


ESERCITAZIONE WEEK 9 DAY 3

 **EPICODE**


Esercizio
Nmap scan

Traccia:

Vedremo da vicino nmap e i suoi comandi.
Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

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

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

 **EPICODE**

W9D1 - Pratica (2) PDF

Esercizio
Nmap scan

Traccia:

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine.
E' molto importante in questa fase essere organizzati e strutturati.
Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:

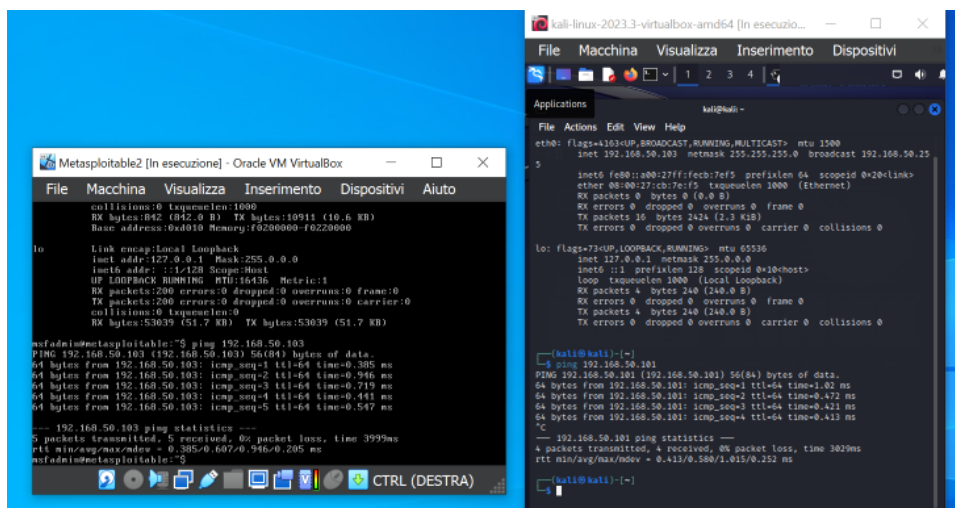
- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

Configurazione delle macchine virtuali:

Per questo esercizio configuriamo due macchine sulla stessa rete in comunicazione tra loro e in modalità interna, in particolare:

- **Kali Linux** sarà la macchina che eseguirà le scansioni verso il target, con indirizzo IP 192.168.50.103;
- **Metasploitable** sarà la macchina bersaglio, con indirizzo IP 192.168.50.101;

Eseguiamo il comando **ping** su entrambe le macchine per verificarne la connessione reciproca:



```
metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

collisions:0 txqueuelen:1000
RX bytes:842 (842.0 B) TX bytes:10911 (10.6 KB)
Base address:0x0010 Memory:f0200000-f0200000

lo:
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:200 errors:0 dropped:0 overruns:0 frame:0
TX packets:200 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:53039 (51.7 KB) TX bytes:53039 (51.7 KB)

mafadin@metasploitable:~$ ping 192.168.50.103
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data:
64 bytes from 192.168.50.103: icmp_seq=1 ttl=64 time=0.305 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=64 time=0.346 ms
64 bytes from 192.168.50.103: icmp_seq=3 ttl=64 time=0.719 ms
64 bytes from 192.168.50.103: icmp_seq=4 ttl=64 time=0.451 ms
64 bytes from 192.168.50.103: icmp_seq=5 ttl=64 time=0.547 ms
--- 192.168.50.103 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.305/0.607/0.946/0.205 ms
mafadin@metasploitable:~$

kali-linux-2023.3-virtualbox-amd64 [In esecuzione...]
File  Macchina  Visualizza  Inserimento  Dispositivi

Applications  kali@kali: ~
File  Actions  Edit  View  Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.50.103 netmask 255.255.255.0 broadcast 192.168.50.255
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 2424 (2.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.472 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.421 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.413 ms
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 0.413/0.586/1.015/0.252 ms
kali@kali:~$
```

Scansione TCP sulle porte well-known

Si esegue il comando **nmap -sT 192.168.50.101 -p 0-1023** e si monitora il traffico con Wireshark.

- L'opzione **-sT** serve per richiedere al tool una scansione più invasiva, che analizzi lo stato delle porte well-known (per convenzione le prime 1024), attendendo che avvenga completamente il meccanismo di 3-way-handshake.
- Si specifica l'indirizzo IP della macchina target, ovvero Metasploitable.
- L'opzione **-p** specifica il range di porte da scannerizzare.

```
(kali@kali)-[~]
$ nmap -sT 192.168.50.101 -p 0-1023
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 14:46 EST
Nmap scan report for 192.168.50.101
Host is up (0.00017s 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

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

(kali@kali)-[~]
$
```

Analizzando la risposta di tale comando, si evince che il tool ha in 13.09 s eseguito una scansione sul target all'indirizzo IP 192.168.50.101, trovando 1012 porte tcp chiuse che decide di non elencare, facendo dunque solo una lista delle porte trovate aperte, indicandone il servizio esposto. Un commento su questi risultati è riportato nella tabella Table1.

Analizzando il traffico su Wireshark, si può notare che ad esempio è stata tentata la connessione da parte della macchina Kali Linux (192.168.50.103) verso Metasploitable (192.168.50.101) alla porta 80, destinata al servizio HTTP.

Time	Source	Destination	Protocol	Length	Info
1.0.000000000	192.168.50.101	192.168.50.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation
2.0.000000405	192.168.50.101	192.168.50.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
3.344.654511884	fe80::a00:27ff:feeb::ff02::2	ff02::2	ICMPv6	70	Router Solicitation from 08:00:27:cb:7e:f5
4.359.995353796	192.168.50.101	192.168.50.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation
5.359.995354215	192.168.50.101	192.168.50.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
6.368.705731110	192.168.50.103	192.168.50.101	TCP	74	42682 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM TSval=585618811 TSecr=0 WS=128
7.366.770656808	192.168.50.103	192.168.50.101	TCP	74	57826 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM TSval=585618811 TSecr=0 WS=128
8.366.774225924	PcsCompu_84:48:ba	Broadcast	ARP	60	Who has 192.168.50.103? Tell 192.168.50.101
9.366.774236668	PcsCompu_cb:7e:f5	PcsCompu_84:48:ba	ARP	42	192.168.50.103 is at 08:00:27:cb:7e:f5
10.366.774373304	192.168.50.101	192.168.50.103	TCP	74	80 → 42682 [SYN, ACK] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=97541 TSecr=585618811 WS=128
11.366.774373359	192.168.50.101	192.168.50.103	TCP	60	443 → 57826 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12.366.774395357	192.168.50.103	192.168.50.101	TCP	66	42682 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=585618815 TSecr=97541
13.366.774450710	192.168.50.103	192.168.50.101	TCP	66	42682 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=585618815 TSecr=97541
14.366.774658318	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.17? Tell 192.168.50.103
15.367.790118385	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.17? Tell 192.168.50.103
16.368.813891756	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.17? Tell 192.168.50.103
17.371.790212868	PcsCompu_cb:7e:f5	PcsCompu_84:48:ba	ARP	42	Who has 192.168.50.101? Tell 192.168.50.103
18.371.790821284	PcsCompu_84:48:ba	PcsCompu_cb:7e:f5	ARP	60	192.168.50.101 is at 08:00:27:84:48:ba
19.373.277907258	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.17? Tell 192.168.50.103
20.374.286179551	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.17? Tell 192.168.50.103
21.375.310904804	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.17? Tell 192.168.50.103

In particolare:

- Dalla sorgente Kali Linux con IP 192.168.50.103 e porta randomicamente assegnata su 42682, viene inviato un pacchetto sulla porta 80 di Metasploitable con IP 192.168.50.101 avente il flag SYN attivo e valore di sequence number pari a 2153859007:

```

[Stream index: 0]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2153859007
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
  Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0xe64b [unverified]
    [Checksum Status: Unverified]
0000 08 00 27 84 48 ba 08 00 27 cb 7e f5 08 00 45 00  ..H...E
0010 00 3c 4d bd 40 00 40 06 06 e2 c0 a8 32 67 c0 a8  <M@...2g
0020 32 65 a6 ba 00 50 80 61 47 bf 00 00 00 00 a0 02  2e...PaG
0030 fa f0 e6 4b 00 00 02 04 05 b4 04 02 08 0a 22 e7  ..K....."
0040 d5 7b 00 00 00 00 01 03 03 07  ..{.....

```

- La macchina target risponde con il flag SYN a ACK attivi, spedendo nel pacchetto un sequence number pari a 1054368308 e un acknowledge number pari al precedente sequence number +1: 2153859008;

```

* Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
* Ethernet II, Src: PcsCompu_84:48:ba (08:00:27:84:48:ba), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
* Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.103
* Transmission Control Protocol, Src Port: 80, Dst Port: 42682, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 42682
  [Stream index: 0]
  [Conversation completeness: Complete, NO_DATA (39)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1054368308
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2153859008
0000 08 00 27 cb 7e f5 08 00 27 84 48 ba 08 00 45 00  ..H...E
0010 00 3c 00 00 40 00 40 06 54 9f c0 a8 32 65 c0 a8  <@...T...2e
0020 32 67 00 50 a6 ba 3e d8 62 34 80 61 47 c0 a0 12  2gP...>b4aG
0030 16 a0 c5 90 00 00 02 04 05 b4 04 02 08 0a 00 01  ..C....."
0040 7d 05 22 e7 d5 7b 01 03 03 07  }...{.....

```

- Kali Linux risponderà verso la macchina target con un pacchetto avente un sequence number pari a 2153859008 e un acknowledge number pari al sequence number ricevuto in precedenza +1: 1054368309;

```

Wireshark - Packet 12 - eth0
* Frame 12: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
* Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_84:48:ba (08:00:27:84:48:ba)
* Internet Protocol Version 4, Src: 192.168.50.103, Dst: 192.168.50.101
* Transmission Control Protocol, Src Port: 42682, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 42682
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Complete, NO_DATA (39)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2153859008
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1054368309
0000 08 00 27 84 48 ba 08 00 27 cb 7e f5 08 00 45 00  ..H...E
0010 00 34 4d be 40 00 40 06 06 e9 c0 a8 32 67 c0 a8  4M@...2g
0020 32 65 a6 ba 00 50 80 61 47 c0 3e d8 62 35 80 10  2e...PaG>b5
0030 01 f6 e6 43 00 00 01 01 08 0a 22 e7 d5 7f 00 01  ..C....."
0040 7d 05  ..{.....

```

- Essendosi concluso positivamente il 3-way-handshake, la porta viene dichiarata come aperta. Viene infine mandato un segnale di reset RST dalla macchina attaccante verso quella target:

```

Wireshark - Packet 13 - eth0
* Transmission Control Protocol, Src Port: 42682, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 42682
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Complete, NO_DATA (39)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2153859008
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1054368309
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x014 (RST, ACK)
    Window: 562
    [Calculated window size: 642561]
0000 08 00 27 84 48 ba 08 00 27 cb 7e f5 08 00 45 00  ..H...E
0010 00 34 4d bf 40 00 40 06 06 e8 c0 a8 32 67 c0 a8  4M@...2g
0020 32 65 a6 ba 00 50 80 61 47 c0 3e d8 62 35 80 14  2e...PaG>b5
0030 01 f6 e6 43 00 00 01 01 08 0a 22 e7 d5 7f 00 01  ..C....."
0040 7d 05  ..{.....

```

Questo meccanismo si ripete su altre porte, ad esempio la porta 53 che risulta aperta, mentre su altre porte viene mandato il flag SYN, non viene ricevuto il pacchetto contenente SYN-ACK e quindi in quel caso non si stabilisce un canale di connessione, per cui vengono considerate chiuse. Ad esempio per la porta 443, non si riceve in risposta al SYN, il SYN-ACK ma direttamente un segnale di RST (reset):

BROWSER	286	Local Master Announcement	METASPLOITABLE, WORKSTATION,
BROWSER	257	Domain/Workgroup Announcement	WORKGROUP, NT Workstation
TCP	74	42682 → 80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
TCP	74	57826 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
ARP	60	Who has 192.168.50.103?	Tell 192.168.50.101
ARP	42	192.168.50.103 is at	08:00:27:cb:7e:f5
TCP	74	80 → 42682	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
TCP	60	443 → 57826	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	66	42682 → 80	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=5856
TCP	66	42682 → 80	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
ARP	42	Who has 192.168.50.1?	Tell 192.168.50.103
ARP	42	Who has 192.168.50.1?	Tell 192.168.50.103
ARP	42	Who has 192.168.50.103?	Tell 192.168.50.103

Scansione SYN sulle porte well-known

Come si evince dalla figura, questo comando richiede i privilegi di amministratore per cui si invia il comando **sudo nmap -sS 192.168.50.101 -p 0-1023**.

L'opzione -sS serve per avviare una scansione sulle porte TCP meno invasiva, poiché non si attende il completamento del 3-way-handshake. Dettagli sui risultati ottenuti si rimandano al paragrafo di report.

```
(kali@kali)-[~]
$ nmap -sS 192.168.50.101 -p 0-1023
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101 -p 0-1023
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 14:51 EST
Nmap scan report for 192.168.50.101
Host is up (0.00034s latency).
Not shown: 1012 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
MAC Address: 08:00:27:BB:E2:2B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.24 seconds
```

Dall'acquisizione del traffico Wireshark, a seguito del segnale di SYN inviato da Kali Linux, la macchina target risponde con SYN-ACK e subito dopo la macchina attaccante manda un segnale di reset RST.

Esempio sulla porta 80:

192.168.50.103	192.168.50.101	TCP	58 45761 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.50.103	192.168.50.101	TCP	58 45761 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.50.103	192.168.50.101	TCP	58 45761 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.50.103	192.168.50.101	TCP	58 45761 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.50.103	192.168.50.101	TCP	58 45761 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.50.103	192.168.50.101	TCP	58 45761 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.50.101	192.168.50.103	TCP	60 256 → 45761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.50.101	192.168.50.103	TCP	60 111 → 45761 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.50.101	192.168.50.103	TCP	60 554 → 45761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.50.101	192.168.50.103	TCP	60 113 → 45761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.50.101	192.168.50.103	TCP	60 587 → 45761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.50.101	192.168.50.103	TCP	60 445 → 45761 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.50.101	192.168.50.103	TCP	60 443 → 45761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.50.101	192.168.50.103	TCP	60 80 → 45761 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.50.103	192.168.50.101	TCP	54 45761 → 111 [RST] Seq=1 Win=0 Len=0
192.168.50.103	192.168.50.101	TCP	54 45761 → 445 [RST] Seq=1 Win=0 Len=0
192.168.50.103	192.168.50.101	TCP	54 45761 → 80 [RST] Seq=1 Win=0 Len=0
192.168.50.101	192.168.50.103	TCP	60 110 → 45761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- La macchina Kali Linux con IP 192.168.50.103 invia dalla porta assegnata random 45761, un pacchetto sulla porta 80 della macchina Metasploitable con IP 192.168.50.101, con il flag SYN attivo e sequence number pari a 1033523943:

```

> Frame 16: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_84:48:ba (08:00:27:84:48:ba)
> Internet Protocol Version 4, Src: 192.168.50.103, Dst: 192.168.50.101
> Transmission Control Protocol, Src Port: 45761, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 45761
  Destination Port: 80
  [Stream index: 7]
  [Conversation completeness: Incomplete (35)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1033523943
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  0110 .... = Header Length: 24 bytes (6)
0000 08 00 27 84 48 ba 08 00 27 cb 7e f5 08 00 45 00  ..H...T...E...
0010 00 2c 89 3e 00 00 36 06 15 71 c0 a8 32 67 c0 a8  .,.>...6...q...2g...
0020 32 65 b2 c1 00 50 3d 9a 52 e7 00 00 00 60 02    2e...P...R...
0030 04 00 6a 76 00 00 02 04 05 b4                  .jV...

```

- La macchina target risponde con il flag SYN e ACK attivo, mandando un pacchetto che ha un sequence number 3703266247 e un acknowledge number pari al precedente sequence number +1: 1033523944.

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 45761, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 45761
  [Stream index: 7]
  [Conversation completeness: Incomplete (35)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3703266247
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1033523944
  0110 .... = Header Length: 24 bytes (6)
> Flags: 0x012 (SYN, ACK)
  Window: 5840
  [Calculated window size: 5840]
0000 08 00 27 cb 7e f5 08 00 27 84 48 ba 08 00 45 00  ..H...T...E...
0010 00 2c 00 00 40 00 40 06 54 af c0 a8 32 65 c0 a8  .,.>...@...T...2e...
0020 32 67 00 50 b2 c1 dc bb 5b c7 3d 9a 52 e8 60 12    2g P...[...= R...
0030 16 d0 1f 12 00 00 02 04 05 b4 00 00             .....

```

- La macchina attaccante interrompe la comunicazione con un segnale di reset RST. Il sequence number sarà 1033523944, mentre non essendoci un acknowledge number, si può notare che è pari a 0:


```

> Frame 29: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_84:48:ba (08:00:27:84:48:ba)
> Internet Protocol Version 4, Src: 192.168.50.103, Dst: 192.168.50.101
~ Transmission Control Protocol, Src Port: 45761, Dst Port: 80, Seq: 1, Len: 0
  Source Port: 45761
  Destination Port: 80
  [Stream index: 7]
  [Conversation completeness: Incomplete (35)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1033523944
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  0101 .... = Header length: 20 bytes (5)
0000 08 00 27 84 48 ba 08 00 27 cb 7e f5 08 00 45 00 ...H...T...E...
0010 00 28 00 00 40 00 40 06 54 b3 c0 a8 32 67 c0 a8 ...@...T...2g...
0020 32 65 b2 c1 00 50 3d 9a 52 e8 00 00 00 00 00 04 2e...P...R...
0030 00 00 06 2f 00 00 .../...

```

Abbiamo così evidenziato la differenza tra i due tipi di scansione TCP.

Scansione con switch -A sulle porte well-known

```

(kali㉿kali)-[~]
└─$ nmap -A 192.168.50.101 -p 0-1023
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 15:00 EST
Nmap scan report for 192.168.50.101
Host is up (0.00051s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|  STAT:
|  FTP server status:
|    Connected to 192.168.50.103
|    Logged in as ftp
|    TYPE: ASCII
|    No session bandwidth limit
|    Session timeout in seconds is 300
|    Control connection is plain text
|    Data connections will be plain text
|    vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open  domain      ISC BIND 9.4.2
|_dns-nsid:
|  bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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         41021/udp  mountd
|  100005  1,2,3         43224/tcp  mountd
|  100021  1,3,4         39708/udp  nlockmgr
|  100021  1,3,4         52720/tcp  nlockmgr
|  100024  1             32768/udp  status
|  100024  1             59410/tcp  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?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: -4h36m51s, deviation: 3h32m08s, median: -7h06m52s
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-12-20T07:56:45-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MA
C: <unknown> (unknown)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 321.40 seconds

```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.090000000	192.168.50.103	192.168.50.101	ICMPv6	70	Router Solicitation from 08:00:27:cb:7e:f5
2	12.231173396	192.168.50.103	192.168.50.101	TCP	74	58748 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=453989351 TSecr=0 WS=128
3	12.231204127	192.168.50.103	192.168.50.101	TCP	74	55128 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=453989351 TSecr=0 WS=128
4	12.231464963	192.168.50.101	192.168.50.103	TCP	74	80 → 58748 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=849887 TSecr=453989351
5	12.231465334	192.168.50.101	192.168.50.103	TCP	60	443 → 55128 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	12.231509978	192.168.50.103	192.168.50.101	TCP	66	58748 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=453989352 TSecr=849887
7	12.231583385	192.168.50.103	192.168.50.101	TCP	66	58748 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=453989352 TSecr=849887
8	12.232299806	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
9	13.252027904	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
10	14.284711990	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
11	17.408831569	PcsCompu_cb:7e:f5	PcsCompu_bb:e2:2b	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
12	17.408862139	PcsCompu_bb:e2:2b	PcsCompu_cb:7e:f5	ARP	60	192.168.50.101 is at 08:00:27:bb:e2:2b
13	18.736422391	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
14	19.743950573	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
15	20.767778909	PcsCompu_cb:7e:f5	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.103
16	25.237926312	192.168.50.103	192.168.50.101	TCP	74	37864 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=454002358 TSecr=0 WS=128
17	25.237979333	192.168.50.103	192.168.50.101	TCP	74	38380 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=454002358 TSecr=0 WS=128
18	25.238049358	192.168.50.103	192.168.50.101	TCP	74	34120 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=454002358 TSecr=0 WS=128

No.	Time	Source	Destination	Protocol	Length	Info
2610	66.448355613	192.168.50.103	192.168.50.101	EXEC	72	Client -> Server data
2611	66.448429722	192.168.50.101	192.168.50.103	TCP	74	514 → 50756 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=855336 TSecr=454043568
2612	66.448429936	192.168.50.101	192.168.50.103	TCP	66	25 → 52956 [ACK] Seq=1 Ack=45 Win=5824 Len=0 TSval=855336 TSecr=454043568
2613	66.448430009	192.168.50.101	192.168.50.103	TCP	66	23 → 35762 [ACK] Seq=1 Ack=15 Win=5824 Len=0 TSval=855336 TSecr=454043568
2614	66.448430085	192.168.50.101	192.168.50.103	TCP	66	512 → 58868 [ACK] Seq=1 Ack=7 Win=5824 Len=0 TSval=855336 TSecr=454043568
2615	66.448452610	192.168.50.103	192.168.50.101	TCP	66	50756 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=454043569 TSecr=855336
2616	66.448488375	192.168.50.103	192.168.50.101	RSH	72	Client -> Server data
2617	66.448616251	192.168.50.101	192.168.50.103	TCP	66	514 → 50756 [ACK] Seq=1 Ack=7 Win=5824 Len=0 TSval=855336 TSecr=454043569
2618	66.487670767	192.168.50.101	192.168.50.103	TCP	66	25 → 48868 [ACK] Seq=1 Ack=24 Win=5824 Len=0 TSval=855340 TSecr=454043568
2619	66.487677490	192.168.50.101	192.168.50.103	TCP	66	23 → 59466 [ACK] Seq=1 Ack=34 Win=5824 Len=0 TSval=855340 TSecr=454043568
2620	66.487677508	192.168.50.101	192.168.50.103	TCP	66	512 → 39432 [ACK] Seq=1 Ack=16 Win=5824 Len=0 TSval=855340 TSecr=454043568
2621	66.487677539	192.168.50.101	192.168.50.103	TCP	66	514 → 43390 [ACK] Seq=1 Ack=24 Win=5824 Len=0 TSval=855340 TSecr=454043568
2622	66.767064707	192.168.50.101	192.168.50.103	SMTP	121	S: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
2623	66.767133711	192.168.50.103	192.168.50.101	TCP	54	57214 → 25 [RST] Seq=8 Win=0 Len=0
2624	66.767378716	192.168.50.101	192.168.50.103	SMTP	107	S: 502 5.5.2 Error: command not recognized
2625	66.767422455	192.168.50.103	192.168.50.101	TCP	54	57214 → 25 [RST] Seq=8 Win=0 Len=0
2626	67.422929435	PcsCompu_bb:e2:2b	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.101

No.	Time	Source	Destination	Protocol	Length	Info
2770	84.299614455	192.168.50.101	192.168.50.103	TELNET	78	Telnet Data ...
2771	84.299614900	192.168.50.101	192.168.50.103	TCP	66	23 → 59464 [FIN, ACK] Seq=13 Ack=46 Win=5824 Len=0 TSval=857130 TSecr=454038564
2772	84.299614931	192.168.50.101	192.168.50.103	SMTP	121	S: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
2773	84.299664570	192.168.50.103	192.168.50.101	TCP	54	59464 → 23 [RST] Seq=46 Win=0 Len=0
2774	84.299668649	192.168.50.103	192.168.50.101	TCP	54	59464 → 23 [RST] Seq=46 Win=0 Len=0
2775	84.299674434	192.168.50.103	192.168.50.101	TCP	54	48798 → 25 [RST] Seq=24 Win=0 Len=0
2776	84.299708448	192.168.50.101	192.168.50.103	SMTP	136	S: 502 5.5.2 Error: command not recognized 500 5.5.2 Error: bad syntax
2777	84.299722693	192.168.50.103	192.168.50.101	TCP	54	48798 → 25 [RST] Seq=24 Win=0 Len=0
2778	84.309130949	192.168.50.101	192.168.50.103	EXEC	82	Server -> Client data
2779	84.309140211	192.168.50.101	192.168.50.103	TCP	66	512 → 39430 [RST, ACK] Seq=17 Ack=46 Win=5824 Len=0 TSval=857131 TSecr=454038564
2780	84.309140242	192.168.50.101	192.168.50.103	RSH	117	Server -> Client data
2781	84.309140271	192.168.50.101	192.168.50.103	TCP	66	514 → 43380 [RST, ACK] Seq=52 Ack=24 Win=5824 Len=0 TSval=857131 TSecr=454038564
2782	84.309165960	192.168.50.103	192.168.50.101	TCP	54	39430 → 512 [RST] Seq=46 Win=0 Len=0
2783	84.309184171	192.168.50.103	192.168.50.101	TCP	54	43380 → 514 [RST] Seq=24 Win=0 Len=0
2784	84.329379172	192.168.50.101	192.168.50.103	Rlogin	67	Data: \001
2785	84.329379662	192.168.50.101	192.168.50.103	TCP	66	513 → 53974 [RST, ACK] Seq=2 Ack=20 Win=5824 Len=0 TSval=857133 TSecr=454038560
2786	84.329417988	192.168.50.103	192.168.50.101	TCP	54	53974 → 513 [RST] Seq=20 Win=0 Len=0

L'opzione -A in Nmap è una scorciatoia che attiva diverse opzioni avanzate allo stesso tempo. Include l'identificazione del sistema operativo (-O), la rilevazione della versione del servizio (-sV), il rilevamento degli script di Nmap (--script), e altre informazioni dettagliate. L'opzione -A è comunemente chiamata "opzione di analisi avanzata". L'utilizzo dello switch -A rende la scansione più invasiva e può richiedere più tempo rispetto a una scansione più leggera. Può anche aumentare la probabilità di essere rilevato, poiché raccoglie

informazioni più dettagliate sulle risorse di rete. Si rimanda al paragrafo successivo per il dettaglio delle informazioni rilevate da questa scansione.

Tabella riassuntiva dei risultati ottenuti

Fonte scan	Target	Tipo di scan	Risultati
Kali Linux 192.168.50.103	Metasploitable 192.168.50.101	TCP completo	1012 porte tcp chiuse e non riportate; Porte aperte: 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
Kali Linux 192.168.50.103	Metasploitable 192.168.50.101	TCP - SYN	1012 porte tcp chiuse e non riportate; Porte aperte 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: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)
Kali Linux 192.168.50.103	Metasploitable 192.168.50.101	TCP switch -A (opzione di analisi avanzata)	Vedi pag 12-13. Accesso a FTP in modalità anonima; SSH: chiavi crittografiche RSA e DSA; Cifrari: SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC4_128_WITH_MD5

Kali Linux 192.168.50.103	Metasploitable 192.168.50.101	UDP	Ci sono 1018 porte udp chiuse e non riportate; <table><tr><th>PORT</th><th>STATE</th><th>SERVICE</th></tr><tr><td>53/udp</td><td>open</td><td>domain</td></tr><tr><td>69/udp</td><td>open filtered</td><td>tftp</td></tr><tr><td>111/udp</td><td>open</td><td>rpcbind</td></tr><tr><td>137/udp</td><td>open</td><td>netbios-ns</td></tr><tr><td>138/udp</td><td>open filtered</td><td>netbios-dgm</td></tr><tr><td>854/udp</td><td>open filtered</td><td>unknown</td></tr></table> MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)	PORT	STATE	SERVICE	53/udp	open	domain	69/udp	open filtered	tftp	111/udp	open	rpcbind	137/udp	open	netbios-ns	138/udp	open filtered	netbios-dgm	854/udp	open filtered	unknown
PORT	STATE	SERVICE																						
53/udp	open	domain																						
69/udp	open filtered	tftp																						
111/udp	open	rpcbind																						
137/udp	open	netbios-ns																						
138/udp	open filtered	netbios-dgm																						
854/udp	open filtered	unknown																						

Table 1-Analisi delle scansioni effettuate

Osservazioni sulle porte TCP aperte

Sono state trovate diverse porte tcp aperte, ovvero in ascolto su un determinato servizio. In genere è buona norma tenere aperte solo le porte necessarie e tenere connessi i servizi di interesse, configurandoli correttamente, in modo da ridurre il rischio di vulnerabilità e accessi non autorizzati.

In particolare:

21/tcp - FTP (File Transfer Protocol):

L'apertura di questa porta indica che il sistema sta eseguendo un server FTP che viene utilizzato per il trasferimento di file. Quindi la macchina target è al momento configurata per accettare connessioni in ingresso per il trasferimento dei file. Alcuni utenti potrebbero accedere al sistema da remoto e poiché sono richieste credenziali, FTP le trasmette in chiaro, senza crittografia. Quindi le informazioni sensibili saranno vulnerabili ad attacchi di tipo "sniffing", a differenza di connessioni FTP sicure come FTPS e SFTP.

22/tcp - SSH (Secure Shell):

SSH è un protocollo di rete crittografato che consente di accedere in modo sicuro a un sistema remoto. Questa porta aperta indica che il sistema supporta connessioni SSH e permette anche trasferimento dei file con protocollo SFTP. È importante configurare correttamente il server SSH per garantire un accesso sicuro. Questo include la gestione delle chiavi SSH, la limitazione degli indirizzi IP autorizzati e l'implementazione di misure di sicurezza come la verifica in due passaggi.

23/tcp - Telnet:

Telnet è un protocollo di rete utilizzato per fornire un accesso bidirezionale a un sistema remoto. Tuttavia, Telnet non è sicuro perché i dati sono inviati in forma non crittografata. Si tratta di un protocollo di rete che consente l'accesso remoto a un sistema, ma a differenza di SSH, Telnet trasmette le informazioni, inclusi nomi utente e password, in forma non crittografata. Ciò rende vulnerabile il traffico a potenziali attacchi di tipo "sniffing", in cui le informazioni possono essere intercettate durante la trasmissione. L'apertura della porta 23 può essere utilizzata per consentire agli amministratori di sistema di accedere e configurare il sistema da remoto. Tuttavia, a causa della mancanza di crittografia, l'uso di Telnet è generalmente sconsigliato in ambienti in cui è richiesta una sicurezza elevata. L'uso di Telnet presenta rischi di sicurezza significativi a causa della trasmissione non crittografata delle credenziali. Gli attaccanti potrebbero intercettare e raccogliere le informazioni sensibili durante il processo di autenticazione.

25/tcp - SMTP (Simple Mail Transfer Protocol):

Utilizzato per la trasmissione di email. Una porta aperta su SMTP indica che il sistema sta eseguendo un server SMTP. Un server con la porta 25 aperta può accettare connessioni in ingresso da altri server di posta elettronica o client di posta per inviare o ricevere messaggi di posta elettronica. Poiché la posta elettronica è un vettore comune per gli attacchi informatici, è importante configurare correttamente il server SMTP per ridurre i rischi di abusi come lo spamming o l'invio di email malevole. Inoltre, la sicurezza del server SMTP stesso è cruciale per impedire accessi non autorizzati e proteggere le informazioni sensibili. Molti server di posta elettronica implementano filtri anti-spam per ridurre la ricezione di messaggi indesiderati. Un server SMTP aperto potrebbe dover gestire filtri e misure di sicurezza per combattere lo spam e altre minacce correlate. Per garantire che le email inviate dal server siano considerate affidabili, è importante configurare correttamente i record DNS, come i record SPF (Sender Policy Framework) e DKIM (DomainKeys Identified Mail), per autenticare l'origine delle email. È importante configurare il server SMTP per evitare il relaying aperto, che potrebbe essere sfruttato dagli attaccanti per inviare email non autorizzate attraverso il server.

53/tcp - Domain Name System (DNS):

Il DNS si occupa della risoluzione dei nomi di dominio in indirizzi IP. Una porta aperta indica che il sistema sta eseguendo un server DNS. La porta 53 è fondamentale per il funzionamento del DNS, che è responsabile della risoluzione dei nomi di dominio in indirizzi IP e viceversa. Un server DNS con la porta 53 aperta accetta richieste di risoluzione dei nomi di dominio da parte di client che cercano di tradurre un nome di dominio in un indirizzo IP. I server DNS sono soggetti a vari rischi di sicurezza, inclusi attacchi di amplificazione DNS, attacchi di avvelenamento della cache DNS e altri tentativi di compromissione. Pertanto, è importante configurare il server DNS in modo sicuro e applicare misure di sicurezza per prevenire attacchi. La porta 53 è a rischio di attacchi DoS e DDoS, specialmente se il server DNS è configurato per gestire un alto volume di richieste. Misure di protezione, come la limitazione delle richieste, possono essere implementate per mitigare questi rischi. L'apertura della porta 53 può essere utilizzata per monitorare il traffico DNS all'interno di una rete. Il monitoraggio del traffico DNS può essere utile per identificare attività anomale o sospette.

80/tcp - HTTP:

Questa è la porta predefinita per le connessioni HTTP, utilizzate per l'accesso a siti web non crittografati. La porta 80 è il porto predefinito per il traffico HTTP, che è utilizzato per la comunicazione web. Se la porta 80 è aperta, il sistema potrebbe essere configurato come un server web che offre contenuti web accessibili attraverso un browser. L'apertura della porta 80 consente agli utenti di accedere ai siti web ospitati su quel server. I visitatori possono richiedere pagine web, file e risorse attraverso il protocollo HTTP.

L'apertura della porta 80 consente di monitorare il traffico web in entrata e in uscita. Il monitoraggio può essere utile per analizzare il comportamento degli utenti, identificare problemi di performance e rilevare attività sospette o tentativi di attacco.

La sicurezza del server web è di primaria importanza. Ciò include la protezione da vulnerabilità, la gestione sicura dei dati dei visitatori, l'utilizzo di connessioni HTTPS per la crittografia dei dati sensibili, e la protezione contro attacchi comuni come injection di SQL o cross-site scripting (XSS). Molte implementazioni sicure richiedono la redirection del traffico HTTP su HTTPS per garantire una connessione cifrata. La configurazione del server web dovrebbe essere gestita per reindirizzare automaticamente le richieste HTTP alla porta 80 verso la porta HTTPS (solitamente la porta 443).

111/tcp - RPCBIND:

RPCBIND è un servizio di mapping delle procedure remote utilizzato nei sistemi UNIX per registrare i servizi che un server RPC rende disponibili. La porta 111 è comunemente utilizzata per la gestione delle chiamate a procedure remote (RPC). Il servizio rpcbind è responsabile di mappare le chiamate di procedura remota ai numeri di porta associati sui server. L'apertura della porta 111 può indicare che il sistema supporta servizi distribuiti basati su RPC. Questi servizi possono includere la condivisione di file, la gestione di servizi di stampa e altri servizi distribuiti su una rete. Aprire la porta 111 espone il sistema a potenziali rischi di sicurezza, in quanto può essere sfruttata dagli attaccanti per scoprire i servizi RPC disponibili e tentare di sfruttare vulnerabilità associate a tali servizi. Per mitigare i rischi di sicurezza, è importante configurare RPCBIND in modo sicuro, limitando l'accesso non autorizzato, implementando protezioni contro attacchi di tipo "portmap" e mantenendo aggiornati i servizi RPC per correggere eventuali vulnerabilità.

139/tcp - NetBIOS Session Service:

Utilizzato per la comunicazione di sessione NetBIOS su reti Microsoft. Questo può indicare la presenza di servizi di condivisione di file o di stampanti. Se la porta 139 è aperta, potrebbe indicare la possibilità di accedere alle risorse di rete di un sistema remoto, come condivisioni di file o stampanti, attraverso il protocollo SMB. La condivisione di risorse tramite NetBIOS può comportare rischi di sicurezza, poiché NetBIOS non crittografa le credenziali durante l'autenticazione. Ciò può rendere vulnerabili le informazioni sensibili a possibili attacchi di tipo "sniffing". È importante configurare adeguatamente il firewall per limitare l'accesso non autorizzato attraverso la porta 139 e per proteggere le risorse di rete da potenziali minacce.

445/tcp - Microsoft-DS:

Questa porta è associata ai servizi Microsoft Directory Services (MS-DS), comunemente utilizzata per la condivisione di file e stampanti su reti Windows. La porta 445 è comunemente utilizzata per il protocollo SMB, che consente la condivisione di file e risorse di rete su sistemi operativi Windows. L'apertura di questa porta indica la possibilità di accedere alle risorse di rete di un sistema, come condivisioni di file, stampanti e altri servizi. L'apertura della porta 445 può indicare la possibilità di accedere in remoto alle risorse di un sistema Windows attraverso il protocollo SMB. Gli utenti possono accedere a cartelle condivise, stampanti e altri servizi di rete utilizzando il protocollo SMB su questa porta. A differenza di NetBIOS su porta 139, che è noto per la trasmissione non crittografata di credenziali durante l'autenticazione, il protocollo SMB su porta 445 supporta la crittografia delle comunicazioni. Ciò rende le interazioni più sicure rispetto a implementazioni più vecchie di SMB. La porta 445 è spesso coinvolta nelle operazioni di backup e ripristino su reti Windows. Gli strumenti di backup possono utilizzare SMB per accedere e archiviare dati su dispositivi di rete.

Se non configurato correttamente, l'accesso attraverso la porta 445 può comportare rischi di sicurezza. Attacchi come WannaCry hanno sfruttato vulnerabilità in SMB per diffondere malware su reti Windows. Configurare un firewall per limitare l'accesso non autorizzato attraverso la porta 445 è essenziale per proteggere le risorse di rete da potenziali minacce. Questa è una pratica consigliata per migliorare la sicurezza del sistema.

La combinazione delle porte 139 e 445 è particolarmente rilevante nel contesto della sicurezza informatica, poiché queste porte possono essere sfruttate da attacchi noti, inclusi quelli che mirano a vulnerabilità di SMB. Nel passato, ci sono stati exploit noti come "EternalBlue" che hanno sfruttato vulnerabilità in SMB per diffondere malware, inclusi attacchi ransomware come WannaCry.

512/tcp exec

Avere la porta 512 aperta indica che il sistema sta ascoltando per connessioni in ingresso su quella porta. La porta 512 è tradizionalmente associata al servizio "exec" nel file **/etc/services** su sistemi UNIX-like. Questa porta è utilizzata per l'esecuzione remota di comandi su un sistema attraverso il protocollo "exec". La porta

512 può essere utilizzata per eseguire comandi remotamente su un sistema. Tuttavia, è importante notare che il protocollo "exec" può comportare rischi di sicurezza se non configurato correttamente, poiché permette l'esecuzione remota di comandi. Dovrebbe essere configurato attentamente per limitare l'accesso e prevenire l'esecuzione di comandi non autorizzati. Inoltre, l'uso di protocolli di connessione sicuri e autenticazione robusta può contribuire a ridurre i rischi.

513/tcp login

L'apertura della porta 513 è tradizionalmente associata al servizio "login" nel file **/etc/services** su sistemi UNIX-like. Questa porta era originariamente utilizzata per il servizio "rlogin", che consentiva l'accesso remoto a un sistema UNIX tramite il protocollo di login remoto. La porta 513 è stata storicamente utilizzata per il servizio di login remoto, che consente agli utenti di accedere a un sistema UNIX da remoto. Questo implicava un processo di autenticazione per verificare l'identità dell'utente. Il servizio di login remoto tramite la porta 513 comporta rischi di sicurezza, in quanto le informazioni di accesso (nome utente e password) vengono trasmesse in chiaro, senza crittografia. Questo rende il servizio vulnerabile agli attacchi di tipo "sniffing", in cui le credenziali possono essere intercettate durante la trasmissione. Oggi, l'uso di servizi come "rlogin" è considerato obsoleto e non sicuro a causa delle vulnerabilità di sicurezza associate alla trasmissione non crittografata delle credenziali. In ambienti moderni, si preferisce l'uso di protocolli più sicuri come SSH (Secure Shell) per l'accesso remoto. È importante configurare attentamente il servizio di login remoto per limitare l'accesso non autorizzato, proteggere le credenziali degli utenti e implementare misure di sicurezza adeguate. Configurare un firewall per limitare l'accesso non autorizzato attraverso la porta 513 è una pratica consigliata per migliorare la sicurezza del sistema.

514/tcp shell


Su questa porta è attivo un servizio di shell ovvero un servizio che consente agli utenti di eseguire comandi su un sistema remoto. La configurazione di una porta per un servizio di shell potrebbe implicare l'abilitazione dell'accesso remoto al sistema, con la possibilità di eseguire comandi da un'origine esterna.

Nella scansione TCP di tipo SYN, si ottengono gli stesis risultati e in aggiunta l'informazione sul MAC ADDRESS della macchina target: **MACAddress: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC).**

SCANSIONE AVANZATA

Per quanto riguarda la scansione avanzata, si ottengono moltissime informazioni, come la versione del sistema operativo, le chiavi crittografiche usate nel protocollo ssh, l'accesso in modalità anonima nel servizio ftp, i cifrari utilizzati, il tipo di server http etc ... Evidenzio in rosso alcune di esempio:

```
nmap-A 192.168.50.101-p 0-1023
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 10:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.00018s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-syst:
|  STAT:
| FTP server status:
|  Connected to 192.168.50.103
|  Logged in as ftp
|  TYPE: ASCII
|  No session bandwidth limit
|  Session timeout in seconds is 300
|  Control connection is plain text
|  Data connections will be plain text
|  vsFTPD 2.3.4- secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

```
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open  telnet    Linux telnetd
25/tcp open  smtp      Postfix smtpd
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
53/tcp open  domain    ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind  2 (RPC #100000)
| rpcinfo:
| program version  port/proto service
| 100003 2,3,4    2049/tcp  nfs
| 100003 2,3,4    2049/udp  nfs
| 100005 1,2,3    35129/udp mountd
| 100005 1,2,3    39561/tcp mountd
| 100021 1,3,4    38977/udp nlockmgr
| 100021 1,3,4    57485/tcp nlockmgr
| 100024 1        37068/udp status
|_ 100024 1        50391/tcp status
139/tcp open  netbios-ssn Samba smbd 3.X- 4.X (workgroup: WORKGROUP)
445/tcp open   Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec      netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell     Netkit rshd
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-12-21T11:04:26-05:00
|_ clock-skew: mean: 3h23m25s, deviation: 3h32m25s, median: 53m12s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 112.87 seconds

Scansione UDP

A scopo di studio ho eseguito anche una scansione udp con il comando:

sudo nmap -sU 192.168.50.101 -p 0-1023

```
(kali㉿kali)-[~]  
$ sudo nmap -sU 192.168.50.101 -p 0-1023  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 11:16 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.00054s latency).  
Not shown: 1018 closed udp ports (port-unreach)  
PORT      STATE      SERVICE  
53/udp    open       domain  
69/udp    open|filtered tftp  
111/udp   open       rpcbind  
137/udp   open       netbios-ns  
138/udp   open|filtered netbios-dgm  
854/udp   open|filtered unknown  
MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1114.73 seconds
```

Alcune delle porte analizzate sono risultate “filtered” ovvero non è stata ricevuta alcuna risposta per cui non si può concludere che esse siano aperte e nemmeno che siano chiuse.