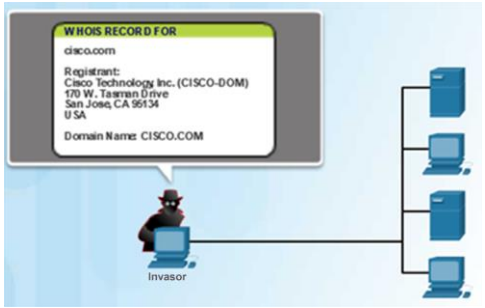
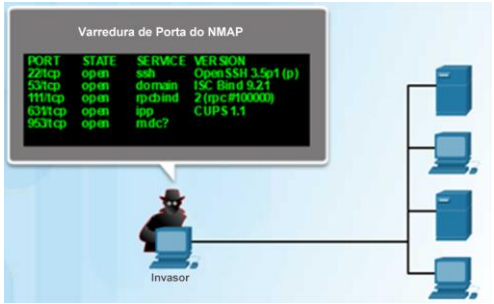
OBJETIVOS

- Exploração de Vulnerabilidade;
- Metodologia PTES;
- Scanner de Portas (NMAP, ZENMAP).

EXPLORAÇÃO DE VULNERABILIDADE

- Exploração de vulnerabilidade – varredura para encontrar a vulnerabilidade a ser explorada
  - **Etapa 1** – Reunir informações sobre o sistema de destino usando o scanner de porta ou engenharia social
  - **Etapa 2** – Determinar as informações aprendidas na Etapa 1
  - **Etapa 3** – Procurar vulnerabilidade
  - **Etapa 4** – Usar um exploit conhecido ou gravar um novo exploit



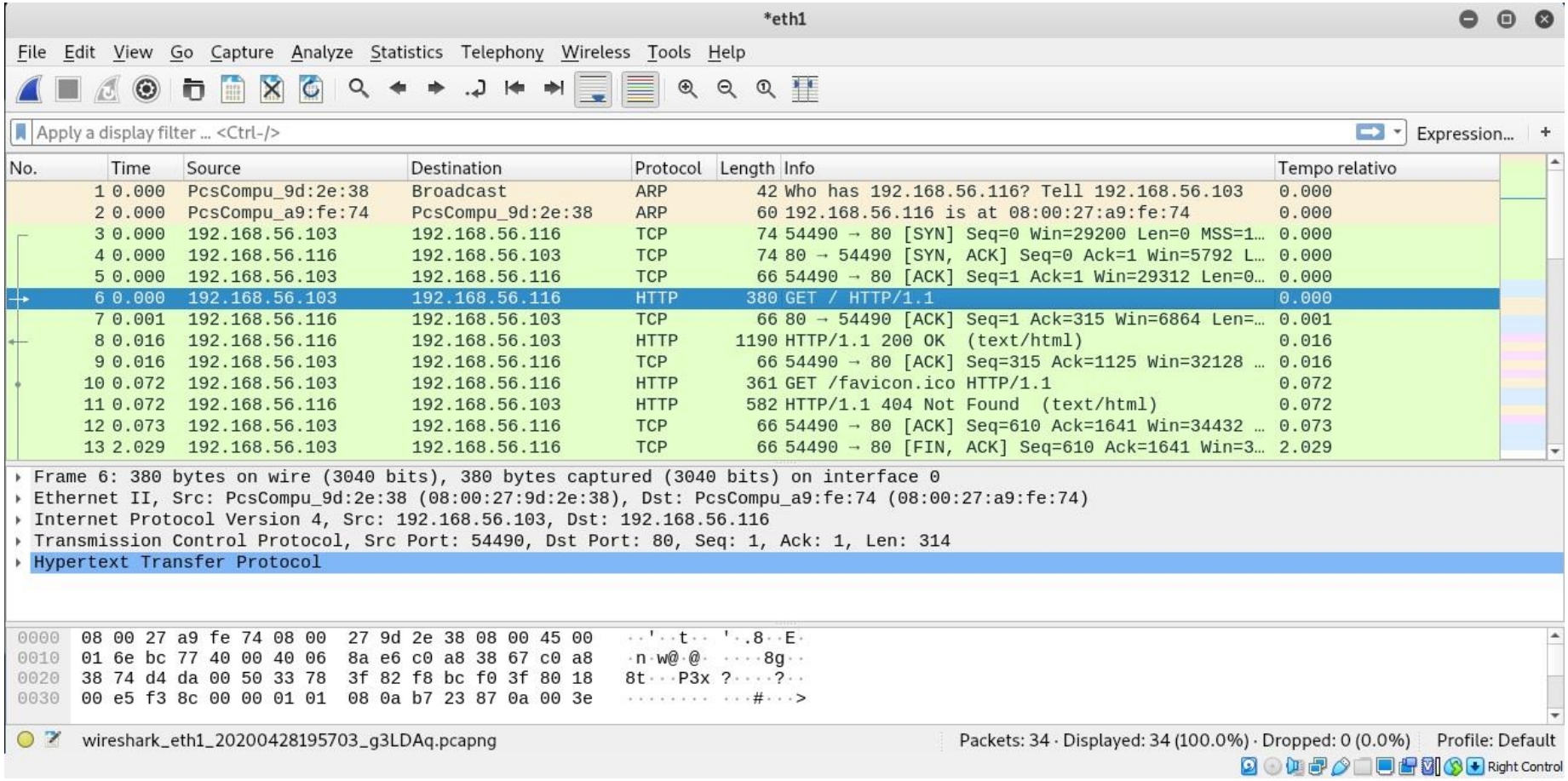


METODOLOGIA PTES

- Preparação;
- Coleta de informações;
- Modelagem;
- Análise de Vulnerabilidades;
- Exploração;
- Pós-Exploração;
- Relatório.

- https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf

PROTOCOLOS


*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info Tempo relativo
1 0.000 PcsCompu_9d:2e:38 Broadcast ARP 42 Who has 192.168.56.116? Tell 192.168.56.103 0.000
2 0.000 PcsCompu_a9:fe:74 PcsCompu_9d:2e:38 ARP 60 192.168.56.116 is at 08:00:27:a9:fe:74 0.000
3 0.000 192.168.56.103 192.168.56.116 TCP 74 54490 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1… 0.000
4 0.000 192.168.56.116 192.168.56.103 TCP 74 80 → 54490 [SYN, ACK] Seq=0 Ack=1 Win=5792 L… 0.000
5 0.000 192.168.56.103 192.168.56.116 TCP 66 54490 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0… 0.000
6 0.000 192.168.56.103 192.168.56.116 HTTP 380 GET / HTTP/1.1 0.000
7 0.001 192.168.56.116 192.168.56.103 TCP 66 80 → 54490 [ACK] Seq=1 Ack=315 Win=6864 Len=… 0.001
8 0.016 192.168.56.116 192.168.56.103 HTTP 1190 HTTP/1.1 200 OK (text/html) 0.016
9 0.016 192.168.56.103 192.168.56.116 TCP 66 54490 → 80 [ACK] Seq=315 Ack=1125 Win=32128 … 0.016
10 0.072 192.168.56.103 192.168.56.116 HTTP 361 GET /favicon.ico HTTP/1.1 0.072
11 0.072 192.168.56.116 192.168.56.103 HTTP 582 HTTP/1.1 404 Not Found (text/html) 0.072
12 0.073 192.168.56.103 192.168.56.116 TCP 66 54490 → 80 [ACK] Seq=610 Ack=1641 Win=34432 … 0.073
13 2.029 192.168.56.103 192.168.56.116 TCP 66 54490 → 80 [FIN, ACK] Seq=610 Ack=1641 Win=3… 2.029
Frame 6: 380 bytes on wire (3040 bits), 380 bytes captured (3040 bits) on interface 0
Ethernet II, Src: PcsCompu_9d:2e:38 (08:00:27:9d:2e:38), Dst: PcsCompu_a9:fe:74 (08:00:27:a9:fe:74)
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.116
Transmission Control Protocol, Src Port: 54490, Dst Port: 80, Seq: 1, Ack: 1, Len: 314
Hypertext Transfer Protocol
0000 08 00 27 a9 fe 74 08 00 27 9d 2e 38 08 00 45 00
0010 01 6e bc 77 40 00 40 06 8a e6 c0 a8 38 67 c0 a8
0020 38 74 d4 da 00 50 33 78 3f 82 f8 bc f0 3f 80 18
0030 00 e5 f3 8c 00 00 01 01 08 0a b7 23 87 0a 00 3e
wireshark_eth1_20200428195703_g3LDAq.pcapng
Packets: 34 · Displayed: 34 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Right Control

IDENTIFICAÇÃO DE PORTAS

```
root@kali:~# ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.103  netmask 255.255.255.0  broadcast 192.168.56.255
        ether 08:00:27:9d:2e:38  txqueuelen 1000  (Ethernet)
        RX packets 3623  bytes 1009488 (985.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2529  bytes 267761 (261.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# service apache2 start
root@kali:~# netstat -nlpt | grep 80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
2890/apache2
```

IDENTIFICAÇÃO DE PORTAS E SERVIÇOS

```
root@kali:~# cat /etc/services | more
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/servi
ce-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
```

SCANNER DE PORTAS (NMAP)

- O **nmap** (network mapper) é uma ferramenta de código aberto usada por administradores de sistema para auditar redes, escaneamento de segurança e encontrar portas abertas em máquinas host.
- É capaz de escanear um host ou toda a sub-rede para encontrar portas TCP e UDP abertas. Esta ferramenta também é usada por atacantes para encontrar portas vulneráveis.
- Se o comando **nmap** for executado sem quaisquer opções, então ele procurará as portas TCP abertas e informará as portas abertas junto com o serviço que está sendo executado nelas.

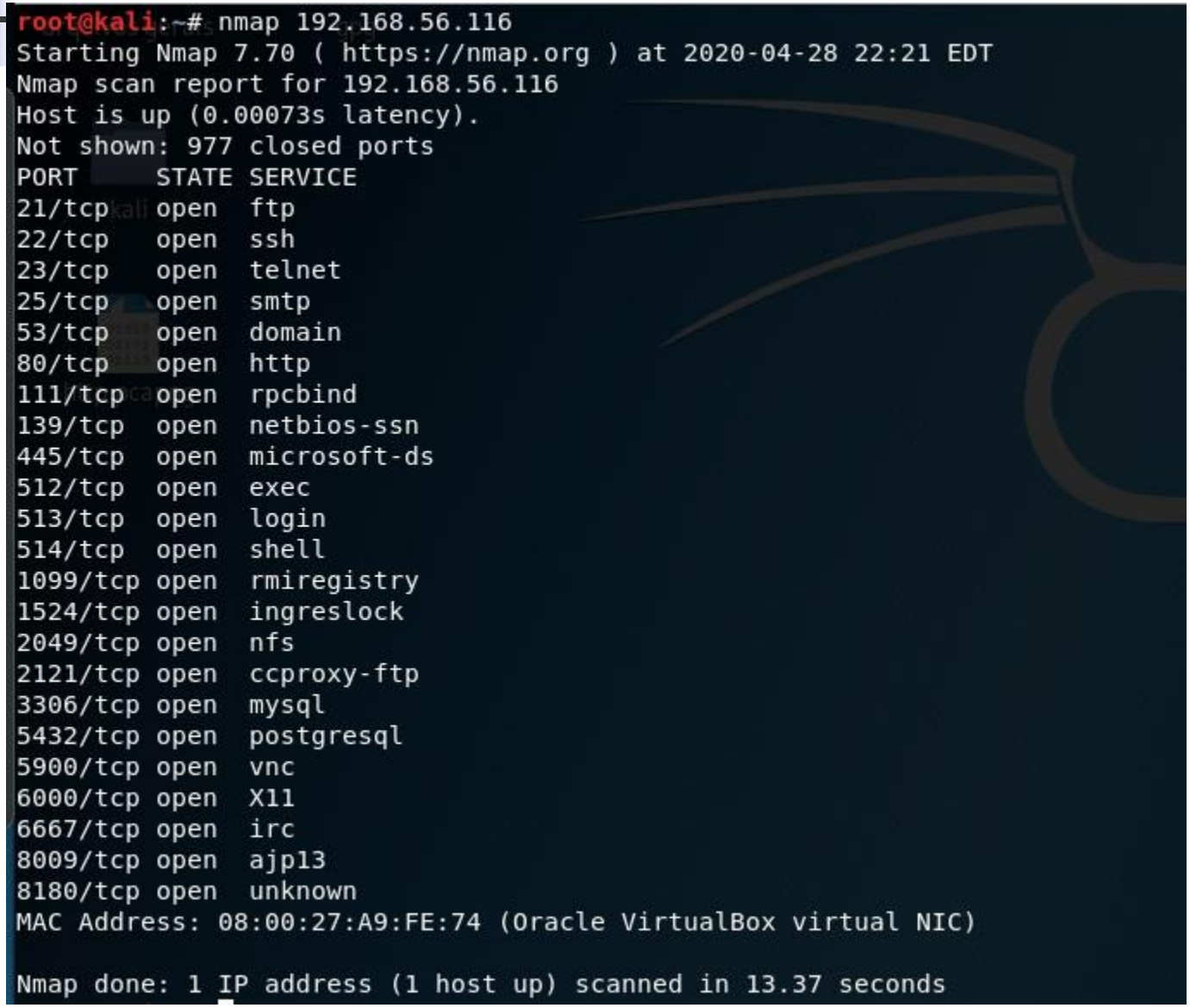
SCANNER DE PORTAS (NMAP)

root@localhost:~# nmap example.com
root@localhost:~# nmap 192.168.1.2

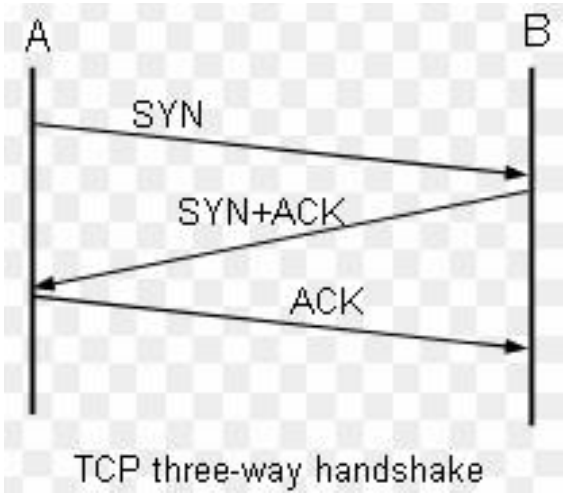
Starting Nmap 6.40 (http://nmap.org) at 2015-03-13 22:02 UTC
Nmap scan report for example.com (192.168.1.2)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open ssh
53/tcp open domain

Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds

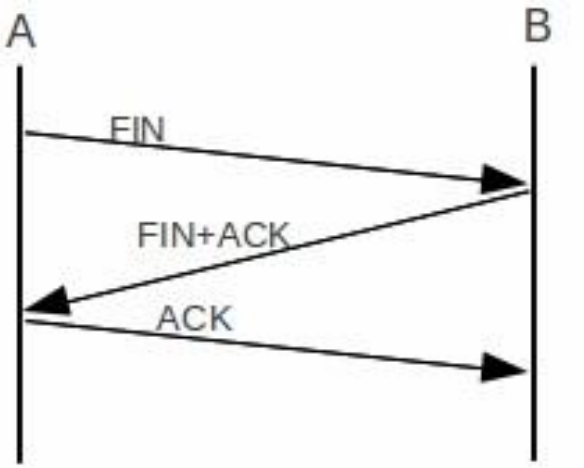
SCANNER DE PORTAS (NMAP)

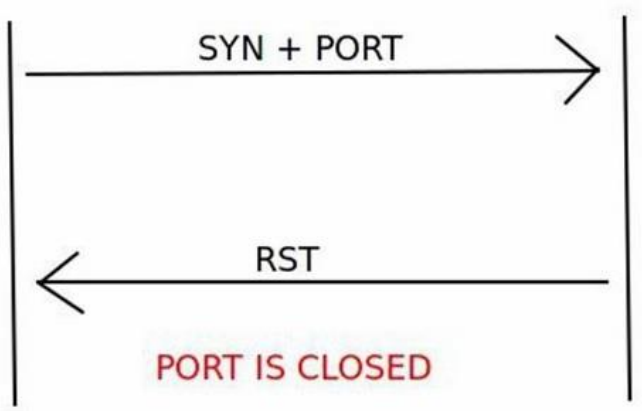


HANDSHAKE TCP



TCP three-way handshake

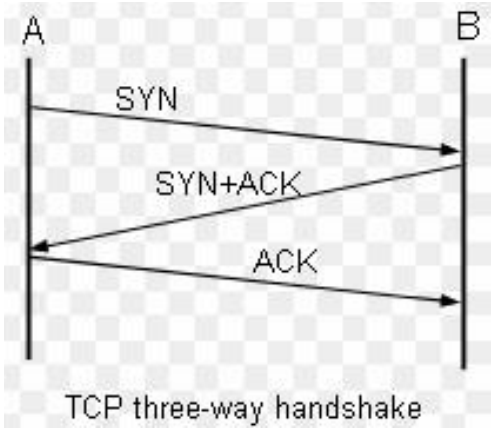




SCANNER DE PORTAS (NMAP)

- TCP Connect
  - Completa o Three way handshake, gera mais tráfego e facilmente detectável (**nmap –sT**);
  - Usado para identificar a versão do serviço e faz o TCP connect (**nmap –sV**);
- Half Open/Syn Connect
  - Envia um Syn e analisa a resposta, se for SYN/ACK a porta está aberta e então é enviado um RST sem completar o handshake;
  - Não completa o three handshake, consome menos tráfego, nível de detecção menor se comparado com o TCP Connect;
  - **Nmap -sS**

SCANNER DE PORTAS (NMAP) – TCP CONNECT



TCP three-way handshake

```
root@kali:~# nmap -sT -p 80 -Pn 192.168.56.116
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-28 23:44 EDT
Nmap scan report for 192.168.56.116
Host is up (0.00052s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```

TCP	74 41982 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1…	2.850
TCP	74 80 → 41982 [SYN, ACK] Seq=0 Ack=1 Win=5792 L…	2.855
TCP	66 41982 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0…	2.855
TCP	66 41982 → 80 [RST, ACK] Seq=1 Ack=1 Win=29312 …	2.855

SCANNER DE PORTAS (NMAP) – TCP CONNECT

- Identificando serviços e SO

```
root@kali:~# nmap -O -p 80 -Pn 192.168.56.116
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-29 00:26 EDT
Nmap scan report for 192.168.56.116
Host is up (0.0017s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:A9:FE:74 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 op
en and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

SCANNER DE PORTAS (NMAP) – TCP CONNECT

- Identificando serviços e SO

```
root@kali:~# nmap -A -p 80 -Pn 192.168.56.116
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-29 00:31 EDT
Nmap scan report for 192.168.56.116
Host is up (0.00049s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
MAC Address: 08:00:27:A9:FE:74 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 op
en and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.49 ms 192.168.56.116
```

SCANNER DE PORTAS (NMAP)

- Algumas opções:
  - -sn: detecção de hosts vivos
  - -sT: TCP connect
  - -sS: Syn Scan / Half Open
  - -sV: descobrir versões de serviços
  - -sU: UDP Scan
  - -Pn: ignora a descoberta de host vivo
  - -O: faz detecção do sistema operacional
  - -A: descobre detalhes sobre o SO e serviços
  - -p-: varre todas as portas (65535)

SCANNER DE PORTAS (NMAP)

- Algumas opções:
  - -sF: FIN Scan (envia flag FIN)
  - -sN: NULL Scan (não envia nenhuma flag)
  - -sX: XMAS Scan (envia FIN+PSH+URG)
  - -f: fragmenta os pacotes
  - -p: define a porta
  - --open: só mostra as portas abertas
  - -oN: salva em arquivo no formato normal
  - -oX: salva em arquivo no formato XML

SCANNER DE PORTAS (NMAP)

- Nível de Agressividade:
  - -T0: usado para previnir IDS
  - -T1: espera cerca de 15s durante o scan
  - -T2: espera cerca de 4s durante o scan
  - -T3: normal
  - -T4: scan rápido
  - -T5: scan muito rápido e barulhento

SCANNER DE PORTAS (NMAP)

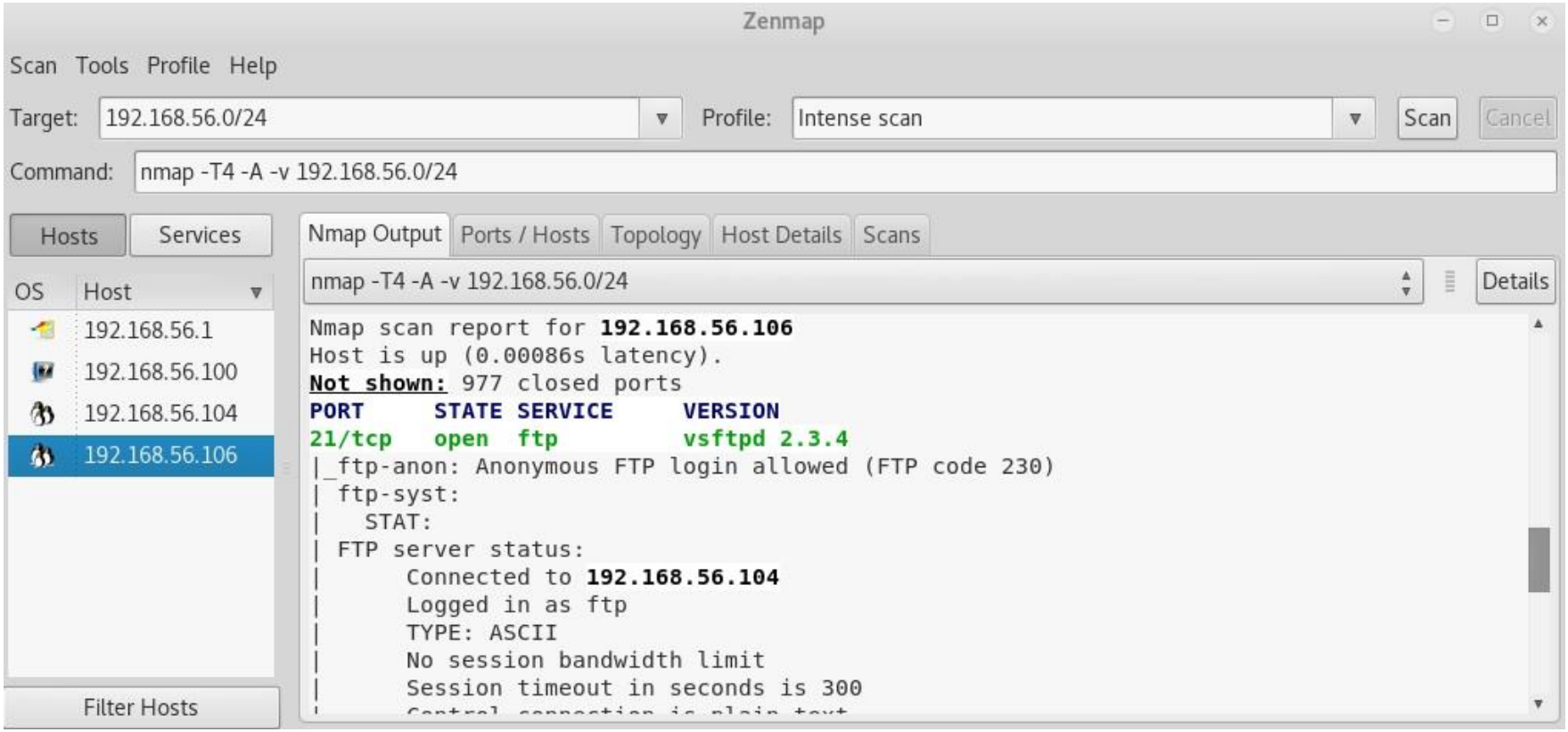
- Alguns exemplos:
  - 1. nmap -v –sS –p 80 192.168.10.20 (TCP)
  - 2. nmap –sS –p80 –Pn 192.168.10.20 (TCP)
  - 3. nmap –sT –p5000 –Pn 192.168.10.20 (TCP)
  - 4. nmap -v –sU –p 161-Pn 192.168.10.20 (UDP)
  - 5. nmap -v –sU –p 53, 161, 162, 5060 -Pn 192.168.10.20 (UDP)
  - 6. nmap -v –sUV –p 53, 161, 162, 5060 -Pn 192.168.10.20 (UDP com descobrimento de serviços)
  - 7. nmap -v –sV -Pn 192.168.10.20 (descobrindo serviços)
  - 8. nmap -v –A -Pn 192.168.10.20 (descobrindo serviços)
  - 9. nmap -v –O 192.168.10.20 (detectando o SO)
  - 10. nmap -v –O –sV -p22 192.168.10.20 (detectando o SO)
  - 11. nmap –T4 –A –v 192.168.56.0/24 (descobre os detalhes dos SOs e serviços com visualização e responde rapidamente)

SCANNER DE PORTAS (ZENMAP)

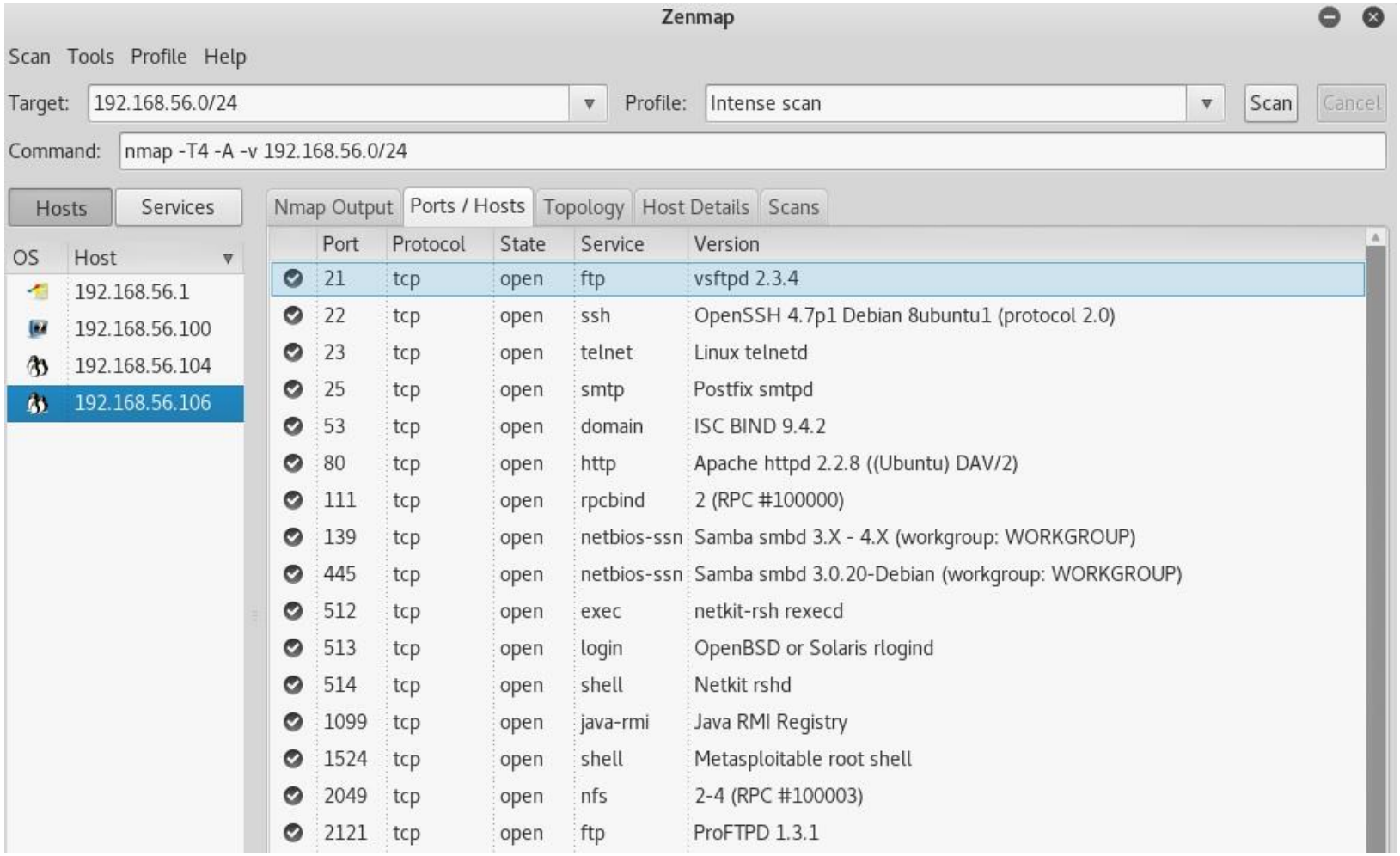
Instalando:

- ✓ wget -q https://nmap.org/dist/zenmap-7.91-1.noarch.rpm
- ✓ apt install alien
- ✓ alien zenmap-7.91–1.noarch.rpm
- ✓ dpkg -i zenmap_7.91–2_all.deb

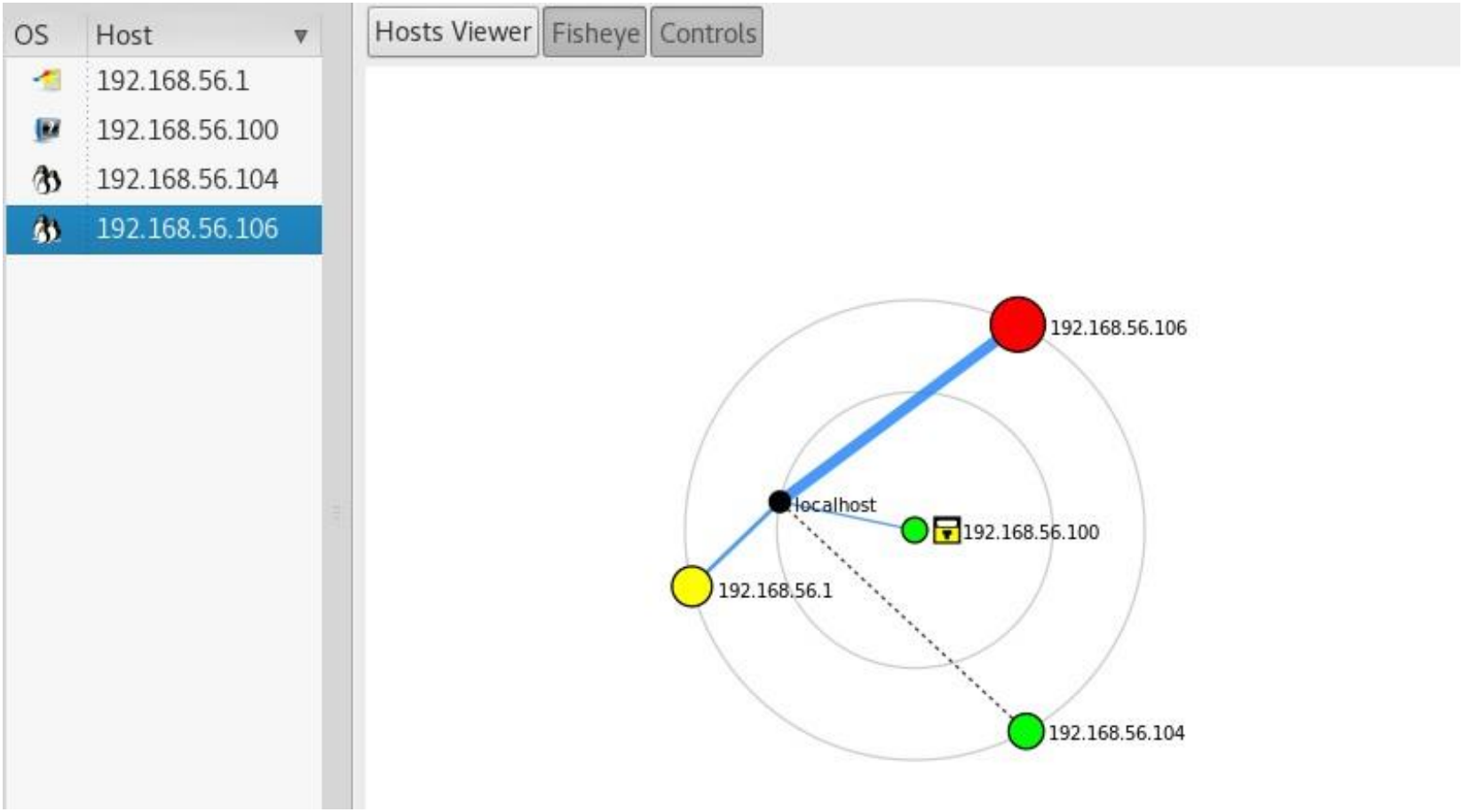
SCANNER DE PORTAS (ZENMAP)



SCANNER DE PORTAS (ZENMAP)



SCANNER DE PORTAS (ZENMAP)



BIBLIOGRAFIA

- NMAP. Nmap Reference Guide. Disponível em: <https://nmap.org/book/man.html> Acesso em 05.10.2024.
- ZENMAP. Nmap Security Scanner GUI. Disponível em: <https://nmap.org/zenmap> Acesso em 05.10.2024.