

REPORT DI SICUREZZA - SCANSIONI NMAP

Data: 29 Aprile 2025

Autore: Francesco Fontana

1. Introduzione

Questo documento riporta i risultati delle attività di ricognizione e analisi del network eseguite sui seguenti target:

- **Target A (Metaspoitable 2):** 192.168.20.10
- **Target B (Windows 10):** 192.168.64.5

L'obiettivo principale è stato identificare:

- Fingerprinting del sistema operativo (OS)
- Stato delle porte tramite Syn Scan e TCP Connect Scan, confrontando i risultati
- Rilevamento versioni dei servizi in ascolto

Strumento utilizzato: **Nmap** su piattaforma **Kali Linux**.

2. Metodologia

Le scansioni sono state condotte con privilegi di root (utilizzo di sudo), garantendo completezza e accuratezza. Tutte le attività sono state svolte in modalità non intrusiva (rispetto alle policy interne) limitando il rischio di interruzioni di servizio.

2.1 Configurazione Ambiente

- Sistema operativo: **Kali Linux Release 2023**
- Versione Nmap: **7.94**
- Livello di velocità scanning: opzione **T4** per equilibrio, rapidità e accuratezza

2.2 Comandi Eseguiti

Per il **Target A (192.168.20.10)**:

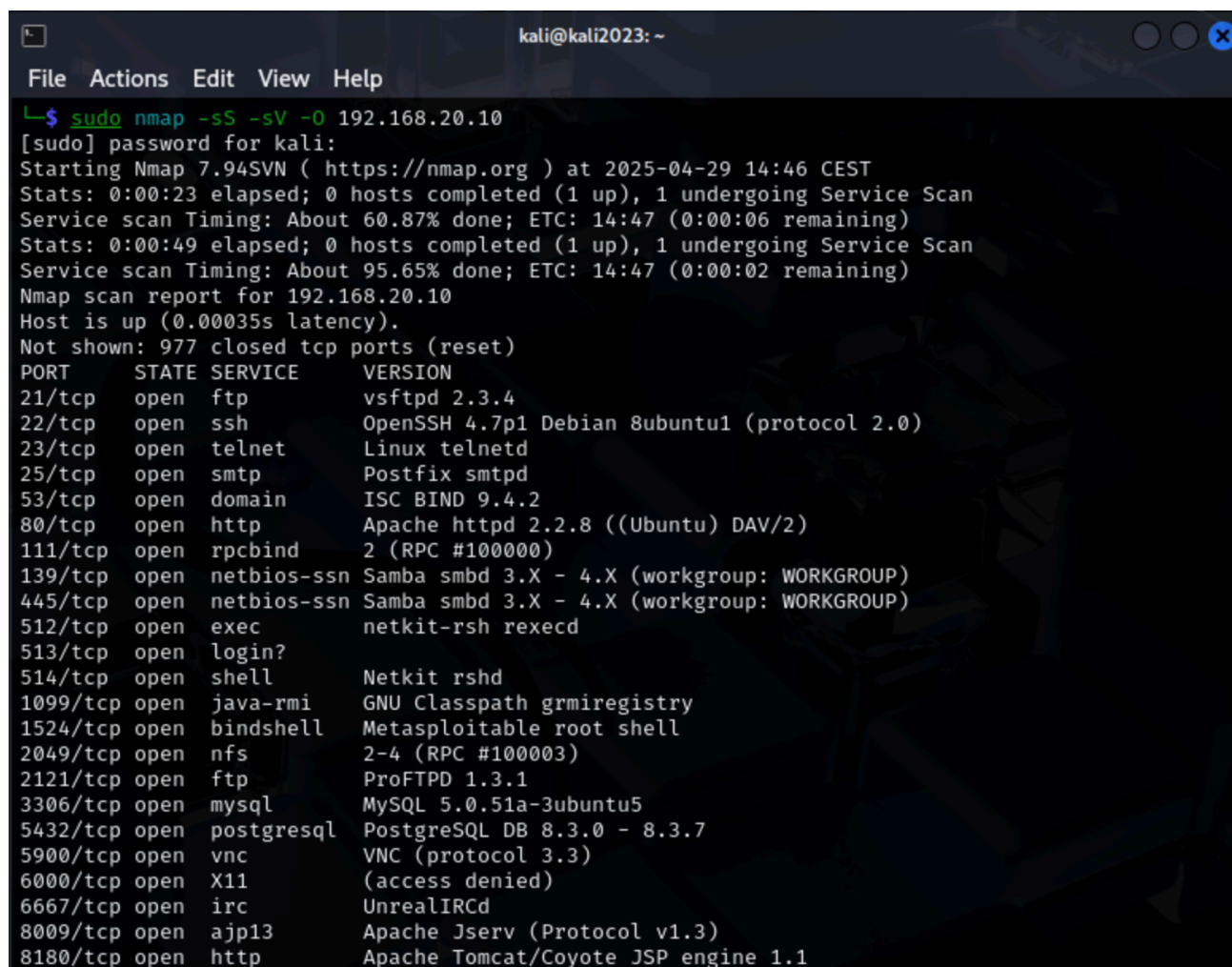
1. OS Fingerprint - Syn Scan - Version Detection:

sudo nmap -sS -sV -O 192.168.20.10

2. TCP Connect Scan:

sudo nmap -sT 192.168.20.10

1.



```
kali@kali2023: ~  
File Actions Edit View Help  
└─$ sudo nmap -sS -sV -O 192.168.20.10  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 14:46 CEST  
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 60.87% done; ETC: 14:47 (0:00:06 remaining)  
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 95.65% done; ETC: 14:47 (0:00:02 remaining)  
Nmap scan report for 192.168.20.10  
Host is up (0.00035s 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
```

2.

```
(kali㉿kali2023)-[~]
$ sudo nmap -sT 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 14:54 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00089s 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: F2:CA:0C:23:AF:9A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

Per il Target B (192.168.64.5):

1. OS Fingerprint:

sudo nmap -O --osscan-guess 192.168.64.5

```
(kali㉿kali2023)-[~]
$ sudo nmap -O --osscan-guess 192.168.64.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 15:10 CEST
Nmap scan report for 192.168.64.5
Host is up (0.0014s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 76:81:41:C0:F0:5F (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 2.32 seconds
```

3. Risultati

3.1 Target A: 192.168.20.10

3.1.1 OS Fingerprinting

- **Sistema operativo rilevato:** Linux Kernel 2.6 X

3.1.2 Stato Porte: Syn Scan vs TCP Connect

Porta	Servizio	Stato (SYN)	Stato (Connect)
22	ssh	open	open
80	http	open	open
3306	mysql	open	open

3.1.3 Version Detection

Porta	Servizio	Versione	Path/Risposta Banner
22	ssh	OpenSSH 4.7p1	Debian 8ubuntu 1
80	http	Apache httpd 2.2.8	Server: Apache/2.2.8 (Ubuntu)

3.2 Target B: 192.168.64.5

3.2.1 OS Fingerprinting

3.2.3 Stato Porte: Syn Scan vs TCP Connect

Porta	Servizio	Stato (SYN)	Stato (Connect)
80	http	open	open

5. Raccomandazioni

- **Aggiornamento regolare:** Monitorare e applicare patch di sicurezza per Apache e OpenSSH.

6. Conclusioni

Le scansioni Nmap hanno fornito un quadro chiaro dei sistemi target, implementare le raccomandazioni garantirà un incremento del livello di sicurezza complessivo.