

S5L3

NMAP

Come da consegna, inizio effettuando uno scan nmap per individuare il sistema operativo della macchina Metasploit. Per quanto il tool non riesca a trovare risultati precisi, il OS-Guess propone come possibile sistema operativo Linux 2.6.x

```
kali@kali: ~  
(kali@kali)-[~]  
$ sudo nmap -O --osscan-guess 192.168.1.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:42 CET  
Nmap scan report for 192.168.1.101  
Host is up (0.0086s latency).  
Not shown: 977 closed tcp ports (reset)  
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:B7:1E:00 (Oracle VirtualBox virtual NIC)  
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.18 - 2.6.32 (96%), Linux 2.6.21 (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.9 (96%), Linux 2.6.23 (96%), Linux 2.6.24 - 2.6.28 (95%)  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.94%E=4%D=12/20%OT=21%CT=1%CU=36028%PV=Y%D=1%DC=D%G=Y%M=080027%  
OS:TM=6582B72A%P=x86_64-pc-linux-gnu)SEQ(SP=CE%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%  
OS:TS=6)SEQ(SP=CE%GCD=2%ISR=CF%TI=Z%CI=Z%II=I%TS=6)OPS(O1=M5B4ST11NW7%O2=M5  
OS:B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(  
OS:W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0  
OS:XO=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R  
OS:=Y%DF=Y%T=40%W=16A0%S=0%A=S+F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40  
OS:%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q  
OS:=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A  
OS:=S+F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%R  
OS:UCK=G%RUD=6)IE(R=Y%DFI=N%T=40%CD=S)  
  
Network Distance: 1 hop
```

```
kali@kali: ~  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.1.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:45 CET  
Nmap scan report for 192.168.1.101  
Host is up (0.0019s latency).  
Not shown: 977 closed tcp ports (reset)  
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:B7:1E:00 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds  
  
(kali@kali)-[~]  
$
```

Procedo con una scansione SYN, che da
come risultati queste porte e questi servizi.
Notare la voce “(reset)” nella riga
“Not shown: 977 closed ports”

Il prossimo scan della consegna è quello TCP. La differenza tra i due è nella voce evidenziata precedentemente: in questa scansione il risultato è “(conn-refused)”

```
kali@kali: ~  
  
(kali@kali)-[~]  
$ sudo nmap -sT 192.168.1.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:46 CET  
Nmap scan report for 192.168.1.101  
Host is up (0.0080s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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:B7:1E:00 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
  
(kali@kali)-[~]  
$ sudo nmap -sv 192.168.1.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:51 CET  
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Nmap scan report for 192.168.1.101  
Host is up (0.0051s latency).  
Not shown: 977 closed tcp ports (reset)  
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?  
25/tcp    open  smtp?  
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 - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec?  
513/tcp   open  login?  
514/tcp   open  shell?  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ccproxy-ftp?  
3306/tcp  open  mysql?  
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          UnrealIRCd  
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:B7:1E:00 (Oracle VirtualBox virtual NIC)  
Service Info: Host: 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 193.86 seconds  
  
(kali@kali)-[~]  
$
```

L'ultima scansione della macchina Meta è quella della versione dei servizi attivi, i risultati sono quelli nell'immagine qui riportata

```
root@kali: /home/kali

(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# nmap -O 192.168.1.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:55 CET
Nmap scan report for 192.168.1.102
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.1.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:F4:03:D5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft
Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2
012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.33 seconds
```

Passiamo adesso alla macchina Windows 7, per la quale è stato richiesto di fare una scansione del sistema operativo.

Come ci mostrano i risultati non è possibile trovare con certezza il sistema operativo della macchina, poiché tutte le porte sono filtrate.

Nonostante tutto rileva il fatto che sia una macchina Windows di qualche tipo.

Come scansionare Windows?

Probabilmente il metodo migliore per riuscire ad effettuare la scansione su windows sia modificare il suo firewall per aprire delle porte alla macchina Kali