

Consegna M3 – week 9 day 1 – Daniele Rufo

Ho eseguito le scansioni richieste dall’esercizio e raccolto i dati in una tabella. Sotto ho aggiunto anche gli screenshot delle scansioni così da avere anche l’output mandato al prompt da nmap e poter verificare le osservazioni.

Fonte	Target	Metodologia	Osservazioni
192.169.50.100	192.169.50.101	-sS	-sS (SYN) è una scansione in modalità stealth. È più rapida e genera meno rumore perché non conclude il 3wayhandshake (si ferma al syn/ack e poi manda un rst per chiudere il canale). Ha più possibilità quindi di passare i controlli di IDS/Firewall e non essere rilevato, inoltre, aiuta a non sovraccaricare la linea con molte richieste tcp. La scansione -sN (TCP NULL) è ancora meno invasiva perché invia pacchetti senza flag (SYN,ACK, RST, PSH, FIN, URG, CWR)
192.169.50.100	192.169.50.101	-sT	-sT (TCP) invece per ogni porta controllata chiude il 3wayhandshake e quindi lascia traccia. Il risultato a video risulta uguale a quello del comando -sS
192.169.50.100	192.169.50.101	-A	Metodologia di scan aggressiva (A) e completa. Impiega più tempo, ma recupera molte più informazioni sui servizi in uso. Basta paragonare infatti i risultati delle scansioni: con -sS e -sT sappiamo che la porta 80 è aperta per un servizio http, ma con -A anche il nome della macchina, l’OS ed il server (Apache). Vediamo ancora come l’analisi sia più approfondita infatti con “ftp -anon IP” controlla anche se sono permessi login anonimi e ne riporta lo stato (beccata la nostra kali di cui riporta l’IP).

Scansione con -sS

```
(kali@kali)-[~]
└─$ sudo nmap -sS -p1-1023 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 12:05 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00029s latency).
Not shown: 1011 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: 08:00:27:59:6D:7F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

(kali@kali)-[~]
└─$
```

## Scansione con -sT

```
(kali@kali)-[~]
$ sudo nmap -sT -p1-1023 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 12:06 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00040s latency).
Not shown: 1011 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
MAC Address: 08:00:27:59:6D:7F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

(kali@kali)-[~]
$
```

## Scansione con -sN

```
File  Macchina  Visualizza  Aiuto
[Icons] 1 2 3 4 [Window]

kali@kali: ~
(kali@kali)-[~]
$ sudo nmap -sN 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 11:53 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:59:6D:7F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

## Scansione con switch -A (3screenshot)

1/3

```
(kali@kali)-[~]
$ sudo nmap -A -p1-1023 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 12:13 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
Not shown: 1011 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 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
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
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-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

2/3

```
kali@kali: ~
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         59384/tcp  mountd
|   100005  1,2,3         60032/udp  mountd
|   100021  1,3,4         34723/tcp  nlockmgr
|   100021  1,3,4         58970/udp  nlockmgr
|   100024  1             39400/tcp  status
|   100024  1             39825/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 rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
MAC Address: 08:00:27:59:6D:7F (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-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2024-07-02T12:14:33-04:00
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s
```

```
514/tcp open  shell           Netkit rshd
MAC Address: 08:00:27:59:6D:7F (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-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-07-02T12:14:33-04:00
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s
|_ smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1   0.59 ms  192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.42 seconds
```

```
(kali㉿kali)-[~]
$
```