GAC119 - REO 1: Levantamento de Dados com Nmap

Mateus Carvalho Gonçalves - 201810245
Pedro Antônio de Souza - 201810557

ANÁLISE 1

Alvo: Roteador wifi utilizado na residência de Mateus

Descrição: A análise do roteador citado acima foi feita com nmap, utilizando a ferramenta GUI de apoio zenmap. O comando utilizado foi `nmap -T4 - O -A -v <ip>` .

Análise: Por meio desse escaneamento foi possível verificar que três serviços estavam abertos: SSH, Telnet e HTTP, conforme a figura abaixo.

	Porta	Protocolo	Estado	Serviço	Versão
✓	22	tcp	open	ssh	Dropbear sshd 2019.78 (protocol 2.0)
✗	23	tcp	filtered	telnet	
✓	80	tcp	open	http	micro_httpd

Pela experiência dos autores, o único serviço que poderia ser desabilitado seria o Telnet. Isso porque o HTTP é a base de comunicação da Internet e o SSH é um protocolo de comunicação seguro, já que ele é criptografado.

Também foi possível obter o endereço MAC da máquina e descobrir o sistema operacional utilizado: Linux. A figura abaixo mostra parte da saída produzida pelo nmap, que diz respeito ao SO.

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.31 - 2.6.35
```

Outra saída interessante produzida pelo nmap é o TCP Sequence Prediction. A dificuldade encontrada foi igual a 202.

ANÁLISE 2

Alvo: Roteador wifi utilizado na residência de Pedro

Descrição: A análise do roteador citado acima foi feita com nmap, utilizando a ferramenta GUI de apoio zenmap. O comando utilizado foi `nmap -T4 - O -A -v <ip>` .

Análise: Ao escanear a máquina, foi possível verificar que sete serviços estavam abertos: FTP, Telnet, "tcpwrapped", HTTP, UPnP e dois serviços NetBIOS. A figura abaixo mostra a relação de portas e serviços.

	Porta	Protocolo	Estado	Serviço	Versão
✓	21	tcp	open	ftp	vsftpd 2.0.8 or later
✓	23	tcp	open	telnet	
✓	53	tcp	open	tcpwrapped	
✓	80	tcp	open	http	
✓	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
✓	445	tcp	open	netbios-ssn	Samba smbd 3.6.25 (workgroup: WORKGROUP)
✓	1900	tcp	open	upnp	Portable SDK for UPnP devices 1.6.19 (Linux 3.10.14; UPnP 1.0)

O FTP pertence ao serviço de armazenamento compartilhado provido pelo roteador. Dessa forma, esse serviço é opcional e pode ser desligado caso seja necessário.

Por sua vez, o Telnet representa um perigo para a rede pois é um protocolo desprovido de criptografia. Portanto, esse protocolo beneficia ataques do tipo man-in-the-middle.

O "tcpwrapped" significa que um programa de controle de acesso à rede está protegendo a porta. Isso significa que o nmap conseguiu completar um handshake TCP sem que o host remoto recebesse nenhum dado.

Já o HTTP, como dito na análise 1, é essencial para a comunicação na Internet.

Os serviços NetBIOS são utilizados para a comunicação entre os computadores da rede local. Contudo, pelo conhecimento limitado dos autores, não sabemos afirmar se esse tipo de serviço é essencial ou representa algum tipo de perigo para a rede.

Por fim, o UPnP é um protocolo que visa facilitar a conexão de dispositivos na rede sem a necessidade de configurações manuais.

Além dos serviços, foi possível obter o endereço MAC e verificar que o sistema operacional utilizado pelo roteador é um Linux. A figura abaixo mostra parte da saída produzida pelo nmap, que diz respeito ao SO.

```
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.13
```

ANÁLISE 3

Alvo: Servidor DNS primário do provedor (Vivo) de Mateus

Descrição: A análise do servidor foi feita com nmap, utilizando a ferramenta GUI de apoio zenmap. Inicialmente, o comando utilizado foi `nmap -T4 - O -A -v <ip>`. Porém o resultado foi que o servidor estava desligado, e completava com a dica de tentar novamente adicionando o parâmetro `-Pn` caso houvesse certeza que o servidor estava ativo.

Análise: Na segunda tentativa, a análise do servidor foi realizável. Entretanto, não foi possível levantar dados sobre ele. O sistema operacional não foi detectado, mesmo após duas tentativas. Também, ao fazer a análise das 1000 portas, o resultado foi de que elas são todas filtradas.

```
Initiating OS detection (try #1) against 187.50.250.115
Retrying OS detection (try #2) against 187.50.250.115
```

```
Nmap scan report for 187.50.250.115
Host is up.
All 1000 scanned ports on 187.50.250.115 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   6.88 ms menuvivofibra (192.168.15.1)
2   ... 30
```

Um detalhe curioso é que o relatório mostrou o roteador analisado no item 1 deste documento, como mostra a figura anterior.

ANÁLISE 4

Alvo: Servidor DNS da Namecheap Inc. (ns1.epizy.com).

Descrição: A análise do servidor foi feita com nmap, utilizando a ferramenta GUI de apoio zenmap. O comando utilizado foi `nmap -T4 - O -A -v <ip>`. Através do site Myip.ms, foi possível descobrir o IP 107.189.11.47 relativo ao domínio do servidor.

Análise: O escaneamento da máquina encontrou dois serviços: um de domínio e um MySQL. A figura abaixo apresenta a relação de portas e serviços encontrados no servidor.

	Porta	Protocolo	Estado	Serviço	Versão
✓	53	tcp	open	domain	PowerDNS Authoritative Server 4.2.3
✓	3306	tcp	open	mysql	

Como esperado, o servidor dispõe de um serviço de domínio para a resolução de nomes. Além disso, também há um servidor MySQL presente na máquina. É provável que esse último serviço seja responsável por armazenar a relação de nomes e IPs.

Não foi possível descobrir o sistema operacional do servidor. Contudo, como pode ser visto na próxima figura, o nmap supôs com 95% de certeza que o SO é Linux 3.10.

```
Aggressive OS guesses: Linux 3.10 - 4.11 (95%), Linux 3.13 (94%),
Linux 3.18 (93%), Linux 3.2 - 4.9 (93%), Linux 3.13 or 4.2 (92%),
Linux 4.10 (92%), Linux 4.2 (92%), Linux 4.4 (92%), Asus RT-AC66U WAP
(92%), Linux 3.10 (92%)
```