

Report S5L3

Os fingerprint

Effettuando l'OS fingerprint su Metasploitable con Nmap, ottieni informazioni dettagliate sul sistema operativo in esecuzione sul target. Nel caso della metasploit sono tornate meno informazioni del previsto questo probabilmente dovuto a qualche linguaggio scorretto nelle impostazioni della metasploit.

```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nmap -O 192.168.1.188  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:29 CEST  
Nmap scan report for 192.168.1.188  
Host is up (0.0014s latency).  
Not shown: 979 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
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  
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  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port
```

Syn scan

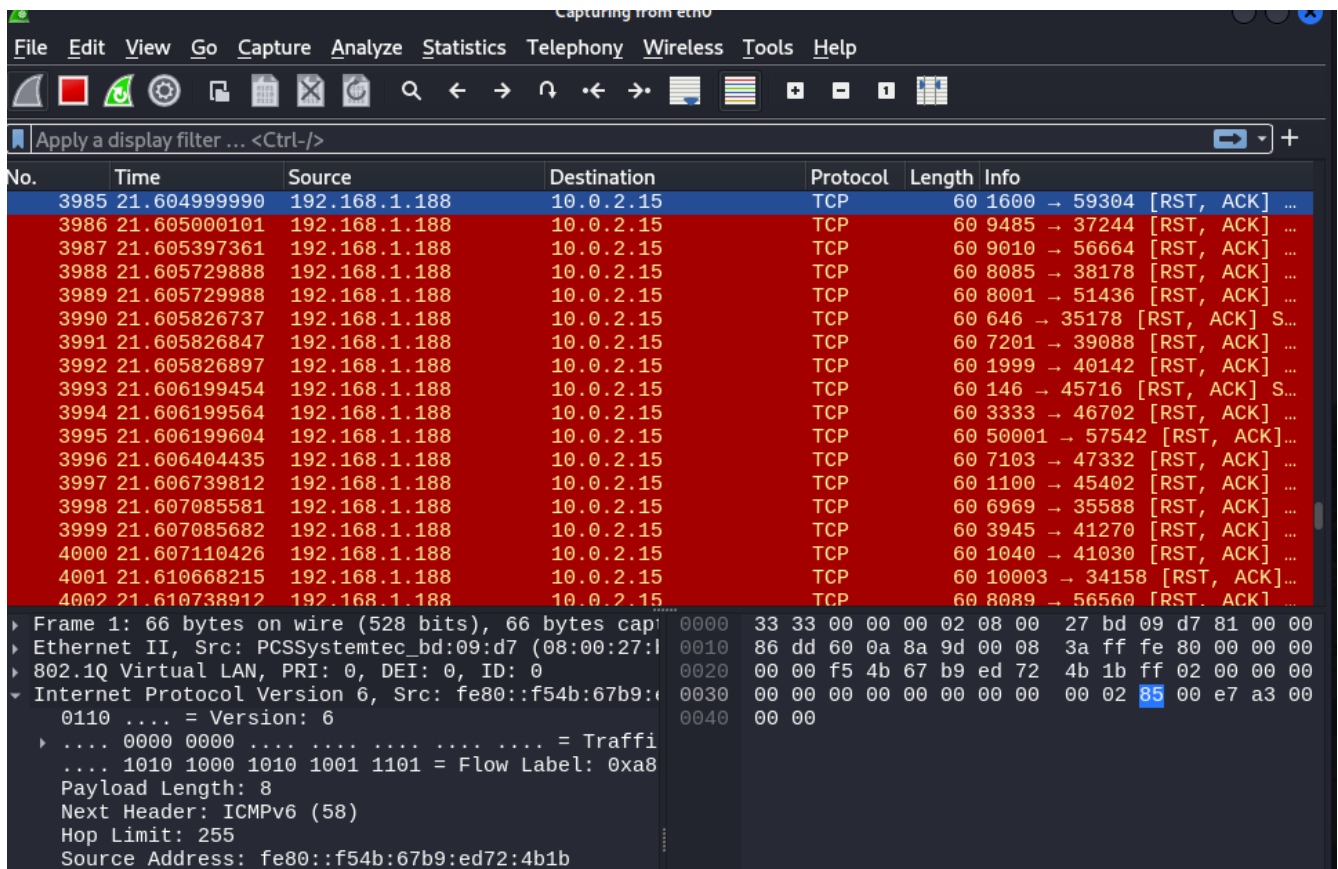
Effettuando una SYN scan su Metasploitable con Nmap, ottieni una lista delle porte aperte e attive sul sistema target. Questa tecnica invia pacchetti SYN alle porte di destinazione e attende le risposte SYN-ACK, indicando che la porta è aperta. La SYN scan è veloce e meno invasiva, spesso non registrata nei log del sistema target, quindi è utile per una ricognizione discreta. Le informazioni raccolte ti permettono di identificare i servizi in esecuzione e di pianificare ulteriori analisi e attacchi mirati. Inoltre, la SYN scan aiuta a valutare la superficie di attacco del sistema, evidenziando potenziali punti di ingresso per exploit.

No.	Time	Source	Destination	Protocol	Length	Info
266	12.761156695	10.0.2.15	192.168.1.188	TCP	58	37497 → 1045 [SYN] Seq=0...
267	12.761166949	10.0.2.15	192.168.1.188	TCP	58	37497 → 9071 [SYN] Seq=0...
268	12.761171906	10.0.2.15	192.168.1.188	TCP	58	37497 → 416 [SYN] Seq=0 ...
269	12.761175871	10.0.2.15	192.168.1.188	TCP	58	37497 → 783 [SYN] Seq=0 ...
270	12.761180368	10.0.2.15	192.168.1.188	TCP	58	37497 → 15003 [SYN] Seq=...
271	12.761185264	10.0.2.15	192.168.1.188	TCP	58	37497 → 2006 [SYN] Seq=0...
272	12.761189430	10.0.2.15	192.168.1.188	TCP	58	37497 → 32768 [SYN] Seq=...
273	12.761194367	10.0.2.15	192.168.1.188	TCP	58	37497 → 3493 [SYN] Seq=0...
274	12.761202478	10.0.2.15	192.168.1.188	TCP	58	37497 → 9011 [SYN] Seq=0...
275	12.761207204	10.0.2.15	192.168.1.188	TCP	58	37497 → 14238 [SYN] Seq=...
276	12.761212702	10.0.2.15	192.168.1.188	TCP	58	37497 → 3030 [SYN] Seq=0...
277	12.761218450	10.0.2.15	192.168.1.188	TCP	58	37497 → 5999 [SYN] Seq=0...
278	12.761229796	10.0.2.15	192.168.1.188	TCP	58	37497 → 9595 [SYN] Seq=0...
279	12.761235874	10.0.2.15	192.168.1.188	TCP	58	37497 → 19780 [SYN] Seq=...
280	12.761241802	10.0.2.15	192.168.1.188	TCP	58	37497 → 3211 [SYN] Seq=0...
281	12.854106739	10.0.2.15	192.168.1.188	TCP	58	37499 → 1048 [SYN] Seq=0...
282	12.854124824	10.0.2.15	192.168.1.188	TCP	58	37499 → 16113 [SYN] Seq=...
283	12.854130241	10.0.2.15	192.168.1.188	TCP	58	37499 → 5922 [SYN] Seq=0...

Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface eth0	
Ethernet II, Src: PCSSystemtec_bd:09:d7 (08:00:27:10:00:00), Dst: 192.168.1.188 (08:00:00:08:00:20)	0000 52 54 00 12 35 02 08 00 27 bd 09 d7 08 00 45
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.188	0010 00 56 ea c1 40 00 40 06 f9 cf 0a 00 02 0f 22
Transmission Control Protocol, Src Port: 35820, Dst Port: 45567	0020 27 17 8b ec 01 bb c8 e9 d5 82 2a a7 89 60 50
Transport Layer Security	0030 7b fc 56 59 00 00 17 03 03 00 29 00 00 00 00
	0040 00 00 26 a1 49 d5 5d 59 f9 5e ad 29 f6 95 62
	0050 70 83 5e 5c 53 90 a0 37 65 40 83 ea a3 52 b7
	0060 ff 0d 7b a2

Tcp connect

Effettuando una TCP connect scan su Metasploitable con Nmap, ottieni una lista delle porte aperte e attive sul sistema target. Questa tecnica stabilisce una connessione completa (SYN, SYN/ACK, ACK) con ogni porta, quindi è meno discreta rispetto alla SYN scan, poiché spesso viene registrata nei log del sistema target.



No.	Time	Source	Destination	Protocol	Length	Info
3985	21.604999990	192.168.1.188	10.0.2.15	TCP	60	1600 → 59304 [RST, ACK] ...
3986	21.605000101	192.168.1.188	10.0.2.15	TCP	60	9485 → 37244 [RST, ACK] ...
3987	21.605397361	192.168.1.188	10.0.2.15	TCP	60	9010 → 56664 [RST, ACK] ...
3988	21.605729888	192.168.1.188	10.0.2.15	TCP	60	8085 → 38178 [RST, ACK] ...
3989	21.605729988	192.168.1.188	10.0.2.15	TCP	60	8001 → 51436 [RST, ACK] ...
3990	21.605826737	192.168.1.188	10.0.2.15	TCP	60	646 → 35178 [RST, ACK] S...
3991	21.605826847	192.168.1.188	10.0.2.15	TCP	60	7201 → 39088 [RST, ACK] ...
3992	21.605826897	192.168.1.188	10.0.2.15	TCP	60	1999 → 40142 [RST, ACK] ...
3993	21.606199454	192.168.1.188	10.0.2.15	TCP	60	146 → 45716 [RST, ACK] S...
3994	21.606199564	192.168.1.188	10.0.2.15	TCP	60	3333 → 46702 [RST, ACK] ...
3995	21.606199604	192.168.1.188	10.0.2.15	TCP	60	50001 → 57542 [RST, ACK]...
3996	21.606404435	192.168.1.188	10.0.2.15	TCP	60	7103 → 47332 [RST, ACK] ...
3997	21.606739812	192.168.1.188	10.0.2.15	TCP	60	1100 → 45402 [RST, ACK] ...
3998	21.607085581	192.168.1.188	10.0.2.15	TCP	60	6969 → 35588 [RST, ACK] ...
3999	21.607085682	192.168.1.188	10.0.2.15	TCP	60	3945 → 41270 [RST, ACK] ...
4000	21.607110426	192.168.1.188	10.0.2.15	TCP	60	1040 → 41030 [RST, ACK] ...
4001	21.610668215	192.168.1.188	10.0.2.15	TCP	60	10003 → 34158 [RST, ACK]...
4002	21.610738912	192.168.1.188	10.0.2.15	TCP	60	8089 → 56560 [RST, ACK] ...

Offset	Length	Protocol	Info
0000	33	33	00 00 00 02 08 00 27 bd 09 d7 81 00 00
0010	86	dd	60 0a 8a 9d 00 08 3a ff fe 80 00 00 00
0020	00	00	f5 4b 67 b9 ed 72 4b 1b ff 02 00 00 00
0030	00	00	00 00 00 00 00 00 00 00 00 00 02 85 00 e7 a3 00
0040	00	00	

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0
Ethernet II, Src: PCSSTemtec_bd:09:d7 (08:00:27:09:d7:81), Dst: Virtual LAN (08:00:00:00:00:00)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
Internet Protocol Version 6, Src: fe80::f54b:67b9:ed72:4b1b, Dst: :::::85
0110 = Version: 6
.... 0000 0000 = Traffic Class: 0x00
.... 1010 1000 1010 1001 1101 = Flow Label: 0xa8
Payload Length: 8
Next Header: ICMPv6 (58)
Hop Limit: 255
Source Address: fe80::f54b:67b9:ed72:4b1b

Effettuando una version detection su Metasploitable con Nmap, ottieni informazioni dettagliate sui servizi in esecuzione sulle porte aperte, inclusa la versione specifica di ciascun servizio. Questa tecnica invia varie richieste ai servizi e analizza le risposte per identificare con precisione il software e la versione. Le informazioni raccolte ti permettono di identificare potenziali vulnerabilità specifiche per quelle versioni dei servizi. La version detection è fondamentale per una valutazione approfondita della sicurezza del sistema.

```
File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:56 CEST
Nmap scan report for 192.168.1.188
Host is up (0.0056s latency).
Not shown: 978 filtered tcp ports (no-response)
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
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  tcpwrapped
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  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          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel
```

Effettuando l'OS fingerprint su un sistema Windows 7 con Nmap, ottieni informazioni dettagliate sul sistema operativo in esecuzione, come la versione specifica di Windows e i dettagli sulla rete. Questo processo analizza le risposte ai pacchetti TCP/IP per determinare il sistema operativo. Le informazioni raccolte ti permettono di identificare vulnerabilità specifiche associate a quella versione di Windows.

Conoscere il sistema operativo esatto è fondamentale per pianificare ulteriori test di sicurezza e individuare exploit mirati. L'OS fingerprinting fornisce un quadro chiaro del sistema, aiutandoti a comprendere meglio la sua configurazione e le sue potenziali debolezze.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.1.229  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 15:38 CEST  
Nmap scan report for 192.168.1.229  
Host is up (0.0046s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49157/tcp open  unknown  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge|general purpose|switch  
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450  
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)  
No exact OS matches for host (test conditions non-ideal).  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 14.75 seconds  
  
(kali@kali)-[~]
```


Il problema per quanto riguarda la macchina di windows 7 è che aprte con un'impostazione di firewall che impedisce il ping alla macchina, per effettuare questa scansione è quindi necessario disattivare il firewall che si mette nel mezzo, ho tentao di ottenere una risposta inserendo un -T1 -Pn ma il tempo di attesa eccessivo non mi ha permesso di riscontrare un risultato utile in tempo. Risulta quindi necessario disattivare il firewall manualmente o tramite exploit.

```
kali@kali: ~  
File Actions Edit View Help  
All 1000 scanned ports on 192.168.1.229 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/  
.  
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds  
  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.1.229  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 15:26 CEST  
Nmap scan report for 192.168.1.229  
Host is up (0.0070s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
49152/tcp open  msrpc        Microsoft Windows RPC  
49153/tcp open  msrpc        Microsoft Windows RPC  
49154/tcp open  msrpc        Microsoft Windows RPC  
49155/tcp open  msrpc        Microsoft Windows RPC  
49157/tcp open  msrpc        Microsoft Windows RPC  
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/  
.  
Nmap done: 1 IP address (1 host up) scanned in 71.16 seconds  
  
(kali@kali)-[~]  
$
```

