



# SEGURANÇA CIBERNÉTICA

PROF. ENG. DANIEL JOSÉ PIMENTA

# ANÁLISE DE VULNERABILIDADES

## Mapeamento de Redes

É o processo de descoberta de hosts ativos, sistemas operacionais utilizados, serviços abertos e tudo que for possível descobrir sobre determinada rede.

Para isso, são utilizadas algumas ferramentas que utilizam protocolos de manipulação de pacotes como *TCP*, *UDP*, *ICMP*.

Atualmente, o mapeamento de redes é parte importante no processo de *Penetration Test*, ou *pentest*, em que profissionais simulam ataques, como um agente malicioso na rede.

O mapeamento de rede é uma das primeiras fases desse processo, para identificar os servidores e aplicações que estão disponíveis na rede.

# ANÁLISE DE VULNERABILIDADES

## *Host Scan*

A primeira fase tem como objetivo descobrir quais são os servidores, máquinas ou dispositivos ligados à rede.

## *Service Scan/OS fingerprint*

*Service Scan/OS fingerprint* objetiva descobrir quais são serviços no servidor e qual o seu sistema operacional.

## *Port Scan*

*Port Scan* tem como objetivo descobrir quais são as portas TCP e UDP abertas nesses servidores.

## *Varredura*

A varredura de vulnerabilidades é a fase de pesquisa que indica quais vulnerabilidades os servidores possuem.



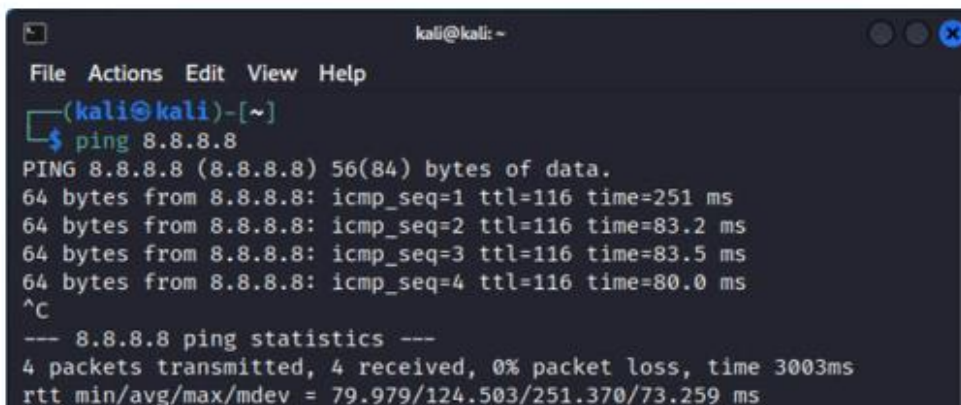
# ANÁLISE DE VULNERABILIDADES

## HOT SCAN PING

O utilitário *ping* é encontrado nativamente na maioria dos sistemas operacionais. Essa ferramenta utiliza o protocolo *ICMP* (*Internet Control Message Protocol* ou, em português, Protocolo de Mensagens de Controle da Internet).

O *ping* envia um pacote de *ICMP Request* para uma máquina. Se a máquina alvo estiver ativa e respondendo pacotes *ICMP*, ela responderá com um pacote *ICMP Reply*.

A execução do *ping* é muito simples e é demonstrada na imagem a seguir.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=251 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=83.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=83.5 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=80.0 ms  
^C  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 79.979/124.503/251.370/73.259 ms
```

# ANÁLISE DE VULNERABILIDADES

## HOT SCAN NMAP

### NMAP

O *nmap* desempenha essa tarefa de uma forma mais completa, testando não apenas pacotes *ICMP* de diferentes tipos, mas também verificando as portas 443 e 80 do protocolo *TCP* (*Transport Layer Protocol*, ou, em português, Protocolo da Camada de Transporte).

O *nmap*, por padrão, primeiro descobre se o *host* está ativo e, caso esteja, executa uma varredura nas mil portas mais utilizadas



# ANÁLISE DE VULNERABILIDADES

## HOT SCAN NMAP

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans

nmap -T4 -A -v www.guiapadreeustaquio.com.br

NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating Ping Scan at 15:16
Scanning www.guiapadreeustaquio.com.br (50.116.87.169) [4 ports]
Completed Ping Scan at 15:16, 2.55s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:16
Completed Parallel DNS resolution of 1 host. at 15:16, 11.46s elapsed
Initiating SYN Stealth Scan at 15:16
Scanning www.guiapadreeustaquio.com.br (50.116.87.169) [1000 ports]
Discovered open port 443/tcp on 50.116.87.169
Discovered open port 995/tcp on 50.116.87.169
Discovered open port 53/tcp on 50.116.87.169
Discovered open port 993/tcp on 50.116.87.169
Discovered open port 21/tcp on 50.116.87.169
Discovered open port 587/tcp on 50.116.87.169
```

# ANÁLISE DE VULNERABILIDADES

## SERVICE SCAN

### SERVICE SCAN

Depois de descobrir quais portas estão abertas nos *hosts*, é importante determinar quais serviços e quais as versões desses serviços. Com a opção *'-sV'*, o *nmap* executa essa varredura.

Nesse método, são enviados pacotes para estabelecer a conexão com o 3-*way handShake* e, em seguida, envia pacotes solicitando informações sobre os serviços

Command: `nmap -sV`

Hosts

Services

Nmap Output

Ports / Hosts





Topology

Host Details

Scans

OS

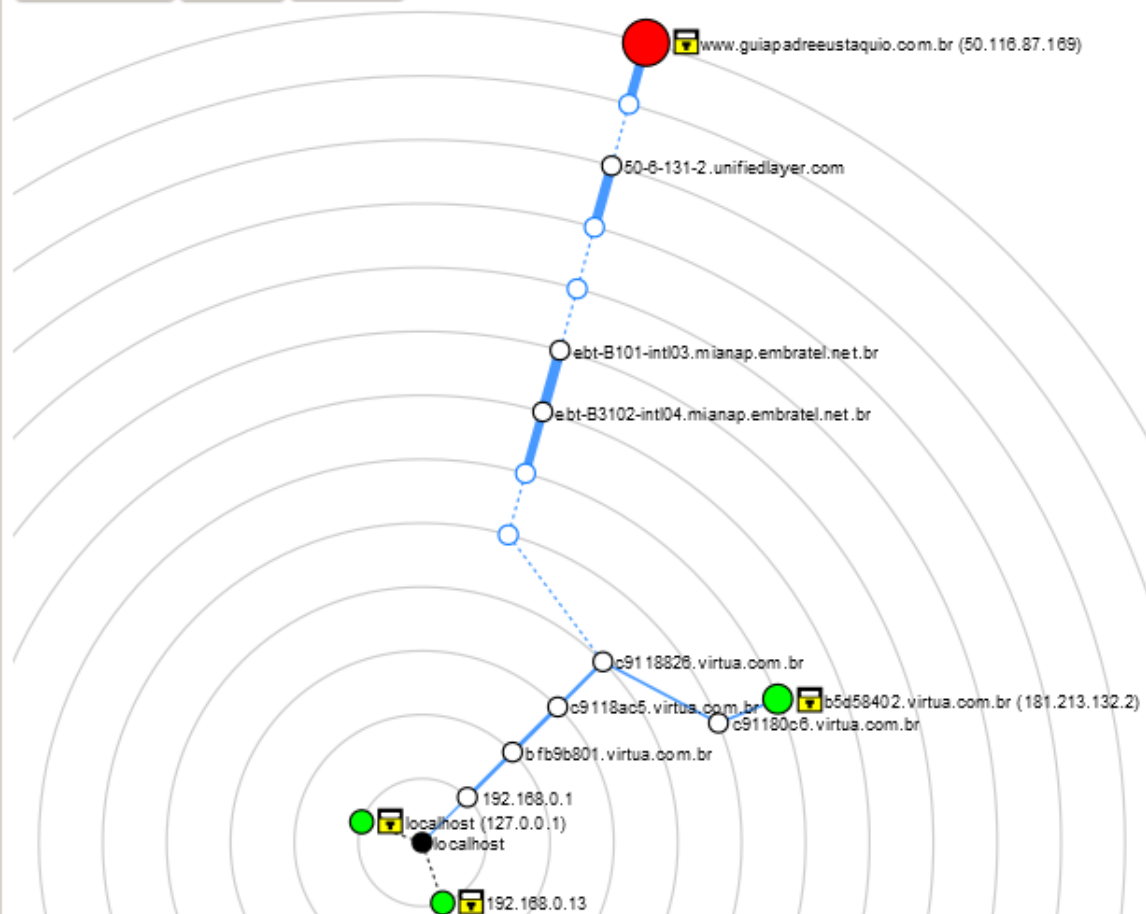
Host

	localhost (127.0.0.1)
	192.168.0.13
	b5d58402.virtua.com.br (181.213.132.2)
	www.guiapadreeustaquio.com

Hosts Viewer

Fisheye

Controls



Filter Hosts



# ANÁLISE DE VULNERABILIDADES

## OS FINGERPRINT

### OS FINGERPRINT

O *nmap* também é capaz de tentar identificar qual é o sistema operacional de determinado servidor. Isso é possível devido a diferentes implementações em relação a redes e serviços em cada sistema operacional.

Cada sistema possui uma definição do valor padrão de *TTL* (*Time to Live*, ou Tempo de Vida) para diferentes protocolos. A tabela a seguir mostra alguns exemplos importantes de *TTL* padrão de *ICMP*.

# ANÁLISE DE VULNERABILIDADES OS FINGERPRINT

Sistema Operacional	TTL padrão
FreeBSD 5	64
Windows 10	128
Linux Kernel 2.4	255

Tabela – TTL de sistemas operacionais no protocolo ICMP.

Fonte: site do subinsb.com

Target:

Profile:

Command:

Hosts

Services

OS	Host
	localhost (127.0.0.1)
	192.168.0.13
	b5d58402.virtua.com.br (181.213.132.2)
	www.guiapadreeσταquιο.com.br (50.116. ...)
	www.guiacaicara.com.br (162.241.203.81)

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

nmap -sV -O www.guiacaicara.com.br

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-09-03 15:44 Hora oficial do Brasil  
Nmap scan report for [www.guiacaicara.com.br](http://www.guiacaicara.com.br) (162.241.203.81)  
Host is up (0.16s latency).  
rDNS record for 162.241.203.81: 162-241-203-81.unifiedlayer.com  
Not shown: 980 closed tcp ports (reset)  

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
22/tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
25/tcp	filtered	smtp	
26/tcp	open	tcpwrapped	
53/tcp	open	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp	open	http	Apache httpd
110/tcp	open	pop3	Dovecot pop3d
135/tcp	filtered	msrpc	
139/tcp	filtered	netbios-ssn	
143/tcp	open	imap	Dovecot imapd
161/tcp	filtered	snmp	
443/tcp	open	ssl/http	Apache httpd
445/tcp	filtered	microsoft-ds	
465/tcp	open	ssl/smtps?	
587/tcp	open	tcpwrapped	
993/tcp	open	ssl/imap	Dovecot imapd
995/tcp	open	ssl/pop3	Dovecot pop3d
1434/tcp	filtered	ms-sql-m	
2222/tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
3306/tcp	open	mysql	MySQL 5.7.23-23

  
Device type: general purpose  
Running (JUST GUESSING): Linux 3.X|2.6.X (87%)  
OS CPE: cpe:/o:linux:linux\_kernel:3.4 cpe:/o:linux:linux\_kernel:2.6.32  
Aggressive OS guesses: Linux 3.4 (87%), Linux 2.6.32 (86%)  
No exact OS matches for host (test conditions non-ideal).  
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise\_linux:7



# ANÁLISE DE VULNERABILIDADES

## VARREDURA

### VARREDURA

O *nmap* possui vários scripts com diferentes funções e categorias. Duas categorias importantes para a descoberta de vulnerabilidades são ***default*** e ***vuln***.

Os *scripts* da categoria **default** são simples, de rápida execução e dão informações básicas sobre os serviços. Para executá-los, pode-se executar o *nmap* com a opção '`-script "default"`' ou com a opção '`-sC`'.

Target:

www.guiacaicara.com.br

▼

Profile:

Command:

nmap www.guiacaicara.com.br -sc

Hosts

Services

OS	Host
	localhost (127.0.0.1)
	192.168.0.13
	b5d58402.virtua.com.br (181.213.132.2)
	www.guiapadreeustaquio.com.br (50.116.10.10)
	www.guiacaicara.com.br (162.241.203.81)

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

	Port	Protocol ▲	State	Service	Version
	21	tcp	open	ftp	Pure-FTPd
	22	tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
	25	tcp	filtered	smtp	
	26	tcp	open	tcpwrapped	
	53	tcp	open	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
	80	tcp	open	http	Apache httpd
	110	tcp	open	pop3	Dovecot pop3d
	135	tcp	filtered	msrpc	
	139	tcp	filtered	netbios-ssn	
	143	tcp	open	imap	Dovecot imapd
	161	tcp	filtered	snmp	
	443	tcp	open	http	Apache httpd
	445	tcp	filtered	microsoft-ds	
	465	tcp	open	smtps	
	587	tcp	open	tcpwrapped	
	993	tcp	open	imap	Dovecot imapd
	995	tcp	open	pop3	Dovecot pop3d
	1434	tcp	filtered	ms-sql-m	
	2222	tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
	3306	tcp	open	mysql	MySQL 5.7.23-23

# ANÁLISE DE VULNERABILIDADES

## VARREDURA

### VARREDURA

Os *scripts* da categoria ***vuln*** buscam, dentro dos serviços selecionados, vulnerabilidades conhecidas e fáceis de identificar, sem explorá-las.

Para executar esses scripts, pode-se utilizar a opção '*—script “vuln”*'.








Command: `nmap --script "vuln"`

Hosts

Services

OS Host

	localhost (127.0.0.1)
	192.168.0.13
	b5d58402.virtua.com.br (181.213.132.2)
	www.guiapadreeustaquio.com.br (50.116.10.10)
	www.guiacaicara.com.br (162.241.203.81)

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

`nmap --script vuln`

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 16:10 Hora oficial do Brasil
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 34.31 seconds
```