

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
EDUARDO NEVES CÓRDOVA**

**TRABALHO PRÁTICO 1 DE SEGURANÇA DA INFORMAÇÃO E DE
REDES**

**FLORIANÓPOLIS
2016**

IP da máquina Metasploitable2: 10.1.2.5

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:0a:1b
          inet addr:10.1.2.5  Bcast:10.1.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec7:a1b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3851 errors:1 dropped:0 overruns:0 frame:0
          TX packets:3663 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:251477 (245.5 KB)  TX bytes:276572 (270.0 KB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:186 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64913 (63.3 KB)  TX bytes:64913 (63.3 KB)

msfadmin@metasploitable:~$
```

IP da máquina Kali-linux: 10.1.2.6

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.1.2.6 netmask 255.255.255.0 broadcast 10.1.2.255
      inet6 fe80::a00:27ff:fe9d:208b prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:9d:20:8b txqueuelen 1000 (Ethernet)
      RX packets 3685  bytes 298957 (291.9 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 3820  bytes 243736 (238.0 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
      inet6 fe80::a00:27ff:fell:e70a prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:11:e7:0a txqueuelen 1000 (Ethernet)
      RX packets 32  bytes 5464 (5.3 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 82  bytes 7072 (6.9 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 0 (Local Loopback)
      RX packets 47  bytes 4224 (4.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 47  bytes 4224 (4.1 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

a) nmap -sV 10.1.2.5

```
root@kali:~# nmap -sV 10.1.2.5

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-25 10:39 EDT
Nmap scan report for 10.1.2.5
Host is up (0.0019s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?         Netkit rshd
514/tcp   open  shell          GNU Classpath grmiregistry
1099/tcp  open  rmiregistry    Metasploitable root shell
1524/tcp  open  nfs            2-4 (RPC #100003)
2049/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            Unreal ircd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C7:0A:1B (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.18 seconds
root@kali:~#
```

-sV (Version detection): Lista informações de portas abertas com o serviço e a versão do computador alvo.

b) nmap -v 10.1.2.5

```
root@kali:~# nmap -v 10.1.2.5

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-25 09:21 EDT
Initiating ARP Ping Scan at 09:21
Scanning 10.1.2.5 [1 port]
Completed ARP Ping Scan at 09:21, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:21
Completed Parallel DNS resolution of 1 host. at 09:21, 0.02s elapsed
Initiating SYN Stealth Scan at 09:21
Scanning 10.1.2.5 [1000 ports]
Discovered open port 25/tcp on 10.1.2.5
Discovered open port 23/tcp on 10.1.2.5
Discovered open port 445/tcp on 10.1.2.5
Discovered open port 3306/tcp on 10.1.2.5
Discovered open port 21/tcp on 10.1.2.5
Discovered open port 80/tcp on 10.1.2.5
Discovered open port 139/tcp on 10.1.2.5
Discovered open port 111/tcp on 10.1.2.5
Discovered open port 22/tcp on 10.1.2.5
Discovered open port 53/tcp on 10.1.2.5
Discovered open port 5900/tcp on 10.1.2.5
Discovered open port 6667/tcp on 10.1.2.5
Discovered open port 513/tcp on 10.1.2.5
Discovered open port 514/tcp on 10.1.2.5
Discovered open port 2121/tcp on 10.1.2.5
Discovered open port 1524/tcp on 10.1.2.5
Discovered open port 6000/tcp on 10.1.2.5
Discovered open port 1099/tcp on 10.1.2.5
Discovered open port 512/tcp on 10.1.2.5
Discovered open port 8180/tcp on 10.1.2.5
Discovered open port 8009/tcp on 10.1.2.5
Discovered open port 5432/tcp on 10.1.2.5
Discovered open port 2049/tcp on 10.1.2.5
Completed SYN Stealth Scan at 09:21, 0.11s elapsed (1000 total ports)
Nmap scan report for 10.1.2.5
Host is up (0.0015s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C7:0A:1B (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
root@kali:~#
```

Com a porta 2049, do serviço NFS, permite ler/escrever um arquivo em qualquer lugar do computador alvo. Como o ssh está rodando no computador atacado, é possível sobrescrever as chaves de acesso por um arquivo criado pelo atacante, dando acesso total à máquina atacada.

Na porta 21, roda um servidor FTP. Essa versão contém uma backdoor que foi introduzido no código fonte por um intruso desconhecido. Se a nome de usuário que é enviado terminar com a sequência “:”, a versão que possui backdoor abrirá um terminal na porta 6200.

c) nmap -sP 10.1.2.0/24

```
root@kali:~# nmap -sP 10.1.2.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-25 09:44 EDT
Nmap scan report for 10.1.2.3
Host is up (0.00091s latency).
MAC Address: 0A:00:27:00:00:16 (Unknown)
Nmap scan report for 10.1.2.4
Host is up (0.00088s latency).
MAC Address: 08:00:27:0D:78:49 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.1.2.5
Host is up (0.0016s latency).
MAC Address: 08:00:27:C7:0A:1B (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.1.2.6
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.10 seconds
root@kali:~#
```

-sn (No port scan): Lista todos o hosts do IP 10.1.2.0 ao 10.1.2.24, sem fazer um escaneamento de portas. Permite um reconhecimento da rede sem atrair muita atenção.

No teste foram encontrados 4 host conectados.

- 1) O adaptador de rede do virtual box
- 2) O adaptador de rede local do Kali
- 3) O servidor do metasploitable2
- 4) O servido local do Kali

d) `nmap -sS -O -v www.inf.ufsc.br`

```
root@kali:~# nmap -sS -O -v www.inf.ufsc.br
Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-25 10:43 EDT
Initiating Ping Scan at 10:43
Scanning www.inf.ufsc.br (150.162.60.21) [4 ports]
Completed Ping Scan at 10:43, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:43
Completed Parallel DNS resolution of 1 host. at 10:43, 0.05s elapsed
Initiating SYN Stealth Scan at 10:43
Scanning www.inf.ufsc.br (150.162.60.21) [1000 ports]
Discovered open port 443/tcp on 150.162.60.21
Discovered open port 80/tcp on 150.162.60.21
Completed SYN Stealth Scan at 10:43, 4.93s elapsed (1000 total ports)
Initiating OS detection (try #1) against www.inf.ufsc.br (150.162.60.21)
Retrying OS detection (try #2) against www.inf.ufsc.br (150.162.60.21)
Nmap scan report for www.inf.ufsc.br (150.162.60.21)
Host is up (0.012s latency).
Not shown: 998 filtered ports
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: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/o:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.09 seconds
Raw packets sent: 2048 (93.308KB) | Rcvd: 33 (1.876KB)
root@kali:~#
```

-sS (TCP SYN scan): Faz um SYN scan. Pode ser realizado rapidamente, escaneando milhares de portas por segundo em redes rápidas não impedida por firewalls. É relativamente não intrusiva e discreta já que não realiza uma conexão TCP completa.

-O (Enable OS detection): Detecta os SO's usando TCP/IP fingerprinting.

Foi encontrado somente duas portas abertas no servidor "www.inf.ufsc.br", 998 portas filtradas. A detecção de SO não é precisa pois o nmap não encontrou pelo menos uma porta aberta e uma fechada.

e) `nmap -sT -Pn -n --top-ports 10 --reason -oA hhs_5_tcp hackerhighschool.org`

```
root@kali:~# nmap -sT -Pn -n --top-ports 10 --reason -oA hhs_5_tcp hackerhighschool.org
Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-25 09:46 EDT
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.18s latency).
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack
22/tcp    open  ssh     syn-ack
23/tcp    filtered telnet  no-response
25/tcp    filtered smtp   no-response
80/tcp    open  http    syn-ack
110/tcp   open  pop3    syn-ack
139/tcp   filtered netbios-ssn no-response
443/tcp   open  https   syn-ack
445/tcp   filtered microsoft-ds no-response
3389/tcp  filtered ms-wbt-server no-response

Nmap done: 1 IP address (1 host up) scanned in 2.55 seconds
root@kali:~#
```

-sT (TCP connect scan): O Nmap pede ao sistema operacional subjacente para estabelecer uma conexão com o computador de destino e porta emitindo a chamada de sistema *connect*. Este é a mesma chamada de sistema de alto nível que os navegadores web, clientes P2P, e mais outros aplicativos habilitados para rede utilizam para estabelecer uma conexão. É parte de uma interface de programação conhecida como a API Berkeley Sockets. O Nmap utiliza esta API para obter informações do estado a cada tentativa de conexão.

-Pn (No ping): Não realiza o escaneamento de hosts online.

--reason: Mostra o motivo pelo qual a porta foi detectado com “fechada”, “aberta” ou “filtrada”.

l) Diferenças entre scan TCP e SYN

-sS SYN scan:

Esta técnica, não realiza uma conexão TCP completa. Você manda um pacote SYN, como se fosse realizar uma verdadeira conexão e espera por uma resposta. Um SYN/ACK indica que a porta está escutando. Um RST é um indicativo de que a porta não está escutando. Se um SYN/ACK é recebido, um RST é imediatamente enviado para cortar a conexão. A principal vantagem dessa técnica de escaneamento é que poucos sites manterão um registro.

-sT TCP connect() scan:

Esta técnica é a forma mais básica de escaneamento TCP. A chamada de sistema *connect()* é usada para abrir uma conexão para todas as portas na máquina. Se a porta estiver escutando, *connect()* terá êxito, ao contrário a porta é inalcançável. Este tipo de escanamento é facilmente detectado já que aparecerá nos logs um monte de conexão e mensagens de erro para os serviços que aceitaram a conexão e tiveram imediatamente desconectados. Uma vantagem desta técnica é que não é necessário nenhum privilégio, qualquer usuário na maioria dos sistemas UNIX é livre pra usar essa chamada.

n) Exemplos?

```
nmap -v -iR 100000 -Pn -p 80
```

Pede ao Nmap para escolher 100.000 hosts de forma aleatória e escaneá-los procurando por servidores web (porta 80). A enumeração de hosts é desabilitada com -Pn uma vez que enviar primeiramente um par de sondagens para determinar se um hosts está ativo é um desperdício quando se está sondando uma porta em cada host alvo.

Com o teste realizado, foram encontrados muitas portas “filtradas”, porém pode-se detectar uma quantidade significativa de portas “abertas”. Suscetíveis a possíveis ataques.

nmap -sU -Pn --reason 10.1.2.5

```
root@kali:~# nmap -sU -Pn --reason 10.1.2.5

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-27 11:23 EDT
Stats: 0:13:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.67% done; ETC: 11:40 (0:04:25 remaining)
Stats: 0:13:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.98% done; ETC: 11:40 (0:04:22 remaining)
Stats: 0:13:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.70% done; ETC: 11:40 (0:04:14 remaining)
Nmap scan report for 10.1.2.5
Host is up, received arp-response (0.00056s latency).
Not shown: 993 closed ports
Reason: 993 port-unreaches
PORT      STATE      SERVICE      REASON
53/udp    open       domain       udp-response ttl 64
68/udp    open|filtered dhcpc        no-response
69/udp    open|filtered tftp        no-response
111/udp   open       rpcbind      udp-response ttl 64
137/udp   open       netbios-ns   udp-response ttl 64
138/udp   open|filtered netbios-dgm  no-response
2049/udp  open       nfs          udp-response ttl 64
MAC Address: 08:00:27:C7:0A:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1076.00 seconds
Scan UDP com o motivo das portas da máquina metasploitable2.
```