilhas ou gifs de demonstração estão em meu repositório no github abaixo.

[Link do meu GitHub](#)

Resolução do item 1)

Nmap 7.92 instalado.

A terminal window titled 'seed@VM: ~/Desktop' showing the output of the 'nmap -V' command. The output displays the Nmap version (7.92), platform (x86_64-unknown-linux-gnu), and the libraries it was compiled with and without. The available nsock engines are also listed.

```
[05/31/22]seed@VM:~/Desktop$ nmap -V
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1 libssh2-1.8.0 libz-1.2.11
               libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Figura 1: Versão do Nmap instalado

Resolução do item 2)

Segunda maquina inicializada e ambas podem e conseguem se comunicar.

Resolução do item 3)

Em sua saída é possível ver se o alvo está ativo (UP), a quantidade de portas tcp fechadas (997) e as portas abertas, com seus estados e serviços (21, 22 e 23). Também é possível ver a quantidade de IPs escaneados, nesse caso 1.

```
[05/31/22]seed@VM:~$ nmap 10.0.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 15:04 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

Figura 2: Saída do Nmap da segunda máquina

Resolução do item 4)

A sua saída é semelhante a anterior, sendo que ele traduz o endereço em um IP (rDNS) e mostra as portas abertas (80 e 443).

A diferença entre esse scanner e o do exercício anterior é que o da ufu tem somente duas portas abertas, que são do serviço http, sendo duas aplicações web. Porém o do exercício anterior não tem portas de serviços web, tem portas como ftp, ssh e telnet, que são portar relacionas a o próprio SO, pois foi usado o endereço de uma máquina.

```
[05/31/22]seed@VM:~$ nmap ufu.br
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 15:16 EDT
Nmap scan report for ufu.br (200.19.145.55)
Host is up (0.0031s latency).
rDNS record for 200.19.145.55: bulma.dr.ufu.br
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 278.80 seconds
```

Figura 3: Saída do Nmap do endereço ufu.br

Resolução do item 5)

Etapa 1

O modo verbose (-v) realiza uma descrição detalhada dos passos que o Nmap realiza.

```
[05/31/22]seed@VM:~$ nmap -v ufu.br
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 15:53 EDT
Initiating Ping Scan at 15:53
Scanning ufu.br (200.19.145.55) [2 ports]
Completed Ping Scan at 15:53, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:53
Completed Parallel DNS resolution of 1 host. at 15:53, 0.00s elapsed
Initiating Connect Scan at 15:53
Scanning ufu.br (200.19.145.55) [1000 ports]
Discovered open port 443/tcp on 200.19.145.55
Discovered open port 80/tcp on 200.19.145.55
Connect Scan Timing: About 18.05% done; ETC: 08:33 (13:39:35 remaining)
adjust_timeouts2: packet supposedly had rtt of -10697281974 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -10697281974 microseconds. Ignoring time.
Connect Scan Timing: About 46.80% done; ETC: 22:27 (3:29:14 remaining)
Increasing send delay for 200.19.145.55 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 200.19.145.55 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Completed Connect Scan at 18:58, 11072.86s elapsed (1000 total ports)
Nmap scan report for ufu.br (200.19.145.55)
Host is up (0.0020s latency).
rDNS record for 200.19.145.55: bulma.dr.ufu.br
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Read data files from: /snap/nmap/2629/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11072.96 seconds
```

Figura 4: Saída do Nmap com o modo verbete ativado

Etapa 2

Para varrer um range de portas é utilizado o -p (range). Para o exercício, utilizaremos o -p 0-65535.

Etapa 3

Para o scan nas portas UDP é utilizado o comando -sU.

Etapa 4

Para conseguir identificar o sistema operacional do alvo, é utilizado o comando `-O`. Esse tipo de scan tenta identificar o SO, sendo um palpite, no caso da ufu, pode ser o British Gas embedded, com 92% de certeza.

```
root@VM:/home/seed# nmap -O ufu.br
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 16:35 EDT
Nmap scan report for ufu.br (200.19.145.55)
Host is up (0.00100s latency).
rDNS record for 200.19.145.55: bulma.dr.ufu.br
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: storage-misc
Running (JUST GUESSING): British Gas embedded (92%)
Aggressive OS guesses: British Gas GS-Z3 data logger (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.52 seconds
```

Figura 5: Saída do Nmap com um possível SO

Etapa 5

Saída do nmap está no repositório. O comando realizado foi:

```
nmap -v -p 0-65535 -O ufu.br
```

Resolução do item 6)

Refazendo as buscas para o portalestudante.ufu.br, a etapa 4 como está mostrado na figura 8 e conteúdo do 5 no repositório.

```

root@VM:/home/seed/Desktop# nmap -O www.portalestudante.ufu.br
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-01 20:03 EDT
Nmap scan report for www.portalestudante.ufu.br (200.19.146.67)
Host is up (0.016s latency).
rDNS record for 200.19.146.67: zedd.dr.ufu.br
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc
Running (JUST GUESSING): British Gas embedded (92%)
Aggressive OS guesses: British Gas GS-Z3 data logger (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.14 seconds

```

Figura 6: Saída do Nmap com um possível SO

Resolução do item 7)

```

[06/01/22]seed@VM:~$ nmap serradasaudade.mg.gov.br
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-01 21:35 EDT
Nmap scan report for serradasaudade.mg.gov.br (142.93.252.249)
Host is up (0.15s latency).
rDNS record for 142.93.252.249: servidor.isolucoesweb.com.br
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
8888/tcp  open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 113.29 seconds

```

Figura 7: Saída do Nmap do serradasaudade.mg.gov.br

Etapa 1

É de se notar que sites menores ou do governo não se preocupam com segurança, pois em um servidor web não é seguro ter mais de 10 portas abertas para um site pequeno. Isso

indica o descuido e despreparo que esses sites de cidades menores tem, demonstrando que todo o sistema é falho. É provável que o governo de Minas Gerais, ou o da própria cidade não disponibiliza verba para a segurança do site, provavelmente pois o site é de uma cidade pequena e pouco acessada.

Etapa 2

A coluna *STATE* informa se a porta encontrada está conectada com servers (open), estado desconhecido (unfiltered), sem servers (closed) e portas que não podem ser analisadas por causa de filtros (filtered).

Etapa 3

Com o modo verbose, é possível verificar com mais detalhes os passos do nmap, e também mostra que as portas foram encontradas com muita facilidade, reforçando a ideia do descuido e despreparo.

Resolução do item 8)

Bash script:

```
1 #!/usr/bin/env bash
2
3 arquivo="$1"
4
5 while read cidade; do
6     echo "$cidade"
7     nmap -sS -sU -O -p 0-65535 -Pn -v "$cidade" >> "$cidade".txt
8 done < "$arquivo"
9
10 #Como estava demorando, diminui o comando para
11 nmap -O -p 0-65535 -Pn -v
```

É possível verificar que, quanto menor é a cidade, menor é a segurança do site, e mais

portas desnecessárias estão abertas. Um exemplo seria a de Ribeirão Preto, com uma e Borá com 10 portas abertas, confirmando a afirmação anterior. Existe um problema que dificulta muito investigar esses tipos de site do governo, pois eles sofrem de quedas de servidor muito frequentemente, impedindo de fazer a análise.

Resolução do item 9)

Saídas do nmap está no repositório e a tabela está atualizada. Os serviços mais frequentes encontrados são os http e https, pois a todos as empresas escolhidas tem, de certa forma, uma aplicação web.