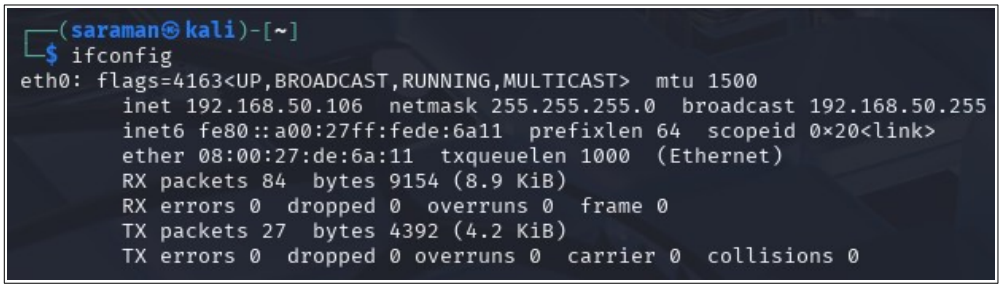
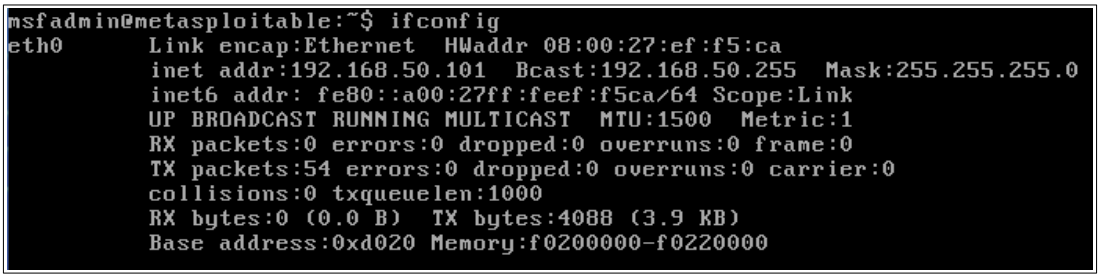
Report esercitazione raccolta informazioni W10D4

In questo esercizio dovremo usare diversi tools per eseguire scansioni da Kali a Metasploitable 2.
Il procedimento ed i risultati degli scan verranno inseriti in una tabella riassuntiva.

Configurazione di Kali:



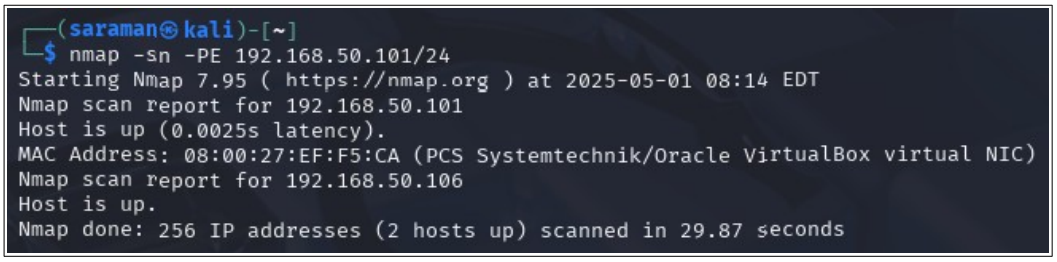
Configurazione di Metasploitable 2:



Assicuriamoci che entrambe le macchine siano su rete interna per permettere la comunicazione e lo svolgimento dei test.

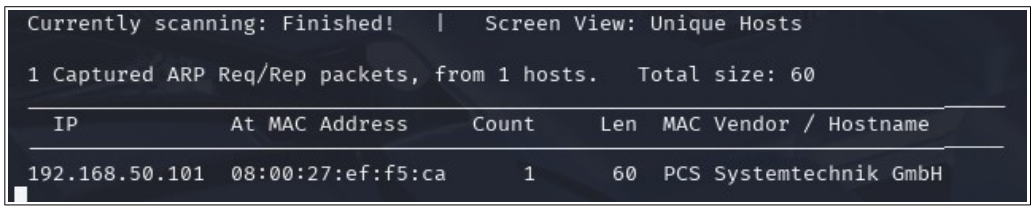
Comando 1:

- Sintassi: nmap -sn -PE <rete target>
- Analisi sintassi: [-sn=ping scan, -PE=icmp echo request]
- Scopo del comando: Questo comando esegue uno scan sulla rete target tramite ping ed echo request per verificare quali host sono attivi. Vista la nostra configurazione troverà sia Kali che Metasploitable 2.
- Output del comando:



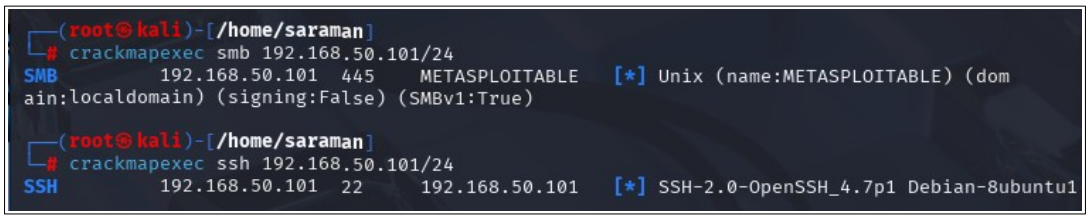
Comando 2:

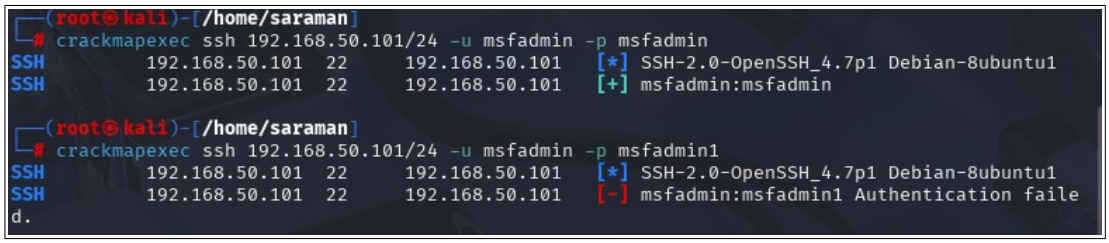
- Sintassi: netdiscover -r <rete target>
- Analisi sintassi: [-r=esegue una scansione attiva ARP, scansiona ogni IP nel range]
- Scopo del comando: Serve per scansionare dispositivi attivi sulla rete utilizzando pacchetti ARP. Non si basa su ICMP e quindi funziona anche se il ping è stato disabilitato.
- Output del comando:



Comando 3:

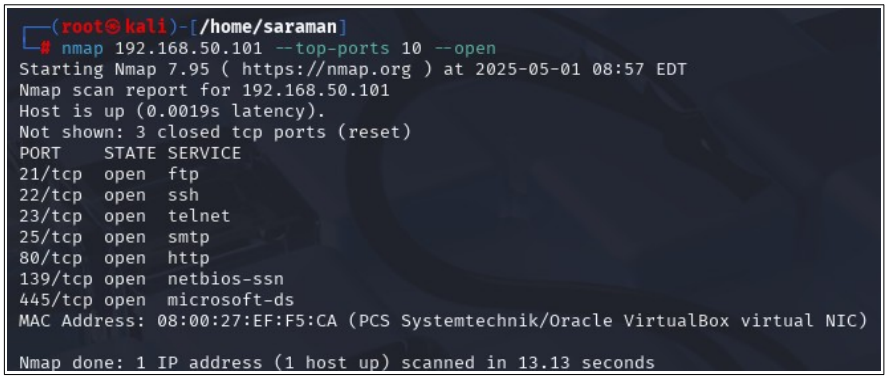
- Sintassi: crackmapexec <modulo> <rete target>
- Analisi sintassi: [ssh=esgue una scansione sulla porta 22, smb= esegue una scansione sulla porta 445]
- Scopo del comando: Esegue una scansione sulla rete target in base al modulo selezionato. Può anche essere usato per testare credenziali sulla porta selezionata.
- Output del comando:





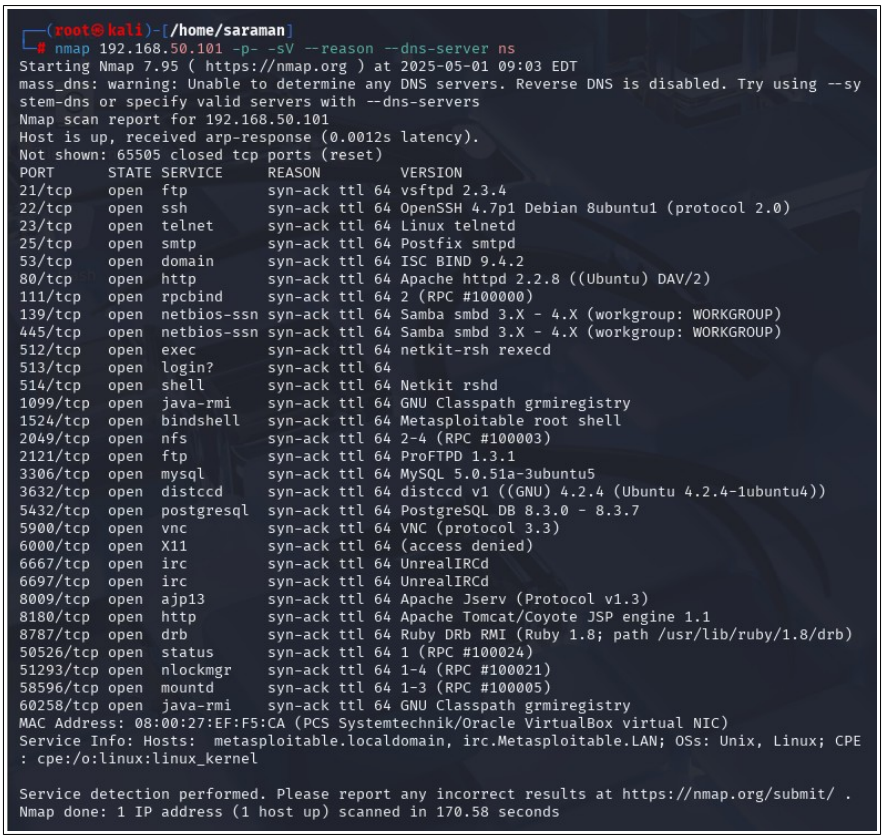
Comando 4:

- Sintassi: nmap <IP target> –top-ports 10 –open
- Scopo del comando: Esegue uno scan sul target per trovare le 10 porte più importanti e determina se sono aperte o meno.
- Output del comando:



Comando 5:

- Sintassi: nmap <IP target> -p- -sV –reason –dns-server ns
- Analisi sintassi: [-p-=scansiona tutte le 65535 porte, -sV=identifica la versione dei servizi sulle porte aperte, --reason=mostra il motivo per cui una porta è aperta/chiusa/filtrata in base al tipo di pacchetto ricevuto, --dns-server<IP dns>=specifica il server DNS da utilizzare per la risoluzione dei nomi]
- Scopo del comando: Esegue una scansione completa delle porte TCP su un host, raccogliendo informazioni sui servizi.
- Output del comando:

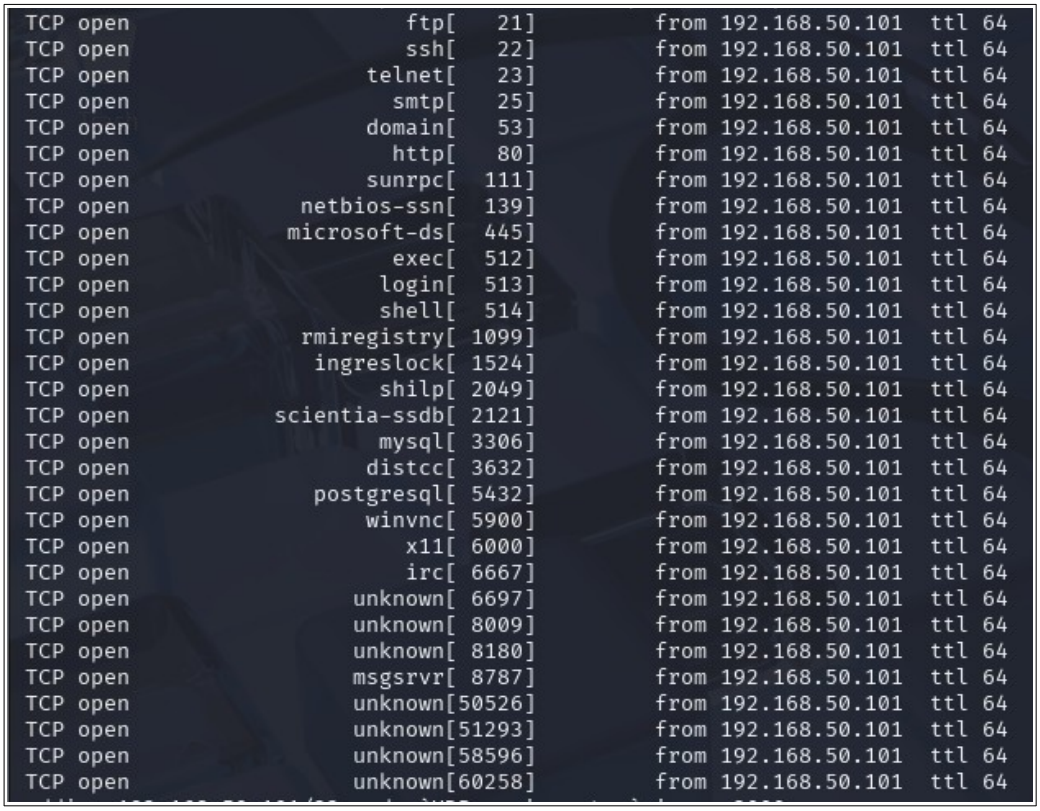


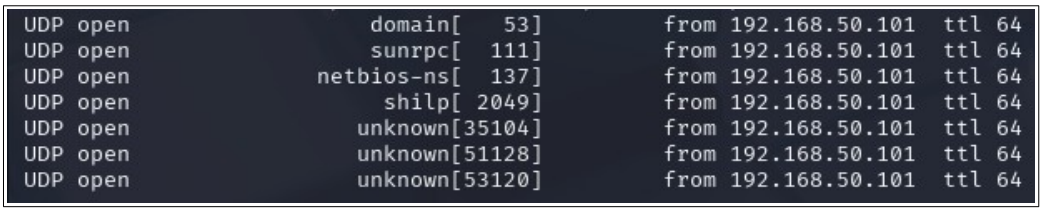
```
┌──(root㉿kali)-[/home/saraman]
└─# nmap 192.168.50.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:03 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
stem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.0012s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
50526/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
51293/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
58596/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
60258/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
MAC Address: 08:00:27:EF:F5:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.58 seconds
```

Comando 6:

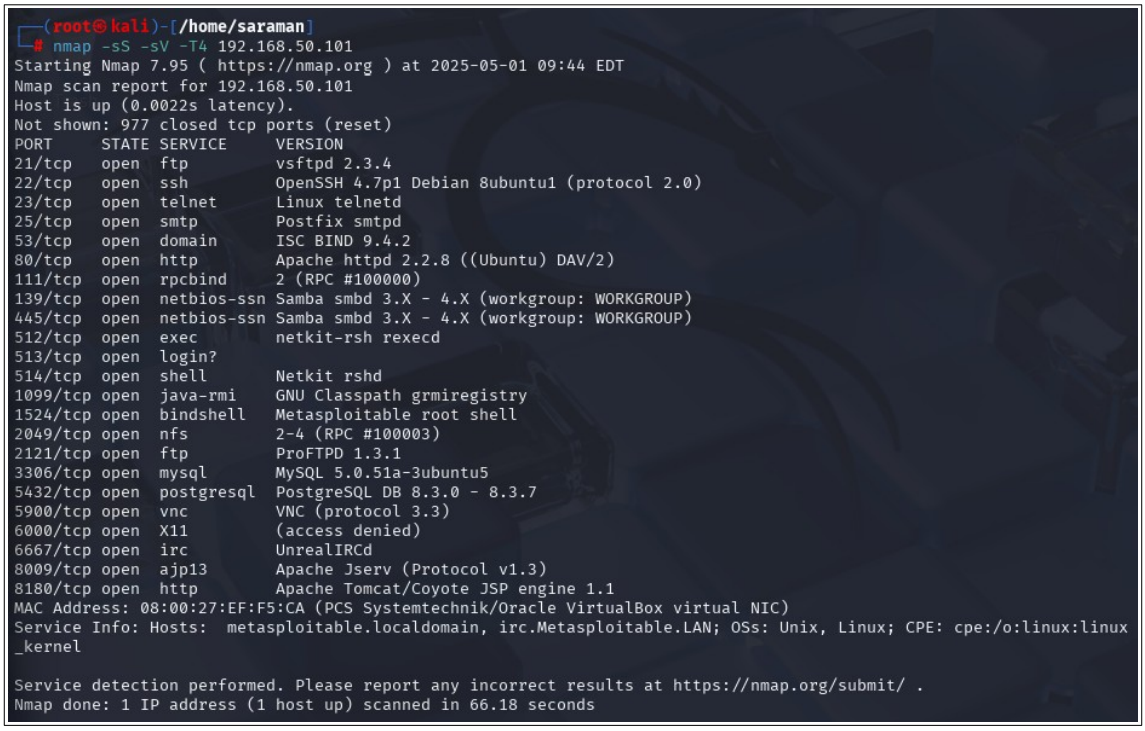
- Sintassi: us -mT -Iv <IP target>:a -r <n. pacchetti> -R <numero massimo di tentativi> && us -mU -Iv <IP target>:a -r <n. pacchetti> -R <numero massimo di tentativi>
- Analisi sintassi: [us=unicorn scan, -mT=modalità TCP, -Iv=modalità interactive e verbose, :a=all ports, &&=concatenazione con operatore AND, -mU=modalità UDP]
- Scopo del comando: Esegue una scansione completa su tutte le porte TCP e UDP.
- Output del comando:





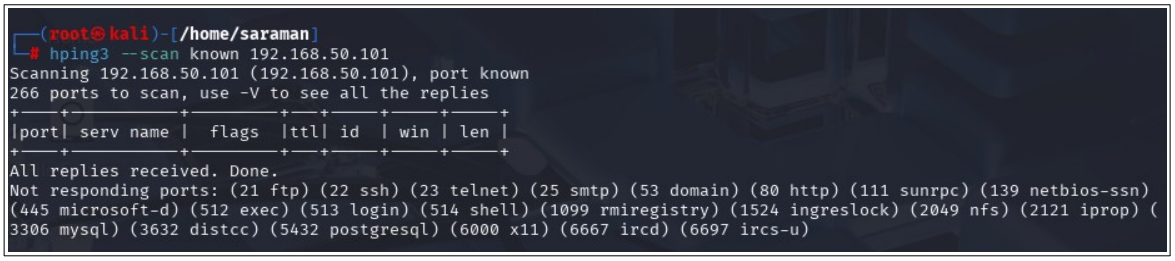
Comando 7:

- Sintassi: nmap -sS -sV -T4 <IP target>
- Analisi sintassi: [-sS=SYN scan, -sV=scannerizza la versione dei servizi sulle porte, -T4=imposta il livello di aggressività della scansione]
- Scopo del comando: Eseguire uno scan SYN sulle porte TCP identificando le porte aperte e quali servizi sono in ascolto.
- Output del comando:



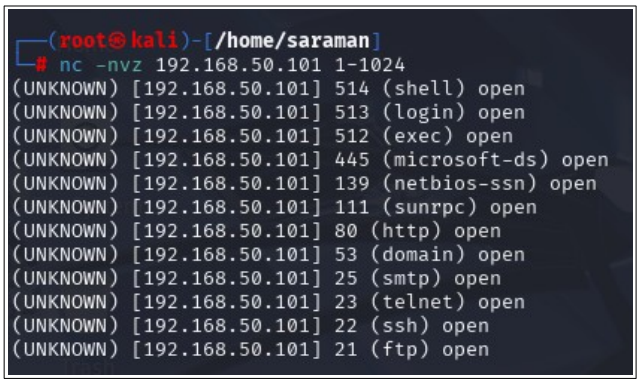
Comando 8:

- Sintassi: hping3 --scan known <IP target>
- Analisi sintassi: [-- scan known=scansiona le porte TCP note]
- Scopo del comando: Esegue una scansione sulle porte TCP verificando se riceve una risposta o meno.
- Output del comando:



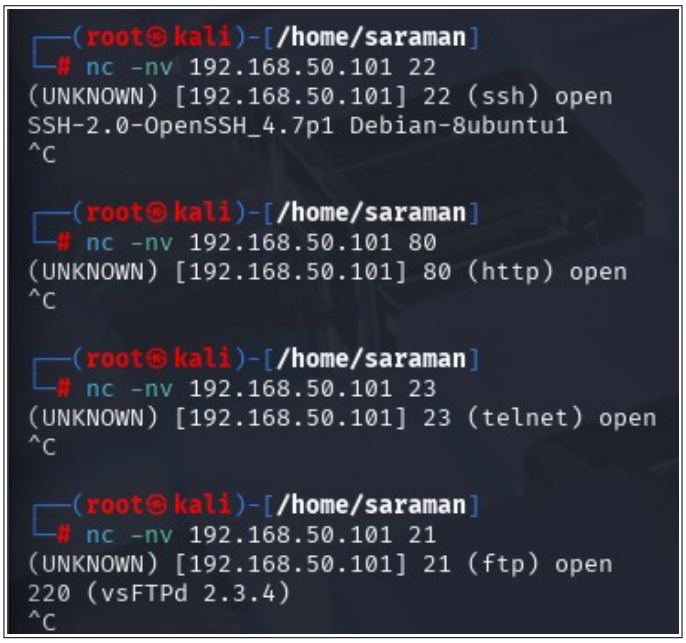
Comando 9:

- Sintassi: nc -nvz <IP target> <range di porte>
- Analisi sintassi: [nc=netcat, -n=l'IP non deve essere risolto tramite DNS, v=verbose, z=non invia né riceve dati, testa solo se la porta è aperta o meno]
- Scopo del comando: Esegue una scansione sulle porte nel range specificato.
- Output del comando:



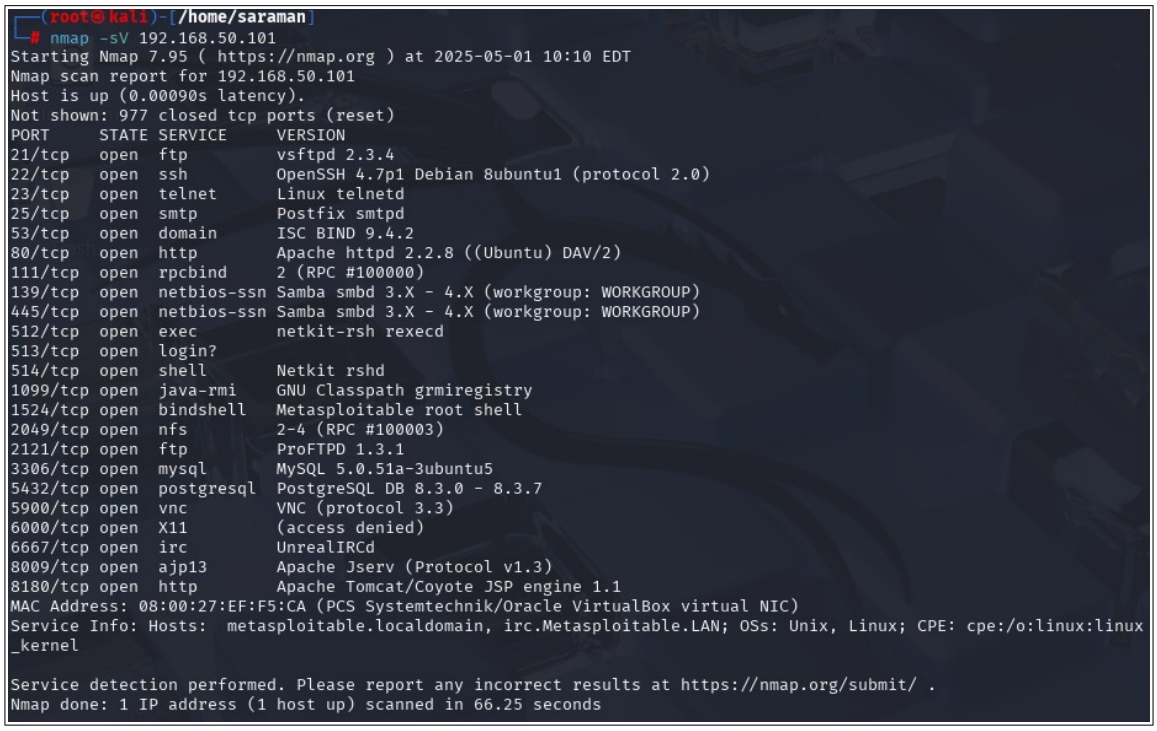
Comando 10:

- Sintassi: nc -nv <IP target> <porta>
- Analisi sintassi: [nc=netcat, -n=l'IP non deve essere risolto tramite DNS, v=verbose]
- Scopo del comando: Si mette in ascolto sulla porta selezionata e (nel caso del servizio SSH), identifica la versione di SSH.
- Output del comando:



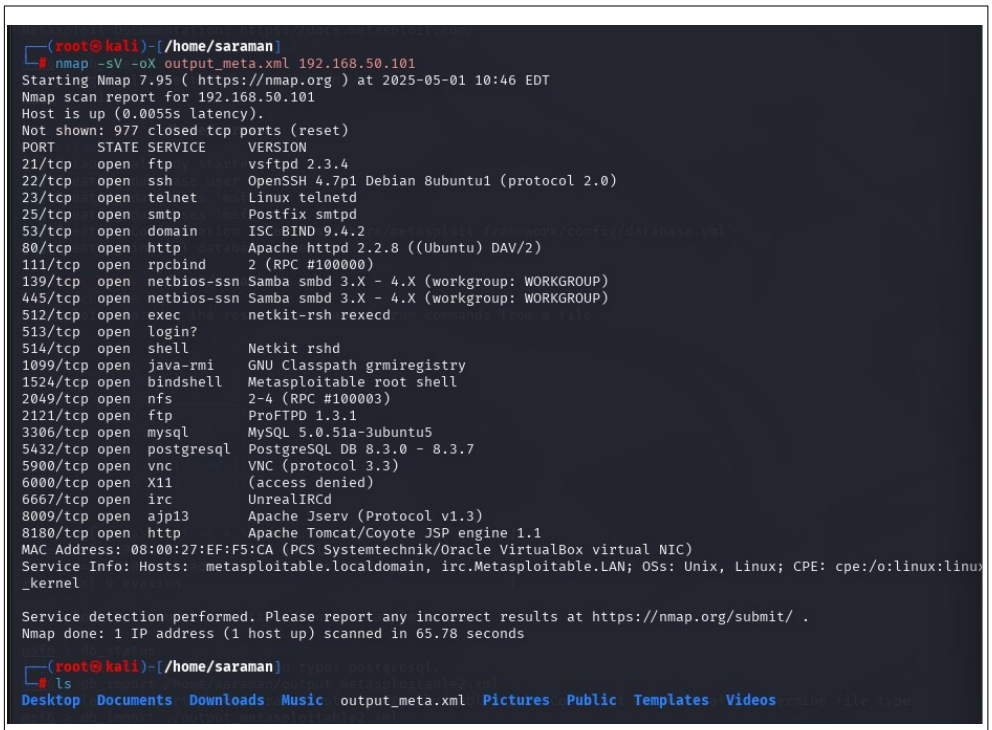
Comando 11:

- Sintassi: nmap -sV <IP target>
- Analisi sintassi: [-sV=rileva le versioni dei servizi]
- Scopo del comando: Scannerizza tutte le porte TCP e specifica la versione del servizio attiva su quella porta.
- Output del comando:



Comando 12:

- Sintassi: db_import <file.xml>
- Analisi sintassi:
- Scopo del comando: Importare un file.xml contenente tutti i dati ricavati da una scansione nmap, sulla console msf.
- Output del comando:

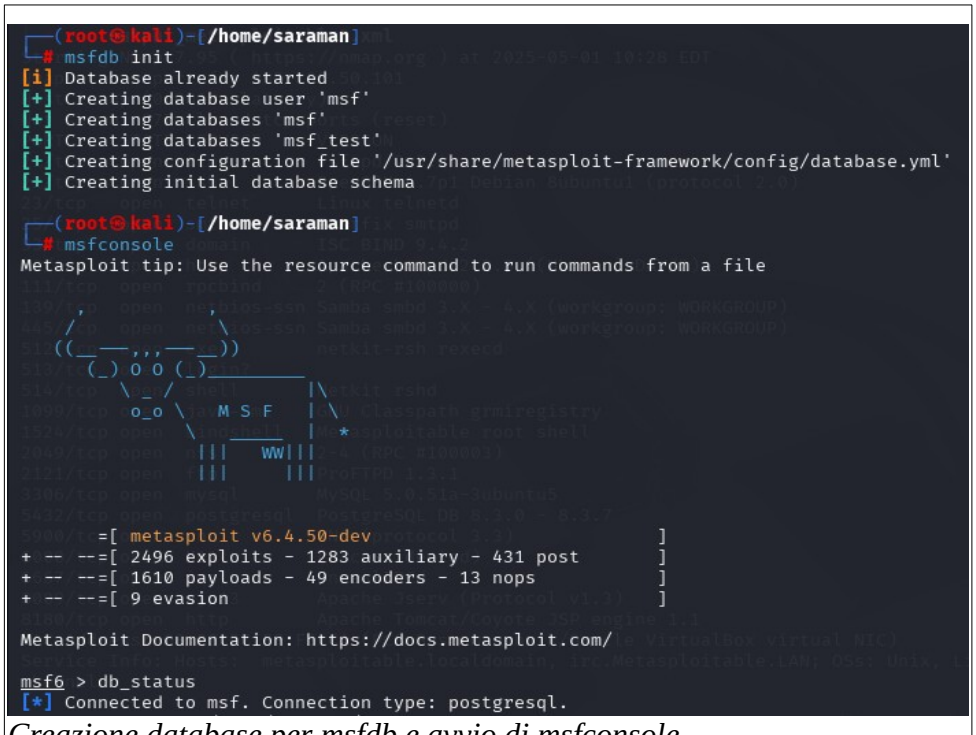


```
┌──(root㉿kali)-[/home/saraman]
└─# nmap -sV -oX output_meta.xml 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 10:46 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0055s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:EF:F5:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.78 seconds

┌──(root㉿kali)-[/home/saraman]
└─# ls
Desktop  Documents  Downloads  Music  output_meta.xml  Pictures  Public  Templates  Videos
```

Creazione file.xml contenente l'output dello scan nmap



```
┌──(root㉿kali)-[/home/saraman]
└─# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(root㉿kali)-[/home/saraman]
└─# msfconsole
Metasploit tip: Use the resource command to run commands from a file

       ,           ,
      /             \
     ((__---,,,---__))
        (_) O O (_)_________
           \ _ /            |\
            o_o \   M S F   | \
                 \  _____   |  *
                  ||| WW|||
                  |||     |||

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
```

Creazione database per msfdb e avvio di msfconsole

```
msf6 > db_import /home/saraman/output_meta.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 192.168.50.101
[*] Successfully imported /home/saraman/output_meta.xml
msf6 > hosts

Hosts
=====

address         mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---                ----  -------  ---------  -----  -------  ----  --------
192.168.50.101  08:00:27:ef:f5:ca        Linux                     server
```

Comando 13:

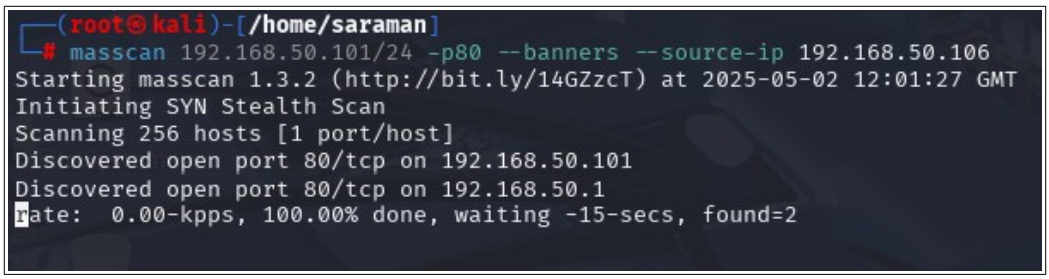
- Sintassi: nmap -f --mtu=<grandezza pacchetti> <IP target>
- Analisi sintassi: [-f=frammentazione pacchetti, --mtu=specifica la dimensione massima dei pacchetti inviati]
- Scopo del comando: Scansiona le porte TCP frammentando i pacchetti inviati per evadere i filtri dei firewall.
- Output del comando:

```
┌──(root㉿kali)-[/home/saraman]
└─# nmap -f --mtu=512 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 11:04 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0035s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:EF:F5:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

Comando 14:

- Sintassi: masscan <rete target> -p<porta> --banners --source-ip <IP target>
- Analisi sintassi: [-p=specificare porta su cui iniziare lo scan, --banners=tenta di leggere i banner (header http ad esempio), --source-ip=IP sorgente dei pacchetti inviati]
- Scopo del comando: Esegue una scansione sulla porta specificata, determinando se la porta è aperta o meno. Per permettere il funzionamento del comando ho usato PfSense come gateway (192.168.50.1).
- Output del comando:



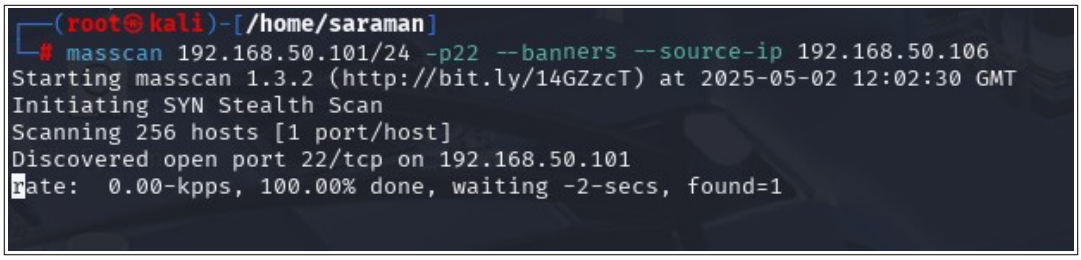


Tabella riassuntiva

Metasploitable 2			
Target (IP/rete/porta)	Comando	Scopo del comando	Risultati
192.168.50.101/24	nmap -sn -PE 192.168.50.101/24	Scan sulla rete per trovare host attivi	2 host attivi
192.168.50.101/24	netdiscover -r 192.168.50.101/24	Scansione ARP sulla rete per trovare dispositivi attivi	1 host attivo
192.168.50.101/24 modulo: SMB, SSH	crackmapexec <SMB,SSH> 192.168.50.101	Scansione tramite modulo sulla rete	Trovate versioni del protocollo sulle relative porte e test credenziali
192.168.50.101 porte: top 10	Nmap 192.168.50.101 –top-ports 10 –open	Scan sulle 10 porte più importanti	7 porte aperte 3 porte chiuse
192.168.50.101 porte: tutte	nmap 192.168.50.101 -p- -sV –reason –dns-server ns	Scansione su tutte le porte TCP ed i servizi relativi	30 porte aperte 65505 porte chiuse
192.168.50.101	us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3	Scansione completa porte TCP e UDP e i relativi servizi	30 porte TCP aperte 7 porte UDP aperte
192.168.50.101	nmap -sS -sV -T4 192.168.50.101	Scan SYN su porte TCP e i relativi servizi	23 porte aperte 977 porte chiuse
192.168.50.101	hping3 --scan known 192.168.50.101	Scansione porte TCP e verifica della risposta	22 porte aperte senza riposta ricevuta
192.168.50.101 range porte: 1-1024	nc -nvz 192.168.50.101 10-1024	Scansione delle porte nel range	12 porte aperte
192.168.50.101 porte: 22,80,23,21	nc -nv 192.168.50.101 <22,80,23,21>	Server in ascolto sulla porta selezionata	Porte aperte e trovata versione protocollo per SSH e FTP
192.168.50.101	nmap -sV 192.168.50.101	Scan su tutte le porte TCP e relativa versione dei servizi	23 porte aperte 977 porte chiuse
192.168.50.101	db_import output_meta.xml	Importazione file .xml contenente i dati di una scansione	File .xml importato su msfconsole, pronto per essere utilizzato
192.168.50.101	nmap -f --mtu=512 192.168.50.101	Scansione porte TCP con frammentazione pacchetti	23 porte aperte 977 chiuse
192.168.50.101/24 porte:80,22	Masscan 192.168.50.101 -p<80,22> --banners --source-ip 192168.50.106	Scansione sulla porta specificata	Porta 80 aperta su due host Porta 22 aperta su un host