

Controle e exploração de vulnerabilidade

Profº Harley Rios

Controle e exploração de vulnerabilidade

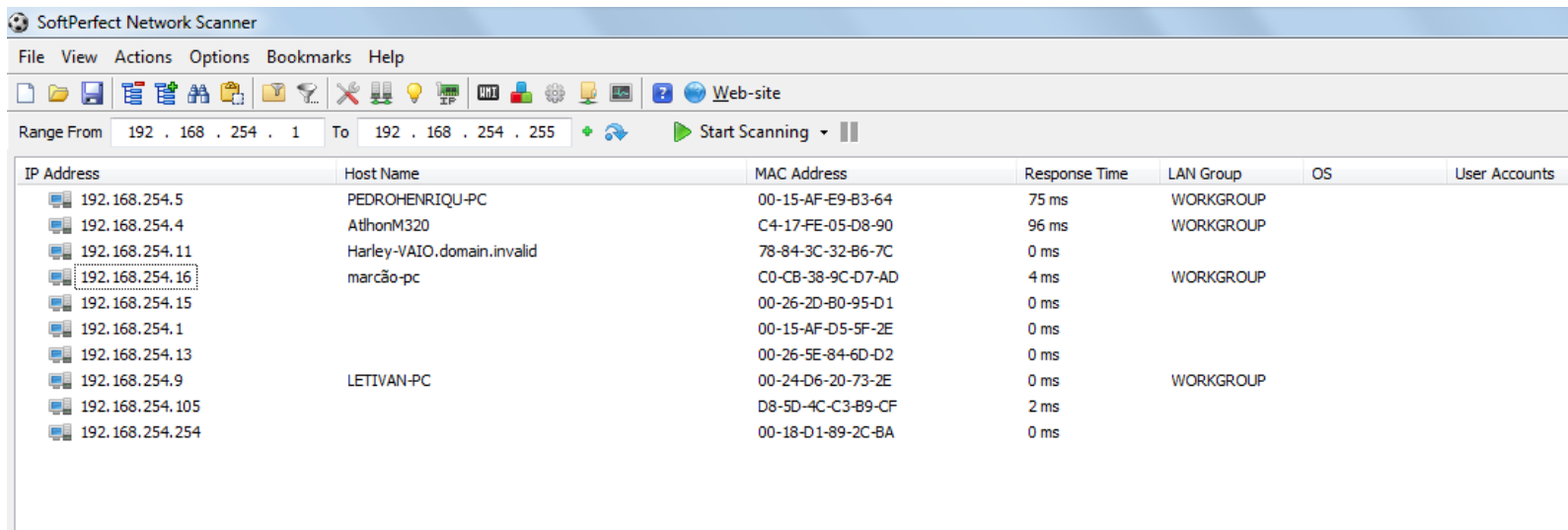
- Varredura em redes, ou scan é uma técnica que consiste em efetuar buscas minuciosas em redes com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados.
- Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

Varredura em redes (*Scan*)

- A varredura em redes e a exploração de vulnerabilidades associadas podem ser usadas de forma:
 - **Legítima:** por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.
 - **Maliciosa:** por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas.
 - Os atacantes também podem utilizar os computadores ativos detectados como potenciais alvos no processo de propagação automática de códigos maliciosos

NetScan

- Ferramenta simples para monitorar rede pública ou privada.



The screenshot shows the SoftPerfect Network Scanner application window. The title bar reads "SoftPerfect Network Scanner". The menu bar includes "File", "View", "Actions", "Options", "Bookmarks", and "Help". The toolbar contains various icons for file operations, network settings, and scanning. Below the toolbar, the "Range From" field is set to "192 . 168 . 254 . 1" and the "To" field is set to "192 . 168 . 254 . 255". A "Start Scanning" button is visible. The main area displays a table of scanned hosts.

IP Address	Host Name	MAC Address	Response Time	LAN Group	OS	User Accounts
192.168.254.5	PEDROHENRIQU-PC	00-15-AF-E9-B3-64	75 ms	WORKGROUP		
192.168.254.4	AthlonM320	C4-17-FE-05-D8-90	96 ms	WORKGROUP		
192.168.254.11	Harley-VAIO.domain.invalid	78-84-3C-32-B6-7C	0 ms			
192.168.254.16	marcão-pc	C0-CB-38-9C-D7-AD	4 ms	WORKGROUP		
192.168.254.15		00-26-2D-80-95-D1	0 ms			
192.168.254.1		00-15-AF-D5-5F-2E	0 ms			
192.168.254.13		00-26-5E-84-6D-D2	0 ms			
192.168.254.9	LETIVAN-PC	00-24-D6-20-73-2E	0 ms	WORKGROUP		
192.168.254.105		D8-5D-4C-C3-B9-CF	2 ms			
192.168.254.254		00-18-D1-89-2C-BA	0 ms			

Free PortScanner

■ Scanner de Portas (Windows)

YOUR PROTECTION IS OUR BUSINESS

[Product Key Explorer - Find over 3000 software product keys from local or remote network computers](#) [Download Now!](#)

[Nsauditor Network Security Auditor - Scan and monitor network for vulnerabilities. Over 45 net tools in one.](#) [Download Now!](#)

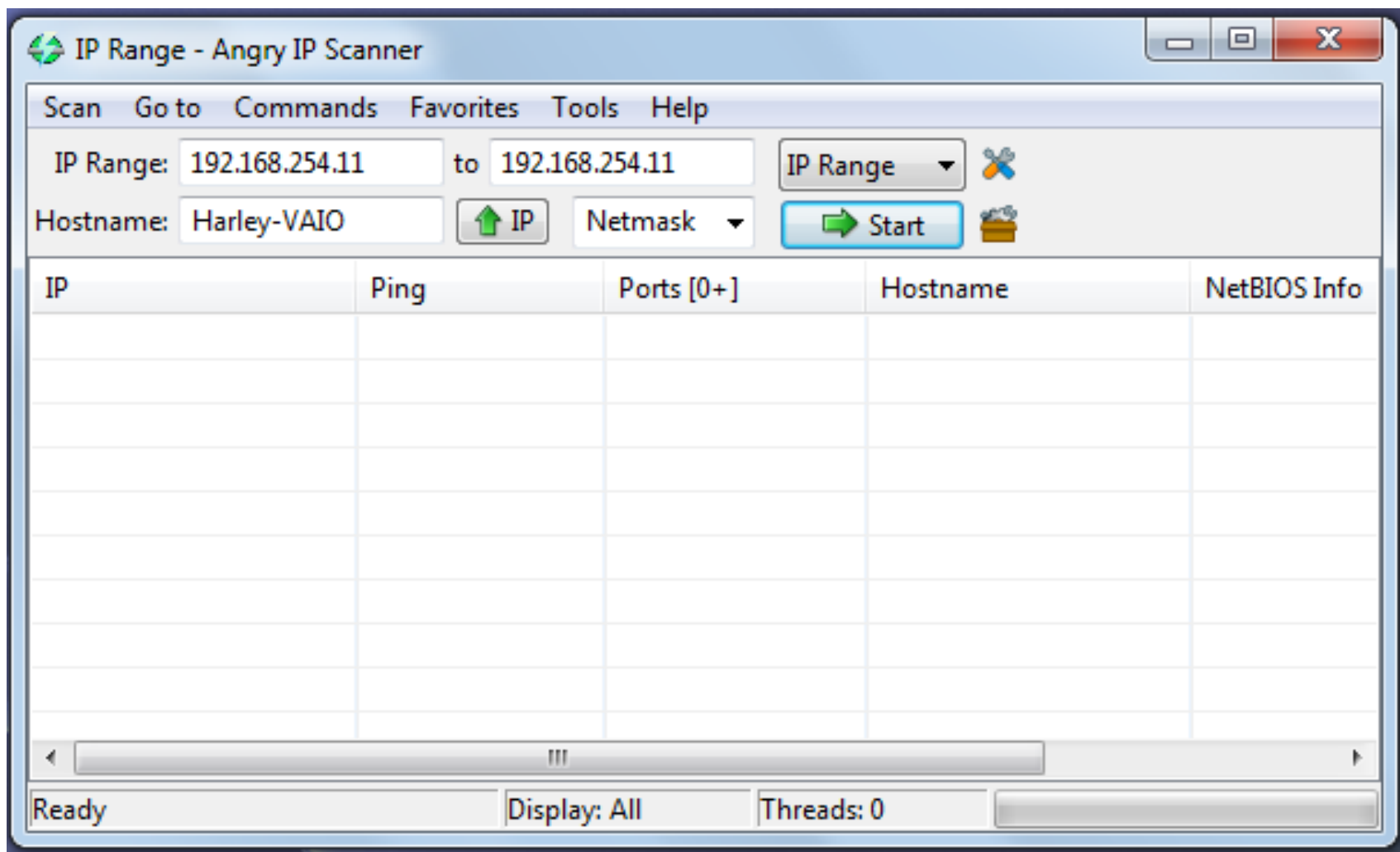
Scan Parameters

IP Address: ☒ Show Closed Ports [Scan](#)

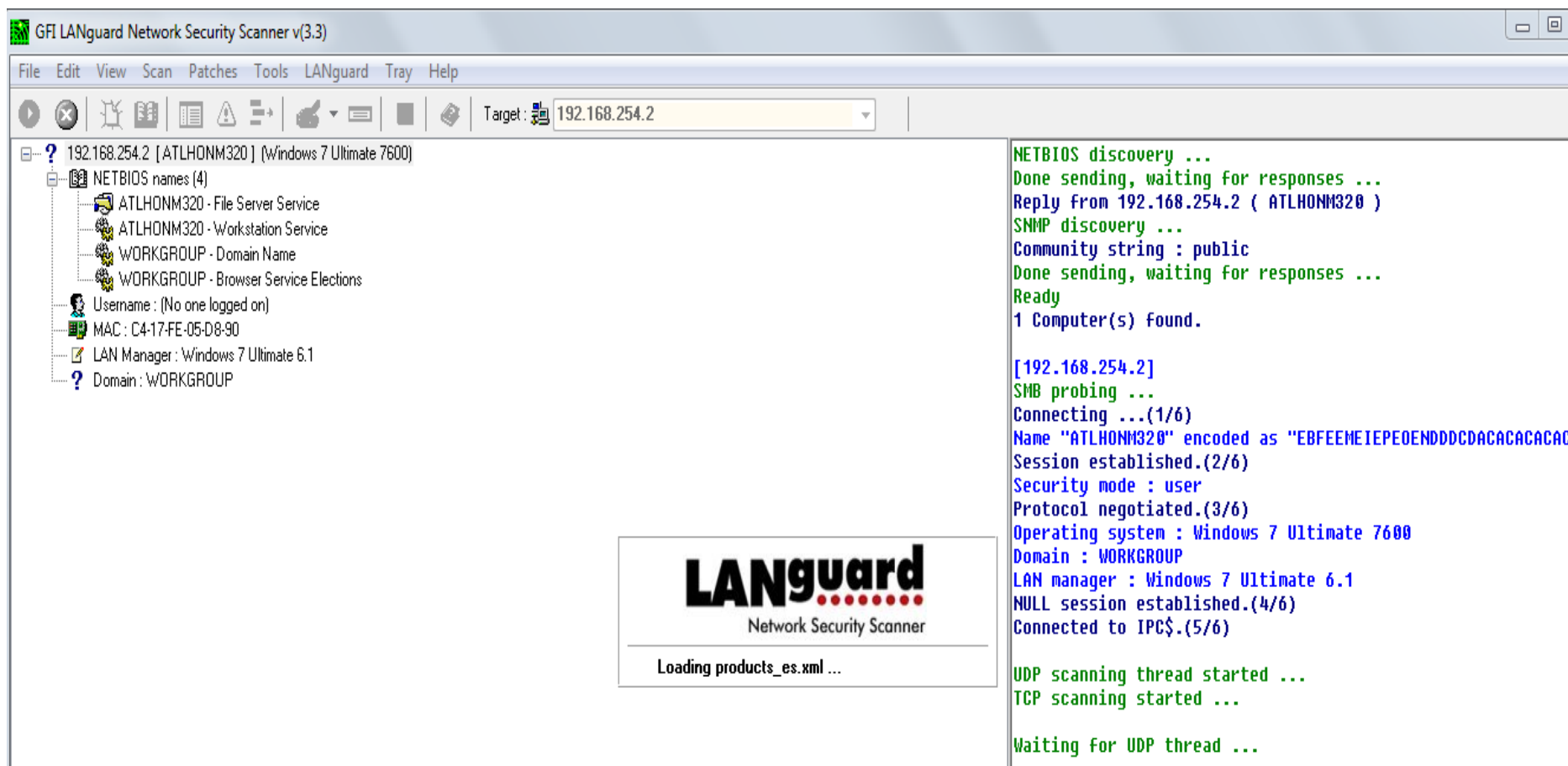
TCP Ports: [Stop](#)

IP address	Port number	Port Status	Port Name	Description
✗ 192.168.254.11	21	Closed	ftp	file
✗ 192.168.254.11	22	Closed	ssh	secure
✗ 192.168.254.11	23	Closed	telnet	telnet
✗ 192.168.254.11	25	Closed	smtp	simple mail transfer
✗ 192.168.254.11	53	Closed	domain	domain name server, name-domain server
✗ 192.168.254.11	80	Closed	http	hypertext transfer protocol, world wide web http
✗ 192.168.254.11	110	Closed	pop3	pop version 3, postoffice v.3, post office, post office p
➡ 192.168.254.11	135	Open	epmap	dce endpoint resolution, location service, ncs local loc
✗ 192.168.254.11	137	Closed	netbios-ns	netbios name service
✗ 192.168.254.11	138	Closed	netbios-dgm	netbios datagram service
➡ 192.168.254.11	139	Open	netbios-ssn	netbios session service
➡ 192.168.254.11	443	Open	https	secure http (ssl), http protocol over tls/ssl
✗ 192.168.254.11	445	Closed	microsoft-ds	microsoft-ds
✗ 192.168.254.11	1080	Closed	socks	socks
✗ 192.168.254.11	1433	Closed	ms-sql-s	microsoft-sql-server
✗ 192.168.254.11	3128	Closed	nd1-aas	Active
✗ 192.168.254.11	3306	Closed	mysql	mysql
✗ 192.168.254.11	8080	Closed	http-alt	common http proxy/second web server port, http alter

IP Range – Angry IP Scanner



LANGUARD



GFI LANguard Network Security Scanner v(3.3)

File Edit View Scan Patches Tools LANguard Tray Help

Target: 192.168.254.2

192.168.254.2 [ATLHONM320] (Windows 7 Ultimate 7600)

- NETBIOS names (4)
 - ATLHONM320 - File Server Service
 - ATLHONM320 - Workstation Service
 - WORKGROUP - Domain Name
 - WORKGROUP - Browser Service Elections
- Username: (No one logged on)
- MAC: C4-17-FE-05-D8-90
- LAN Manager: Windows 7 Ultimate 6.1
- Domain: WORKGROUP

LANGuard
Network Security Scanner

Loading products_es.xml ...

NETBIOS discovery ...
Done sending, waiting for responses ...
Reply from 192.168.254.2 (ATLHONM320)
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
Ready
1 Computer(s) found.

[192.168.254.2]
SMB probing ...
Connecting...(1/6)
Name "ATLHONM320" encoded as "EBFEEMEIEPEOENDDCDACACACACAC"
Session established.(2/6)
Security mode : user
Protocol negotiated.(3/6)
Operating system : Windows 7 Ultimate 7600
Domain : WORKGROUP
LAN manager : Windows 7 Ultimate 6.1
NULL session established.(4/6)
Connected to IPC\$(5/6)

UDP scanning thread started ...
TCP scanning started ...
Waiting for UDP thread ...

Análise de Vulnerabilidades

Scanners de Portas

- **Scanner On-line**
- <http://www.gwebtools.com.br/scanner-porta>
- Scanners são programas de varredura utilizados para detectar possíveis vulnerabilidades em sistemas
- Procuram por certas falhas de segurança que podem permitir ataques e até mesmo invasões.
- Falhas nas configurações da rede ou mesmo desconhecimento por parte dos usuários podem tornar sua rede um prato cheio para os invasores.
- Netstat (DOS)

NMAP

- O nmap é um varredor de endereços de hosts, que pode ser utilizado para verificar a configuração das regras de firewalls.
 - É capaz de verificar uma lista de hosts, determinando o estado das portas associadas aos serviços
-
- Open: aplicação ativa escutando conexões na porta
 - Filtered: firewall já filtrou a porta, não é possível dizer se ela está ativa ou não
 - Closed: nenhuma aplicação ativa escutando conexões/porta
 - Unfiltered: a porta respondeu a sondagem nmap, mas não foi possível determinar se ela está ativa

NMAP

- O destino pode ser definido como nomes de host, endereços IP ou sub-redes.
- Exemplos: `www.pucpr.br`, `192.168.0.0/24`, `192.168.0.1`, `10.0.0.1-254`
- É possível especificar também quais portas serão testadas usando o flag `-p`

Exemplos: `-p 53`; `-p 1024-2048`, etc.

Usando o NMAP

- O Nmap é um portscan de uso geral.

```
# apt-get install nmap
```

- Você deve executá-lo como root:

```
nmap 192.168.254.1
```

```
iptables -A OUTPUT -p tcp --dport 80 -j REJECT
```

nmap 192.168.0.3

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ )
Interesting ports on 192.168.0.3:
(The 1661 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
68/tcp open  dhcpclient
631/tcp open  ipp
MAC Address: 00:0F:B0:55:EE:16 (Compal Electronics)
Nmap finished: 1 IP address (1 host up) scanned in 0.339 seconds
```

NMAP

- Para escanear uma faixa: `nmap 192.168.254.1-254`
- Escaneando com mais detalhes de protocolos uma faixa da rede

```
nmap -sS 192.168.0.0/24 -p 1-150
```

Nmap

■ Outro exemplo (Escaneando um IP)

- nmap 192.168.254.2
- nmap scan report for 192.168.254.2

☐ Host is up (0.00039s latency). Not shown: 997 closed ports

☐ PORT STATE SERVICE

☐ 135/tcp open msrpc

☐ 139/tcp open netbios-ssn

☐ 445/tcp open microsoft-ds

Nmap

Comando route

■ Escaneando um modem/router:

Nmap scan report for 192.168.254.254

(200.131.160.1 ou 71)

■ Host is up (0.0020s latency). Not shown: 998 closed ports

PORT	STATE	SERVICE
------	-------	---------

23/tcp	open	telnet
--------	------	--------

80/tcp	open	http
--------	------	------

Nmap

- `nmap -sT` :
- Com esse parâmetro é feito um escaneamento através de tentativas de conexão TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS;

Nmap -sT 192.168.254.2

Porta 80 (http)

NMAP

- sS Assim, a tentativa será com pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão. Essa técnica dificulta um pouco a detecção;

nmap -sS 192.168.0.1 -p 1-100 (testando nas portas de 1 a 100)

```
[root@linuxserver root]: nmap -sS 192.168.0.1 -p 1-100

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.0.1):
(The 99 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open      ssh

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

O que me mostra que tenho um serviço SSH(usado para acesso remoto) aberto na porta 22.

Nmap

Escanando uma faixa da Rede

■ `nmap -sS 192.168.0.0/24 -p 1-150`

```
[root@linuxserver root]: nmap -sS 192.168.0.0/24 -p 1-150

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.0.1):
(The 149 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh

Interesting ports on (192.168.0.65):
(The 148 ports scanned but not shown below are in state: closed)
Port      State      Service
111/tcp   open       sunrpc
139/tcp   open       netbios-ssn

Interesting ports on (192.168.0.66):
(The 149 ports scanned but not shown below are in state: closed)
Port      State      Service
139/tcp   open       netbios-ssn

Interesting ports on (192.168.0.242):
(The 149 ports scanned but not shown below are in state: closed)
Port      State      Service
139/tcp   open       netbios-ssn
```

Os resultados são mostrados para todos os hosts da rede separadamente. Essa técnica é interessante pra identificar falhas de segurança em toda sua rede interna.

Nmap

- Obter mais informações sobre as portas abertas, incluindo a versão de cada serviço ativo usando a opção "-sV", como em:

```
# nmap -sV 192.168.0.3
```

```
#nmap -sV -p 80 192.168.0.4
```

Nmap

- identificar qual é o sistema operacional usado em cada máquina
- # nmap -O 192.168.0.4

```
[root@linuxserver /]: nmap -O 192.168.0.66

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.0.66):
(The 1548 ports scanned but not shown below are in state: closed)
Port      State      Service
139/tcp    open       netbios-ssn

Remote operating system guess: Windows NT4 / Win95 / Win98

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Nmap

- Um alvo fora da minha rede interna

- `nmap -sT 200.154.56.80`

- Aqui tentamos uma análise por tentativas de conexão TCP (opção `-sT`) ao invés de apenas envio de solicitações de conexão (opção `-sS`)

```
[root@linuxserver root]: nmap -sT 168.143 .48

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on www. .com.br (168.143 .48):
(The 1527 ports scanned but not shown below are in state: closed)
Port      State      Service
7/tcp     open       echo
21/tcp    open       ftp
22/tcp    open       ssh
25/tcp    open       smtp
80/tcp    open       http
99/tcp    open       metagram
110/tcp   open       pop3
111/tcp   open       sunrpc
143/tcp   open       imap2
298/tcp   filtered   unknown
443/tcp   open       https
554/tcp   open       rtsp
665/tcp   open       unknown
852/tcp   open       unknown
854/tcp   open       unknown
949/tcp   filtered   unknown
2049/tcp  open       nfs
3306/tcp  open       mysql
5050/tcp  open       mmcc
6145/tcp  filtered   statsci2-lm
8080/tcp  open       http-proxy
9090/tcp  open       zeus-admin

Nmap run completed -- 1 IP address (1 host up) scanned in 859 seconds
```

Nmap

■ Escaneando portas UDP

- Para usar o scan UDP, usamos a opção "-sU", como em:
- sU - Envia pacotes UDP com 0 byte para determinar o estado dessas portas;

□ # nmap -sU 192.168.0.4

■ Scan completo incluindo todas as portas

nmap -sS -p 0-65535 192.168.0.4

Nmap

■ Escaneando portas UDP

- harley@harley:~\$ sudo nmap -sU 192.168.254.1-254
- Starting Nmap 5.21 (<http://nmap.org>) at 2011-08-29 10:39 BRT
- Nmap scan report for 192.168.254.1
- Host is up (0.0000060s latency).
- Not shown: 998 closed ports
- | PORT | STATE | SERVICE |
|----------|---------------|----------|
| 68/udp | open filtered | dhcpc |
| 5353/udp | open filtered | zeroconf |

Nmap

- Nmap scan report for 192.168.254.105
- Host is up (0.00059s latency).
- Not shown: 996 open|filtered ports

☐ PORT STATE SERVICE

☐ 68/udp closed dhcpc

☐ 1060/udp closed polestar

☐ 1064/udp closed unknown

☐ 5050/udp closed mmcc

☐ MAC Address: D8:5D:4C:C3:B9:CF (Unknown)

NMAP

- 1) Testa todas as portas TCP em um host específico
`nmap -sS espec.ppgia.pucpr.br`
- 2) Testa uma porta UDP de um host específico
`nmap -sU espec.ppgia.pucpr.br -p 53`
- 3) Mostra os protocolos (icmp, ssh) disponíveis nas máquinas da subrede
`nmap -sO www.ppgia.pucpr.br/24`

NMAP

- 4) Descubra os hosts ativos na rede

nmap -sP 10.32.1.1-200

- 5) escanear esta porta específica usando a opção "-sV" para descobrir mais sobre ela, como em:

nmap -sV -p 22543 192.168.0.4

- 6) Testa todas as portas TCP em um host específico, mostrando os pacotes analisados

nmap -sS --packet-trace espec.ppgia.pucpr.br

NMAP

- Descoberta de hosts

```
nmap -sL 128.230.18.30-35
```

- Descobrindo se a porta 161 (snmp) está aberta nos host 172.17.12.0 até 172.17.12.255 utilizando um scan UDP

```
sudo nmap -p 161 -sU 172.17.12.0-255
```

- Verificando se a porta 80 do site <http://www.terra.com.br> está aberta

```
nmap -p 80 208.84.244.116
```

NMAP

- Verificando se o SSH do www.terra.com.br está ativo
`nmap -p 22 208.84.244.116`
- ssh do local host
`nmap -p 22 localhost`
- Scanner mais completo
`nmap -sS -O -v 208.84.244.116`

Ssh usuario@ip

Nmap

- `nmap -sP`: Com essa opção o escaneamento será feito através de pacotes ICMP echo request. Verifica apenas se o host está ativo;
- Escanando o localhost:

```
[root@linuxserver root]: nmap -sS localhost

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1546 ports scanned but not shown below are in state: closed)
Port      State      Service
111/tcp    open       sunrpc
139/tcp    open       netbios-ssn
6000/tcp   open       X11

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Nmap

- Descobrir se porta é de um serviço legítimo:
 - fuser 111/tcp
- Esse comando retornará o número do processo que abriu aquela porta. Conforme a figura abaixo, este comando retornou o processo número 771.

```
[root@linuxserver root]: fuser 111/tcp
111/tcp:          771
```

- Agora para o comando ps, que serve para visualizar processos ativos, passamos o número do processo como parâmetro:

```
[root@linuxserver root]: ps 771
  PID TTY          STAT       TIME COMMAND
  771 ?            S          0:00 portmap
```

- Essa porta é aberta pelo portmap, que é responsável pelo mapeamento de conexões de rede.

Nmap

■ Detalhando serviços ativos

□ nmap -A localhost


```
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
111/tcp    open  rpcbind      2 (rpc #100000)
139/tcp    open  netbios-ssn  Samba smbd (workgroup: LOCALDOMAIN)
6000/tcp   open  X11          (access denied)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.105 days (since Wed Oct  8 13:58:53 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 14.144 seconds
```

nmap

■ Matrix

```
No exact OS matches for host  
Nmap run completed -- 1 IP address (1 host up) scanned  
# sshnuke 10.2.2.2 -rootpw="210H0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Attempting to exploit SSHv1 CRC32 ... successful.  
Resetting root password to "210H0101".  
System open: Access Level (9)  
# ssh 10.2.2.2 -l root  
root@10.2.2.2's password: |
```



Iptables

- `iptables -A OUTPUT -p tcp --dport 80 -j REJECT`

