

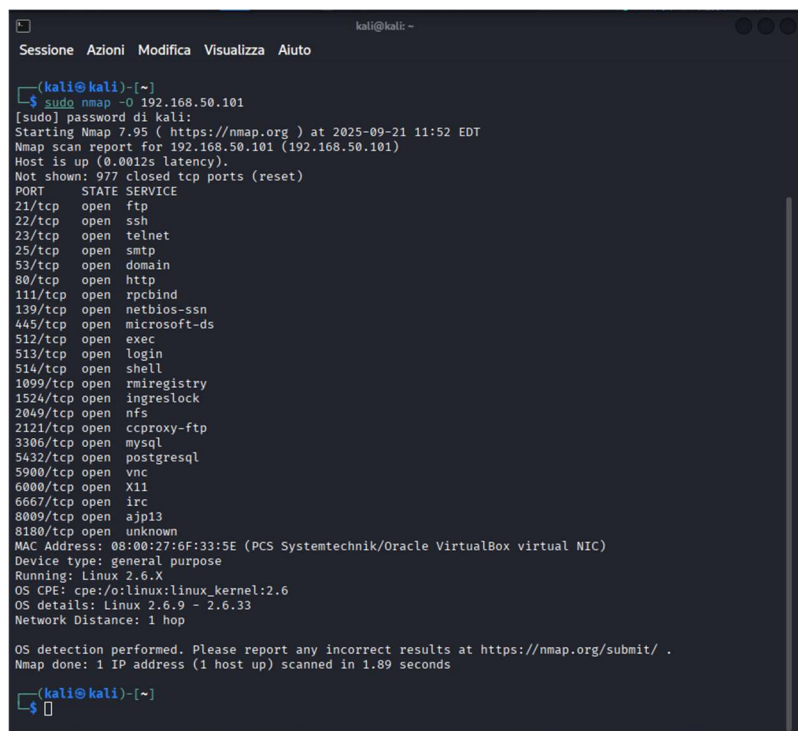
## CONSEGNA W11D2

**Traccia:** Tecniche di scansione con Nmap. Scansione dei servizi: si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable: OS fingerprint, Syn Scan, TCP connect, Version detection. A valle delle scansioni, è prevista la produzione di un report contenente le seguenti info (dove disponibili): IP, Sistema Operativo, Porte Aperte, Servizi in ascolto con versione e descrizione dei servizi.

Di seguito, tramite figure mostriamo 4 comandi volti a fare una scansione di un dispositivo al fine di stabilirne il Sistema Operativo, le porte aperte, i servizi attivi e le versioni presenti nel target. Secondo la scansione sappiamo che il nostro target gira con un sistema linux, più dettagliatamente Linux Kernel 2.6.32 – 3.10. Notiamo che ci sono numerose porte aperte su servizio TCP e nell'ultima immagine tramite nmap -sV riusciamo a vedere anche tutte le versioni dei vari servizi.

## DIFFERENZE TRA SYN SCAN E TCP CONNECT SCAN

Sono entrambe tecniche usate da Nmap per rilevare porte aperte su un target. La prima è definita una connessione stealth, visto che è più difficile da rilevare e provoca meno rumore in quanto fondamentalmente invia un pacchetto SYN alla porta ma non completa la connessione three-way handshake in quanto aspetta solo la prima risposta e in base a quest'ultima si stabilisce se la porta è aperta (SYN-ACK) o chiusa (RST). La seconda invece è una connessione completa per poi essere chiusa risultando quindi più lenta e allo stesso tempo più semplice da rilevare.



```
kali@kali: ~  
Sessione Azioni Modifica Visualizza Aiuto  
  
(kali@kali)~$ sudo nmap -O 192.168.50.101  
[sudo] password di kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 11:52 EDT  
Nmap scan report for 192.168.50.101 (192.168.50.101)  
Host is up (0.0012s 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: 08:00:27:6F:33:5E (PCS Systemtechnik/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  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds  
  
(kali@kali)~$
```

```

(kali@kali)-[~]
$ nmap -sS 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 11:55 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00041s 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: 08:00:27:6F:33:5E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

```

```

(kali@kali)-[~]
$ nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 11:56 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0024s latency).
Not shown: 977 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
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: 08:00:27:6F:33:5E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

```

```

(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 11:57 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00044s 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: 08:00:27:6F:33:5E (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 46.92 seconds

```

## REPORT- SCANSIONE DEI SERVIZI CON NMAP TARGET 192.168.50.101

D'Amora Francesco

### Indice

#### 1) informazioni generali

*Dettagli sulla macchina target*

#### 2) tipologie di scansioni usate

*Descrizione dei comandi usati e degli obiettivi*

#### 3) Risultati della scansione

*Sistema operativo, porte aperte, servizi e versioni del target*

#### 4) Considerazioni di sicurezza

*Spiegazione dei rischi potenziali rilevati ed eventuali soluzioni*

### 1) Info generali

- Target IP: 192.168.50.101
- Sistema Operativo rilevato: Linux Kernel 2.6.32 – 3.10
- MAC Address rilevato: 08:00:27:6F:33:5E
- Stato Host: Attivo

### 2) Scansioni usate

TIPO DI SCANSIONE USATA	COMANDO USATO	OBIETTIVO
OS Fingerprint	nmap -O	Rilevamento del Sistema Operativo
SYN Scan	nmap -sS	Rilevamento porte aperte in modalità stealth
TCP Connect Scan	nmap -sT	Rilevamento porte aperte connessione completa
Version Detection	nmap -sV	Rilevamento dei servizi e delle versioni

### 3) Servizi rilevati

Porta	Servizio	Versione
21	ftp	Vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1 Debian
23	telnet	Linux telnetd
25	smtp	Postfix smtp
53	domain	ISC BIND 9.4.2
80	http	Apache httpd 2.2.8
111	rpcbind	2 (RPC #10000)
139	netbios-ssn	Samba smbd 3.X - 4.X
445	netbios-ssn	Samba smbd 3.X - 4.X
512	exec	Netkit-rsh rexecd
513	login?	
514	shell	Netkit rshd
1099	java-rmi	GNU Classpath grimiregistry
1524	bindshell	Metasploitable root shell
2049	nfs	2-4 (RCP #100003)
2121	ftp	ProFTPD 1.3.1
3306	mysql	MySQL 5.0.51a-3ubuntu5

5432	postgresql	PostgreSQL DB 8.3.0 – 8.3.7
5900	vnc	VNC (protocol 3.3)
6000	X11	(access denied)
6667	irc	UnrealIRCd
8009	ajp13	Apache Jserv (Protocol v1.3)
8180	http	Apache Tomcat/Coyote JSP engine 1.1

#### 4) Considerazioni di sicurezza

Durante la scansione sono stati rilevati molteplici servizi attivi sulla macchina target, molti sono vecchi e non protetti e potrebbero essere sfruttati da un attaccante per entrate nel sistema. Esempio di potenziale rischio:

- Telnet (Porta 23) e FTP (Porta 21): Sono dei protocolli non cifrati.
- Servizi Web (Porte 80): È esposto pubblicamente.
- Database (Porta 3306:mysql e Porta 5432:postgresql): Assicurarsi che l'accesso sia limitato e protetto da credenziali robuste.

Alla luce della scansione si evince un dispositivo dove ci sono molti servizi attivi non aggiornati e/o non protetti adeguatamente come ad esempio la porta 80 che è esposta usando un protocollo http (versione obsoleta con numerose vulnerabilità note) che dovrebbe essere invece cambiato in https che consiste in protocollo cifrato (dunque più sicuro). Stesso discorso vale per la porta 21 dove il protocollo FTP dovrebbe essere sostituito da SFTP che garantisce una cifratura dei dati. Discorso diverso invece ad esempio è per le porte 3306 e 5432 che in quanto porte riservate alla gestione del database bisogna configurarle adeguatamente e impostare password robuste e da cambiare periodicamente per prevenire eventuali attacchi, oltre ad aggiornarle periodicamente visto che nelle versioni adottate presentano vulnerabilità note.