Report di Pandolfi Luciano sull'utilizzo di NETCAT e NMAP con relativa verifica di connessione e scansione di rete (con Wireshark) tra Server (Metasploitable2) e Client (Kali Linux)

- Per prima cosa ho aperto un listener per le connessioni in entrata sul lato Server assegnando un numero di porta (1234);
- Successivamente ho eseguito sul lato Client il comando che permette di reindirizzare una shell sul nostro Sistema, potendo così avere il controllo della macchina tramite terminale.

In seguito dal terminale Client ho eseguito diversi tipi di scan sulla macchina metasploitable2 con nmap:

- Scansione TCP sulle porte well-known;
- Scansione SYN sulle porte well-known;
- Scansione con switch «A» sulle porte well-known.

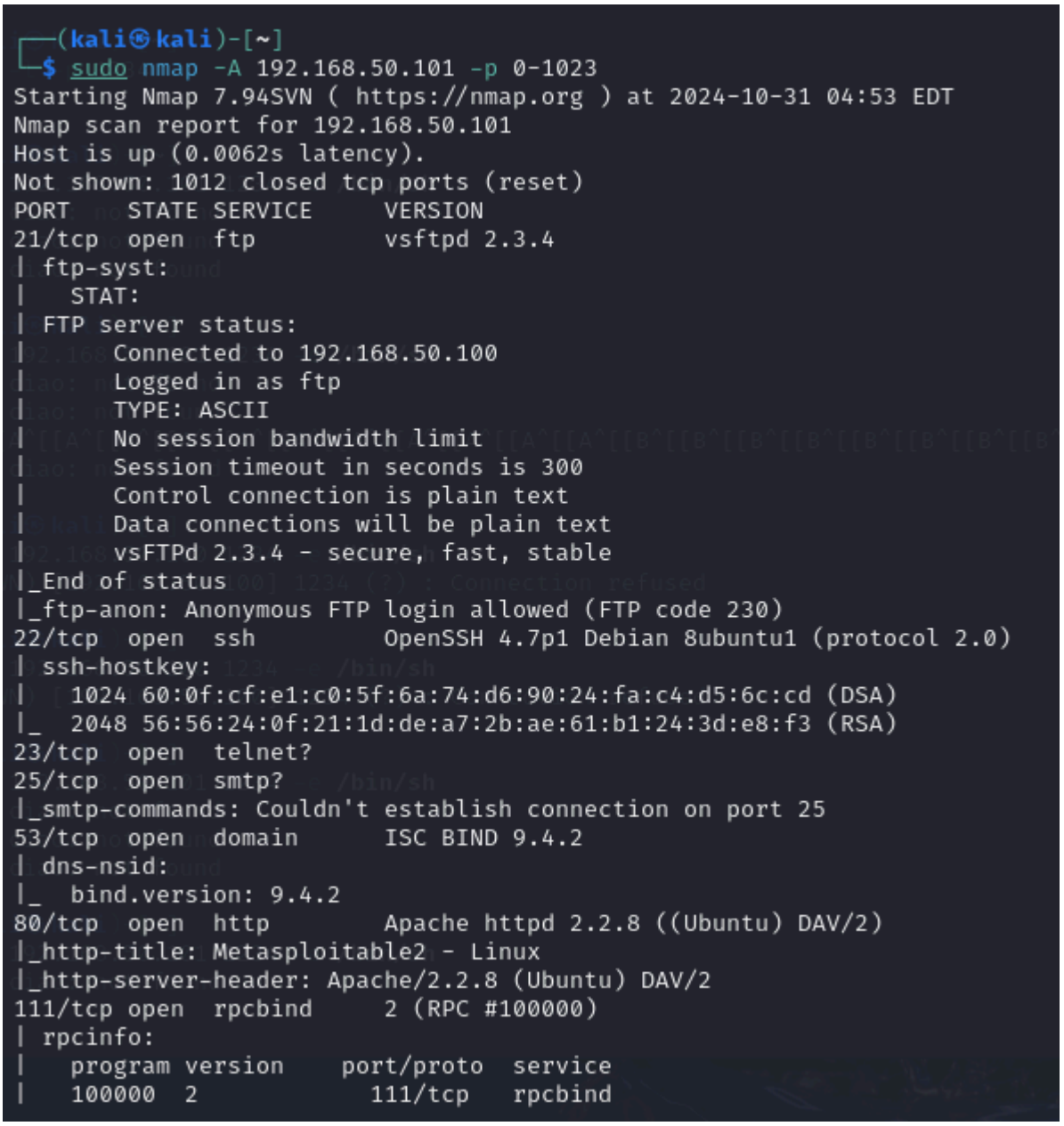
Report di Scansione dei Servizi di Rete

Fonte dello Scan	Target dello Scan	Tipo di Scan	Risultati Ottenuti
Nmap	192.168.50.101	-sS (TCP SYN Scan)	Trovati 12 servizi attivi; Porte aperte: 80,25,53,22,23,111,139,21,445,513,514,512.
Nmap	192.168.50.101	-sT (TCP Connect Scan)	Trovati 12 servizi attivi; Porte aperte: 80,22,139,53,445,25,23,21,111,514,512,513.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 0-1023
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 17:10 EDT
Nmap scan report for 192.168.50.101
Host is up (0.017s latency).
Not shown: 1012 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
MAC Address: 08:00:27:76:FA:58 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.33 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 0-1023
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 03:51 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0084s latency).
Not shown: 1012 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
MAC Address: 08:00:27:76:FA:58 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
```

Scansione con switch «-A» sulle porte well-known, mii ha permesso di recuperare molte informazioni utili sull'ip target, preziose per le fasi successive, come la versione del sistema operativo e dei servizi disponibili in ascolto sulle porte aperte.



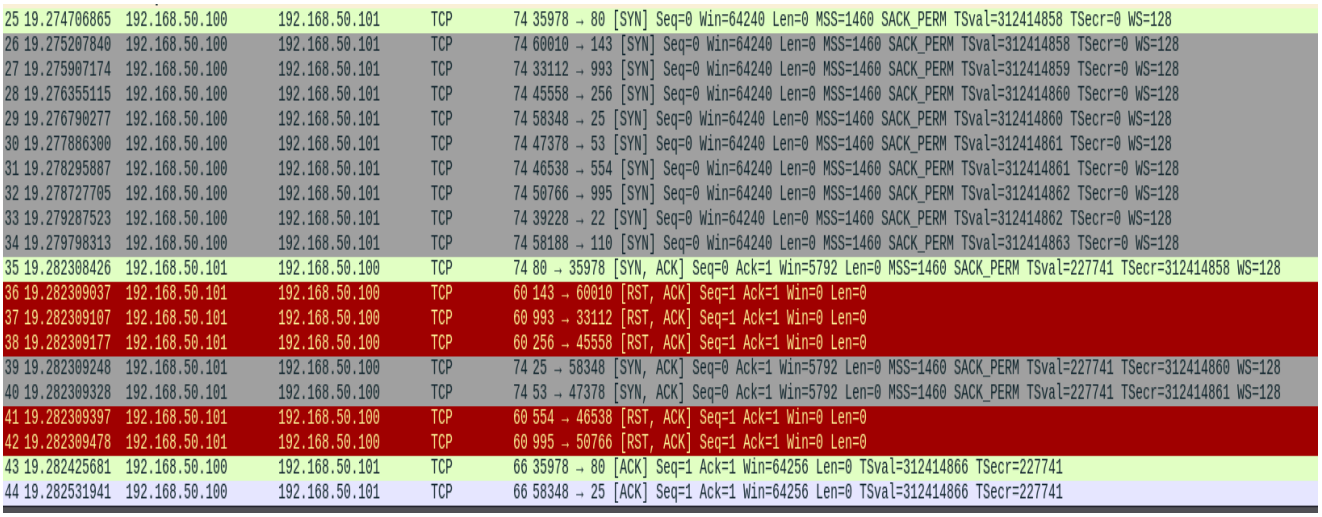
```
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45725/udp   mountd
|   100005  1,2,3      57469/tcp   mountd
|   100021  1,3,4      35703/udp   nlockmgr
|   100021  1,3,4      51114/tcp   nlockmgr
|   100024  1          48081/tcp   status
|_  100024  1          55859/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec?
513/tcp open  login?
514/tcp open  shell?
MAC Address: 08:00:27:76:FA:58 (Oracle VirtualBox virtual NIC)
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=7.94SVN%E=4%D=10/31%OT=21%CT=1%CU=38037%PV=Y%DS=1%DC=D%G=Y%M=0800
OS:27%TM=672346D7%P=x86_64-pc-linux-gnu)SEQ(SP=C3%GCD=1%ISR=CA%TI=Z%CI=Z%II
OS:=I%TS=5)SEQ(SP=C3%GCD=1%ISR=CB%TI=Z%CI=Z%II=I%TS=5)SEQ(SP=C4%GCD=1%ISR=C
OS:B%TI=Z%CI=Z%II=I%TS=5)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%
OS:O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4
OS:=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R
OS:=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=
OS:S+%F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A
OS:%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=40%CD=S)

Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1d11h36m50s, deviation: 2h49m43s, median: -1d13h36m51s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-10-29T15:20:09-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   6.23 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 313.22 seconds
```

Differenze tra Scansione Completa TCP (-sT) e Scansione SYN (-sS), prendendo come riferimento in figura la porta nota 80 (http).

Scansione Completa TCP (-sT):

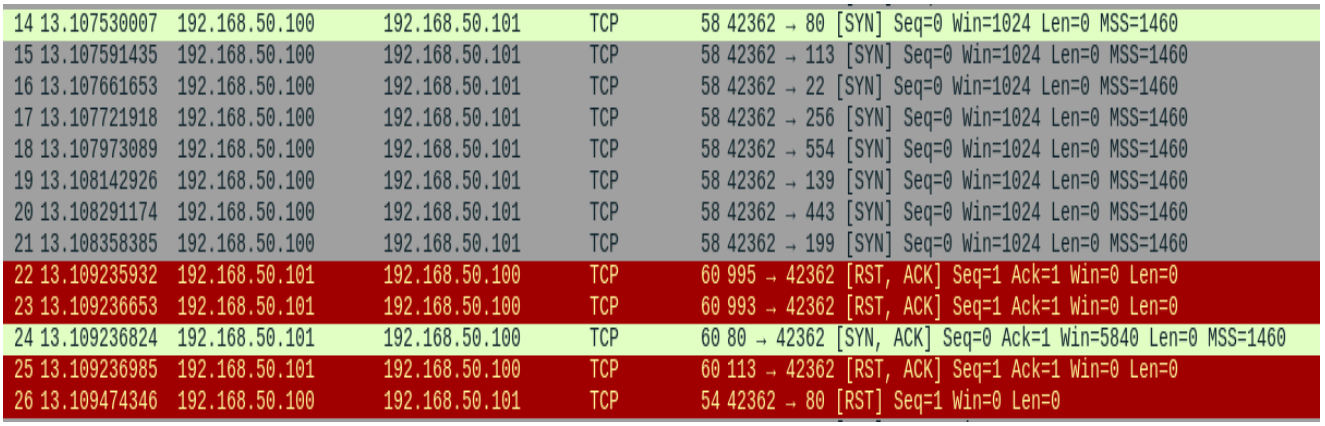
- Stabilisce una connessione "three-way handshake" (SYN, SYN-ACK, ACK) per ogni porta aperta;
- Può essere rilevata facilmente dai sistemi di sicurezza, poiché stabilisce connessioni complete;
- Nel traffico catturato, puoi vedere sequenze di pacchetti SYN, SYN-ACK, ACK, ogni connessione verrà mostrata come un flusso completo quando la porta è aperta;
- Se la porta è chiusa dopo il SYN iniziale restituisce [RST, ACK].



25	19.274706865	192.168.50.100	192.168.50.101	TCP	74 35978 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414858 TSecr=0 WS=128
26	19.275207840	192.168.50.100	192.168.50.101	TCP	74 60010 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414858 TSecr=0 WS=128
27	19.275907174	192.168.50.100	192.168.50.101	TCP	74 33112 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414859 TSecr=0 WS=128
28	19.276355115	192.168.50.100	192.168.50.101	TCP	74 45558 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414860 TSecr=0 WS=128
29	19.276790277	192.168.50.100	192.168.50.101	TCP	74 58348 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414860 TSecr=0 WS=128
30	19.277886300	192.168.50.100	192.168.50.101	TCP	74 47378 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414861 TSecr=0 WS=128
31	19.278295887	192.168.50.100	192.168.50.101	TCP	74 46538 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414861 TSecr=0 WS=128
32	19.278727705	192.168.50.100	192.168.50.101	TCP	74 50766 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414862 TSecr=0 WS=128
33	19.279287523	192.168.50.100	192.168.50.101	TCP	74 39228 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414862 TSecr=0 WS=128
34	19.279798313	192.168.50.100	192.168.50.101	TCP	74 58188 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=312414863 TSecr=0 WS=128
35	19.282308426	192.168.50.101	192.168.50.100	TCP	74 80 → 35978 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=227741 TSecr=312414858 WS=128
36	19.282309037	192.168.50.101	192.168.50.100	TCP	60 143 → 60010 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	19.282309107	192.168.50.101	192.168.50.100	TCP	60 993 → 33112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	19.282309177	192.168.50.101	192.168.50.100	TCP	60 256 → 45558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	19.282309248	192.168.50.101	192.168.50.100	TCP	74 25 → 58348 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=227741 TSecr=312414860 WS=128
40	19.282309328	192.168.50.101	192.168.50.100	TCP	74 53 → 47378 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=227741 TSecr=312414861 WS=128
41	19.282309397	192.168.50.101	192.168.50.100	TCP	60 554 → 46538 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	19.282309478	192.168.50.101	192.168.50.100	TCP	60 995 → 50766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	19.282425681	192.168.50.100	192.168.50.101	TCP	66 35978 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=312414866 TSecr=227741
44	19.282531941	192.168.50.100	192.168.50.101	TCP	66 58348 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=312414866 TSecr=227741

Scansione SYN (-sS):

- Utilizza solo il pacchetto SYN per inviare la richiesta.
- Non completa il "three-way handshake" (manca l'ACK finale), rendendo la scansione meno rilevabile.
- I sistemi target dopo il tipico [SYN] risponderanno con un [SYN-ACK] e successivamente [RST] se la porta è aperta non completando la connessione;
- Risponde invece direttamente con un [RST, ACK] se è chiusa.



14	13.107530007	192.168.50.100	192.168.50.101	TCP	58 42362 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	13.107591435	192.168.50.100	192.168.50.101	TCP	58 42362 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13.107661653	192.168.50.100	192.168.50.101	TCP	58 42362 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	13.107721918	192.168.50.100	192.168.50.101	TCP	58 42362 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	13.107973089	192.168.50.100	192.168.50.101	TCP	58 42362 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	13.108142926	192.168.50.100	192.168.50.101	TCP	58 42362 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	13.108291174	192.168.50.100	192.168.50.101	TCP	58 42362 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	13.108358385	192.168.50.100	192.168.50.101	TCP	58 42362 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	13.109235932	192.168.50.101	192.168.50.100	TCP	60 995 → 42362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.109236653	192.168.50.101	192.168.50.100	TCP	60 993 → 42362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	13.109236824	192.168.50.101	192.168.50.100	TCP	60 80 → 42362 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	13.109236985	192.168.50.101	192.168.50.100	TCP	60 113 → 42362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	13.109474346	192.168.50.100	192.168.50.101	TCP	54 42362 → 80 [RST] Seq=1 Win=0 Len=0