

NETCAT E NMAP SCAN

- Netcat

Utilizziamo Netcat per aprire un listener per connessioni in entrata nella console di destra, Connettiamo invece la console di sinistra all'indirizzo della nostra macchina nella porta assegnata, creando una shell per poter eseguire comandi dal terminale.

```
kali@kali:~$ nc -l -p 9001
ls
sh: 2: pws: not found

kali@kali:~$ nc -l -p 9001
ls
Desktop
Documents
Downloads
Gameshell-save.sh
Gameshell.sh
Music
Pictures
Public
Responder
shell.php
Templates
Videos
pws
pwd
/home/kali
```

Ora utilizziamo dei comandi dalla shell che siamo riusciti a creare, usiamo il comando “whoami” per sapere il nome utente corrente, successivamente usiamo il comando “uname -a” per avere informazioni sul sistema nel quale abbiamo la shell ed infine usiamo il comando “ps -aux” per vedere tutti i processi in esecuzione sulla macchina alla quale siamo connessi.

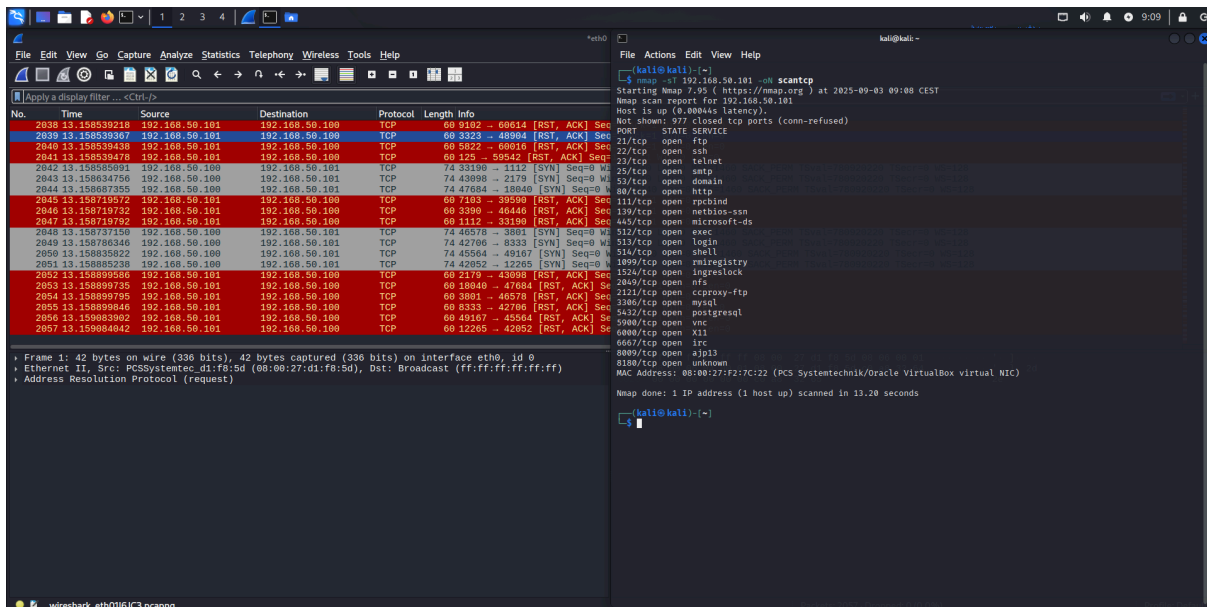
```
kali@kali:~$ nc -l -p 9001
whoami
kali
uname -a
Linux kali 6.12.38-kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-06-12) x86_64 GNU/Linux
ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.2  0.2 23688 14360 ?        Ss   08:40   0:00 /sbin/init splash
root           2  0.0  0.0   0     0 ?        S    08:40   0:00 [kthreadd]
root           3  0.0  0.0   0     0 ?        S    08:40   0:00 [pool_workqueue_release]
root           4  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/R-kvfree_rcu_reclaim]
root           5  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/R-rcu_gp]
root           6  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/R-sync_wq]
root           7  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/R-slab_flushwq]
root           8  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/R-netns]
root          10  0.0  0.0   0     0 ?        I   08:40   0:00 [kworker/0:1-events_power_efficient]
root          11  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/0:0-events_highpri]
root          12  0.2  0.0   0     0 ?        I   08:40   0:01 [kworker/u24:0-events_unbound]
root          13  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/R-mm_percpu_wq]
root          14  0.0  0.0   0     0 ?        I   08:40   0:00 [rcu_tasks_kthread]
root          15  0.0  0.0   0     0 ?        I   08:40   0:00 [rcu_tasks_rude_kthread]
root          16  0.0  0.0   0     0 ?        I   08:40   0:00 [rcu_tasks_trace_kthread]
root          17  0.0  0.0   0     0 ?        S    08:40   0:00 [ksfirqd/0]
root          18  0.0  0.0   0     0 ?        I   08:40   0:00 [rcu_preempt]
root          19  0.0  0.0   0     0 ?        S    08:40   0:00 [rcu_exp_gprp_kthread_worker/0]
root          20  0.0  0.0   0     0 ?        S    08:40   0:00 [rcu_exp_gprp_kthread_worker]
root          21  0.0  0.0   0     0 ?        S    08:40   0:00 [migration/0]
root          22  0.0  0.0   0     0 ?        S    08:40   0:00 [idle_inject/0]
root          23  0.0  0.0   0     0 ?        S    08:40   0:00 [cpuhp/0]
root          24  0.0  0.0   0     0 ?        S    08:40   0:00 [cpuhp/1]
root          25  0.0  0.0   0     0 ?        S    08:40   0:00 [idle_inject/1]
root          26  0.1  0.0   0     0 ?        S    08:40   0:00 [migration/1]
root          27  0.0  0.0   0     0 ?        S    08:40   0:00 [ksfirqd/1]
root          28  0.0  0.0   0     0 ?        I   08:40   0:00 [kworker/1:0-cgroup_destroy]
root          29  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/1:0H-kblockd]
root          30  0.0  0.0   0     0 ?        S    08:40   0:00 [cpuhp/2]
root          31  0.0  0.0   0     0 ?        S    08:40   0:00 [idle_inject/2]
root          32  0.0  0.0   0     0 ?        S    08:40   0:00 [migration/2]
root          33  0.0  0.0   0     0 ?        S    08:40   0:00 [ksfirqd/2]
root          34  0.0  0.0   0     0 ?        I   08:40   0:00 [kworker/2:0-events]
root          35  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/2:0H-events_highpri]
root          36  0.0  0.0   0     0 ?        S    08:40   0:00 [cpuhp/3]
root          37  0.0  0.0   0     0 ?        S    08:40   0:00 [idle_inject/3]
root          38  0.1  0.0   0     0 ?        S    08:40   0:00 [migration/3]
root          39  0.0  0.0   0     0 ?        S    08:40   0:00 [ksfirqd/3]
root          41  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/3:0H-events_highpri]
root          42  0.0  0.0   0     0 ?        S    08:40   0:00 [cpuhp/4]
root          43  0.0  0.0   0     0 ?        S    08:40   0:00 [idle_inject/4]
root          44  0.0  0.0   0     0 ?        S    08:40   0:00 [migration/4]
root          45  0.0  0.0   0     0 ?        S    08:40   0:00 [ksfirqd/4]
root          47  0.0  0.0   0     0 ?        Ic   08:40   0:00 [kworker/4:0H-events_highpri]
```

- Nmap + Facoltativo

Valutiamo di fare una scansione delle porte aperte sulla nostra metasploitable

Fonte	Macchina Target	Tipo di scan	Numero porte attive
192.168.50.100	192.168.50.101	Tcp “-sT”	23 porte attive
192.168.50.100	192.168.50.101	SYN “-sS”	23 porte attive
192.168.50.100	192.168.50.101	“-A”	12 porte attive

Eseguiamo una scansione delle porte TCP catturando con wireshark le richieste fatte dalla nostra macchina attaccante e le risposte date dalla macchina target, possiamo vedere come la macchina attaccante cerchi di creare una connessione 3-way-handshake per scansionare le porte della macchina target.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: ~Ctrl+F

No.	Time	Source	Destination	Protocol	Length	Info
3469	88.919829920	192.168.50.101	192.168.50.100	TCP	60	21 - 59572 [ACK] Seq=1 ACK=1
3470	88.919821080	192.168.50.101	192.168.50.100	TCP	66	21 - 59572 [ACK] Seq=1 ACK=1
3471	88.927854368	192.168.50.101	192.168.50.100	TCP	66	82Response: 220 (vsftpd 2.3.4)
3472	88.927893930	192.168.50.101	192.168.50.100	TCP	66	959572 - 21 [ACK] Seq=1073 A=1
3473	88.930327362	192.168.50.101	192.168.50.100	TCP	74	21 - 59576 [SYN, ACK] Seq=1
3474	88.958922475	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [ACK] Seq=1 ACK=1
3475	88.958960990	192.168.50.101	192.168.50.100	TCP	124	Request: VQ0P003V000000000000
3476	88.960393214	192.168.50.101	192.168.50.100	TCP	66	21 - 59576 [ACK] Seq=1 ACK=1
3477	88.968594147	192.168.50.101	192.168.50.100	TCP	66	82Response: 220 (vsftpd 2.3.4)
3478	88.968902802	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [ACK] Seq=89 ACK=1
3479	88.969061115	192.168.50.101	192.168.50.100	TCP	104	Response: 530 Please login
3480	88.969344612	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [ACK] Seq=89 ACK=1
3481	88.969344782	192.168.50.101	192.168.50.100	TCP	104	Response: 530 Please login
3482	88.969353377	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [ACK] Seq=89 ACK=1
3483	88.969394267	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [ACK] Seq=89 ACK=1
3484	88.970811110	192.168.50.101	192.168.50.100	TCP	104	Response: 530 Please login
3485	88.970813763	192.168.50.101	192.168.50.100	TCP	66	959572 - 21 [ACK] Seq=1073 A=1
3486	88.970374150	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [RST, ACK] Seq=89
3487	88.970394816	192.168.50.101	192.168.50.100	TCP	66	959576 - 21 [RST, ACK] Seq=89
3488	88.979332462	192.168.50.101	192.168.50.100	TCP	66	21 - 59572 [RST, ACK] Seq=89

Frame 3473: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSysteme02:f1:8b:5d, Dst: PCSSysteme02:f2:7c:22 (98:00:27:f2:7c)
 Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
 Transmission Control Protocol, Src Port: 59576, Dst Port: 21, Seq: 0, Len: 0
 Source Port: 59576
 Destination Port: 21
 [Stream index: 1158]
 [Stream Packet Number: 1]
 [Conversation completeness: Complete, WITH_DATA (47)]
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 3926142614
 [Next Sequence Number: 1] (relative sequence number)
 Acknowledgment Number: 0
 Acknowledgment Number (raw): 0
 1010... = Header Length: 48 bytes (16)
 [Length: 0x002 (SYN)]
 Window: 64240
 [Calculated window size: 64240]
 Checksum: 0x66d [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0

wreshark eth0E0F483.pcapng

File Actions Edit View Help

```

kali@kali:~$
kali@kali:~$ nmap -sS 192.168.50.101 -o 19204 -uN --scanmy
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 09:03 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0000000 latency).
Not shown: 1021 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
ftp-anon   Anonymous FTP login allowed (FTP code 230)
ftp:
  STAY:
  FTP server status:
  Logged in as ftp
  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, stable
End of status
22/tcp    open  ssh
Host: 192.168.50.101
224 88:8f:c7:fc:5f:6a:7d:b6:98:24:fa:c4:d5:8c:05d (D5A)
2048 56:56:2a:0f:11:dd:a7:26:b1:61:24:3d:e8:f3 (R3A)
22/tcp    open  telnet
25/tcp    open  smtp
1 smtp-comands: metropolitan.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
21/tcp    open  ftp
bind-version: 9.4.2
80/tcp    open  http
Apache/2.2.8 ((Ubuntu) DAV/2)
[html-render: Metasploitable - Linux
[http-server: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind
2 (RPC #100000)
tcpinfo:
  program version port/proto service
  100000 2 111/tcp  rpcbind
  100000 2 111/udp  rpcbind
  100003 2,3,4 2849/tcp  nfs
  100003 2,3,4 2849/udp  nfs
  100005 1,2,3 4342/tcp  mountd
  100005 1,2,3 5249/udp  mountd
  100021 1,3,4 3443/tcp  nlockmgr
  100021 1,3,4 57945/udp nlockmgr
  3344/tcp  status
  100024 1 56148/tcp  status
139/tcp   open  netbios-ssn Samba smbd 3.0.2-4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.2-4.X (workgroup: WORKGROUP)
512/tcp   open  exec      netkit-rsh rexec
513/tcp   open  login

```