

# Report di Scansione Nmap

Data 20/12/2023

Guglielmo Carratello

## Scansione su Metasploitable2

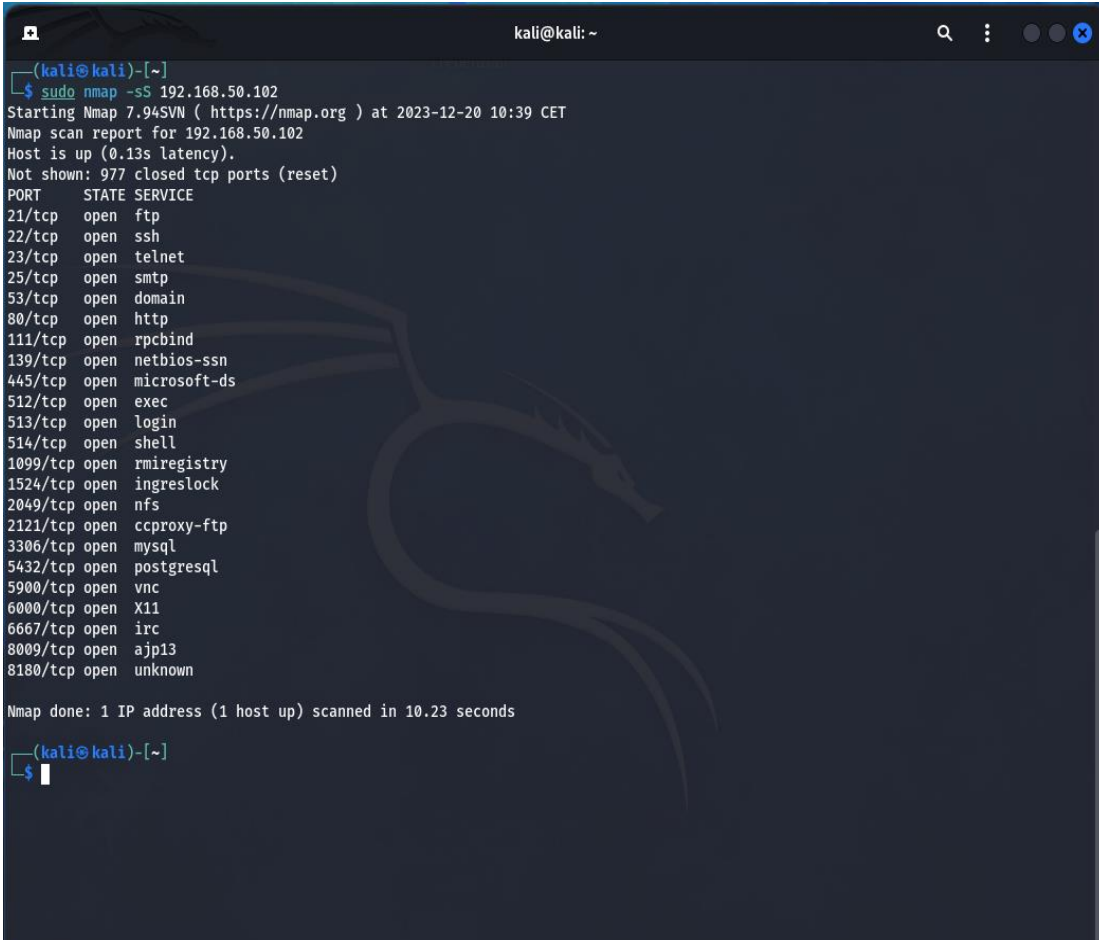
### Obiettivo della Scansione:

La scansione è stata condotta sul target 192.168.50.102, questo appartiene ad una rete differente alla macchina attaccante (Kali Linux) al fine di ottenere informazioni dettagliate sulla sua infrastruttura di rete, i servizi in esecuzione e identificare il sistema operativo. La comunicazione su reti diverse è stata resa possibile utilizzando PfSense (firewall).

### Parametri della Scansione:

#### -sS (Scansione Stealth SYN):

Questa opzione esegue una scansione stealth utilizzando pacchetti SYN senza stabilire una connessione completa. È veloce e discreta, adatta per evitare rilevamenti intrusivi. In pratica manda una richiesta syn, riceve la risposta syn/ack e termina la richiesta con rst/ack senza creare la connessione. Fornisce informazioni sullo stato delle porte aperte e dei servizi attivi per ogni porta.



```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 10:39 CET
Nmap scan report for 192.168.50.102
Host is up (0.13s 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

Nmap done: 1 IP address (1 host up) scanned in 10.23 seconds
(kali@kali)-[~]
└─$
```

-sT (Scansione TCP Connect):

Questa opzione effettua una scansione TCP completa, stabilendo una connessione completa con il target. È più intrusiva rispetto a -sS poiché completa la connessione TCP.

In pratica completa la procedura del Three-way-Handshake, connessione completa con le porte aperte, e quindi più intrusiva e di conseguenza rilevabile.

Utile per identificare servizi che potrebbero rispondere solo a connessioni complete.

```
kali@kali: ~  
└─(kali@kali)-[~]  
$ sudo nmap -sT 192.168.50.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 10:41 CET  
Nmap scan report for 192.168.50.102  
Host is up (0.038s 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  
  
Nmap done: 1 IP address (1 host up) scanned in 10.68 seconds  
  
└─(kali@kali)-[~]  
$
```

-sV (Rilevamento della Versione del Servizio):

Utilizzando questa opzione, Nmap cerca di identificare le versioni dei servizi in esecuzione sulle porte aperte. Fornisce informazioni dettagliate sulle applicazioni e le versioni esatte dei servizi. Utilizzato per individuare potenziali vulnerabilità associate alle versioni specifiche dei servizi.

```
kali@kali: ~  
└─(kali@kali)-[~]  
└─$ sudo nmap -sV 192.168.50.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 10:44 CET  
Nmap scan report for 192.168.50.102  
Host is up (0.037s 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  tcpwrapped     
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  
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 24.38 seconds  
  
└─(kali@kali)-[~]  
└─$
```

-O (Rilevamento del Sistema Operativo):

Questa opzione consente a Nmap di tentare di identificare il sistema operativo in esecuzione sul target. Analizza le risposte ai pacchetti inviati per dedurre il sistema operativo. Sulla pratica questa operazione stabilisce la probabilità del sistema operativo in uso sulla macchina target in base ad alcuni dati presenti nei pacchetti di risposta dalla macchina target.

```
kali@kali: ~  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.50.102  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 10:36 CET  
Nmap scan report for 192.168.50.102  
Host is up (0.097s 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  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)  
Network Distance: 2 hops  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 15.75 seconds  
(kali@kali)-[~]  
$
```

## Risultati della Scansione:

Dati i risultati ottenuti possiamo dedurre che la macchina in esame non ha un sistema di protezione perimetrale che filtra il traffico di rete, di conseguenza siamo riusciti ad ottenere i risultati desiderati per ogni scansione.

## Scansione di Windows7

### Obiettivo della Scansione:

La scansione è stata condotta sul target 192.168.5.101, questo appartiene ad una rete differente alla macchina attaccante (Kali Linux) al fine di ottenere informazioni dettagliate sulla sua infrastruttura di rete, i servizi in esecuzione e identificare il sistema operativo. La comunicazione su reti diverse è stata resa possibile utilizzando PfSense (firewall). Inoltre è presente di default un firewall per Windows7.

### Parametri della Scansione:

-O (Rilevamento del sistema operativo):

```
kali@kali: ~  
└─(kali@kali)-[~]  
$ sudo nmap -O 192.168.5.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 10:59 CET  
Nmap scan report for 192.168.5.101  
Host is up (0.014s latency).  
All 1000 scanned ports on 192.168.5.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specialized|VoIP phone|general purpose|phone  
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player  
OS CPE: cpe:/h:allen-bradley:microlgix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player  
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR168 8 VoIP module, VMware Player virtual NAT device  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 42.44 seconds  
  
└─(kali@kali)-[~]  
$
```

-sS (Scansione Stealth SYN), -sT (Scansione TCP connect), -sV (Rilevamento della versione del servizio):

Abbiamo eseguito tutte e tre i tipi di scansione su windows7

```
kali@kali: ~  
└─(kali@kali)-[~]  
$ sudo nmap -sS 192.168.5.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:01 CET  
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan  
Ping Scan Timing: About 100.00% done; ETC: 11:01 (0:00:00 remaining)  
Nmap scan report for 192.168.5.101  
Host is up (0.048s latency).  
All 1000 scanned ports on 192.168.5.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 67.72 seconds  
  
└─(kali@kali)-[~]  
$ sudo nmap -sT 192.168.5.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:03 CET  
Nmap scan report for 192.168.5.101  
Host is up (0.032s latency).  
All 1000 scanned ports on 192.168.5.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 49.99 seconds  
  
└─(kali@kali)-[~]  
$ sudo nmap -sV 192.168.5.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:04 CET  
Nmap scan report for 192.168.5.101  
Host is up (0.016s latency).  
All 1000 scanned ports on 192.168.5.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 40.88 seconds  
  
└─(kali@kali)-[~]  
$
```



Risultati della scansione:

Si noti che nonostante le macchine comunichino la presenza del firewall nella macchina windows7 non ci ha permesso di stabilire quali porte e servizi sono attivi. Questo perché come da screen nmap fa presente che i pacchetti inviati alle porte sono stati filtrati e di conseguenza bloccati.

L'unico risultato interessante è la versione del sistema operativo in uso. Infatti nella scansione -O (Rilevamento del sistema operativo) in base alla risposta ottenuta nmap comunica che secondo lui il sistema operativo della macchina target è un sistema windows ma fa presente alcune delle versioni possibile senza specificare quella corretta.

Conclusione:

Una volta modificati gli IP delle due macchine target ed impostate sulla stessa rete della macchina attaccante Kali Linux si sono effettuate di nuovo le scansioni, stavolta senza servirci della macchina PfSense dato che siamo sulla stessa rete. Nei confronti di Metasploitable le scansioni sono avvenute come previsto e quindi abbiamo ricevuto gli stessi risultati ottenuti precedentemente così come le risposte di windows7. Infatti windows7 ha ridato gli stessi risultati negativi perché esso ha il firewall attivo.

Per poter ottenere i dati di interesse della macchina windows7 come le porte e i servizi, si potrebbe utilizzare l'opzione (-T) Timing di nmap. Questo permette di impostare degli intervalli di tempo tra una richiesta e l'altra. Ciò permette di bypassare il controllo del firewall e passare inosservati e di conseguenza ottenere i dati che ci interessano. Nello screen si possono vedere le due risposte;

```
kali@kali: ~  
$ sudo nmap -O 192.168.32.101,102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:14 CET  
Nmap scan report for epicode.internal (192.168.32.101)  
Host is up (0.010s latency).  
All 1000 scanned ports on epicode.internal (192.168.32.101) are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:8F:C2:9E (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specialized|VoIP phone|general purpose|phone  
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player  
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_xp_sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player  
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device  
Network Distance: 1 hop  
  
Nmap scan report for 192.168.32.102  
Host is up (0.0082s 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:F8:25:17 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X
```