PROGETTO W9D1 - Pratica

Nmap: Scansioni e Analisi

Ho effettuato tre tipologie di scansioni, TCP, SYN e AGGRESSIVE con Nmap verso la macchina metasploitable con Ip 192.168.50.102 e sniffato il traffico di rete per analizzare e confrontare le scansioni messe in atto.

- Scansione 1: TCP (-sT)

Comando: nmap -oX tcp_scan.xml -sT -r 192.168.50.102

Descrizione: **-oX** tcp_scan.xml salva l'output della scansione nel file tcp_scan.xml
-sT esegue scansione in TCP
-r scansiona le porte per ordine non casuale (inserito solo per apprendimento)

Risultati: tcp_scan.pdf

Wireshark:

Ho filtrato la porta 21,22,23 su wireshark e si nota la stretta di mano (HANDSHAKE):

1. il Client "192.168.50.101" esegue tre richieste SYN al server "192.168.50.102".
2. Il Server risponde con SYN, ACK. (Conferma la disponibilità)
3. Il Client risponde con ACK. (Qui la connessione è realmente stabilita!)
4. Il Client invia un RST al server per chiudere la connessione.

Source	Destination	Protocol	Length	Info
192.168.50.101	192.168.50.102	TCP	74	40484 → 21 [SYN] Seq=0 Win=6
192.168.50.101	192.168.50.102	TCP	74	56998 → 22 [SYN] Seq=0 Win=6
192.168.50.101	192.168.50.102	TCP	74	46394 → 23 [SYN] Seq=0 Win=6
192.168.50.102	192.168.50.101	TCP	74	21 → 40484 [SYN, ACK] Seq=0
192.168.50.101	192.168.50.102	TCP	66	40484 → 21 [ACK] Seq=1 Ack=1
192.168.50.102	192.168.50.101	TCP	74	22 → 56998 [SYN, ACK] Seq=0
192.168.50.101	192.168.50.102	TCP	66	56998 → 22 [ACK] Seq=1 Ack=1
192.168.50.102	192.168.50.101	TCP	74	23 → 46394 [SYN, ACK] Seq=0
192.168.50.101	192.168.50.102	TCP	66	46394 → 23 [ACK] Seq=1 Ack=1
192.168.50.101	192.168.50.102	TCP	66	40484 → 21 [RST, ACK] Seq=1
192.168.50.101	192.168.50.102	TCP	66	56998 → 22 [RST, ACK] Seq=1
192.168.50.101	192.168.50.102	TCP	66	46394 → 23 [RST, ACK] Seq=1

```
┌──(kali㉿kali)-[~]
└─$ nmap -oX tcp_scan.xml -sT -r 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 10:24 EST
Nmap scan report for metasploitable (192.168.50.102)
Host is up (0.00033s 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: 00:0C:29:F9:38:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

- **Scansione 2:** SYN (`-sS`)

Comando: nmap -oX syn_scan.xml -sS -r 192.168.50.102

Descrizione: **-oX** syn_scan.xml salva l'output della scansione nel file syn_scan.xml
-sS esegue scansione SYN
-r scansiona le porte per ordine non casuale (inserito solo per apprendimento)

Output: syn_scan.pdf

Wireshark:

Ho filtrato la porta 21,22,23 su wireshark e si nota la stretta di mano (HANDSHAKE):

1. il Client "192.168.50.101" esegue tre richieste SYN al server "192.168.50.102".
2. Il Server risponde con SYN, ACK. (Conferma la disponibilità)
3. Il Client risponde con RST per chiudere la connessione. (La connessione non viene stabilita)

Source	Destination	Protocol	Length	Info
192.168.50.101	192.168.50.102	TCP	58	62941 → 21 [SYN] Seq=0
192.168.50.101	192.168.50.102	TCP	58	62941 → 22 [SYN] Seq=0
192.168.50.101	192.168.50.102	TCP	58	62941 → 23 [SYN] Seq=0
192.168.50.102	192.168.50.101	TCP	60	21 → 62941 [SYN, ACK] S
192.168.50.101	192.168.50.102	TCP	54	62941 → 21 [RST] Seq=1
192.168.50.102	192.168.50.101	TCP	60	22 → 62941 [SYN, ACK] S
192.168.50.101	192.168.50.102	TCP	54	62941 → 22 [RST] Seq=1
192.168.50.102	192.168.50.101	TCP	60	23 → 62941 [SYN, ACK] S
192.168.50.101	192.168.50.102	TCP	54	62941 → 23 [RST] Seq=1

```
┌──(kali㉿kali)-[~]
└─$ nmap -oX syn_scan.xml -sS -r 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 23:42 CET
Nmap scan report for metasploitable (192.168.50.102)
Host is up (0.00050s 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: 00:0C:29:F9:38:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

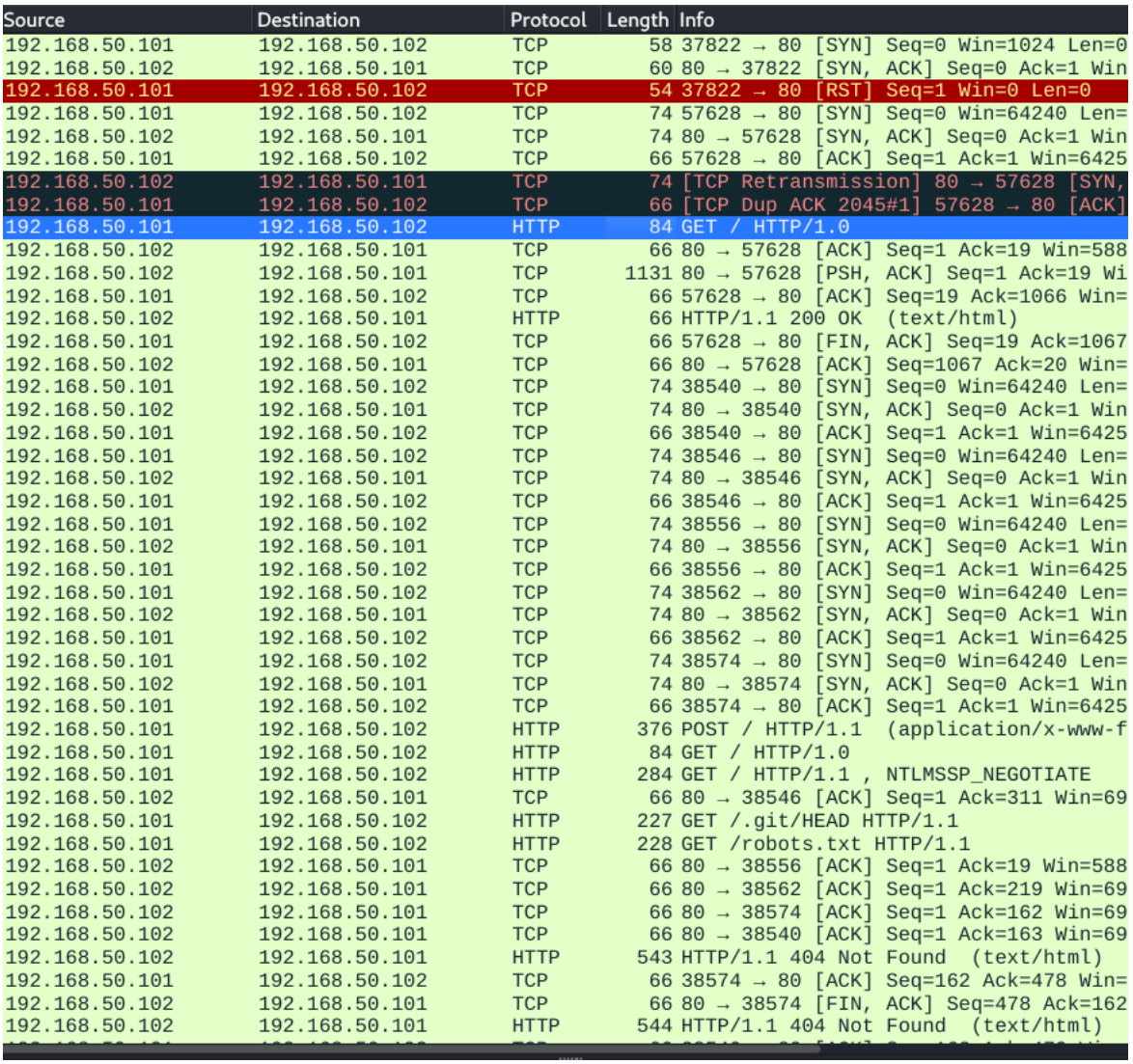
- Scansione 3: Aggressive (-A)

Comando: nmap -oX scan.xml -A 192.168.50.102

Descrizione: **-oX** syn_scan.xml salva l'output della scansione nel file syn_scan.xml
-A rileva OS, versione dei servizi trovati e avvia script di default

Output: aggressive_scan.pdf

Wireshark: Ho filtrato la porta 80 su wireshark e si nota l'handshake completo come la scansione tcp, le chiamate GET e POST, il tipo di servizio e versione che non sono presenti nell'immagine ma si trovano nel PDF.



Source	Destination	Protocol	Length	Info
192.168.50.101	192.168.50.102	TCP	58	37822 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.50.102	192.168.50.101	TCP	60	80 → 37822 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	54	37822 → 80 [RST] Seq=1 Win=0 Len=0
192.168.50.101	192.168.50.102	TCP	74	57628 → 80 [SYN] Seq=0 Win=64240 Len=
192.168.50.102	192.168.50.101	TCP	74	80 → 57628 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	66	57628 → 80 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.102	192.168.50.101	TCP	74	[TCP Retransmission] 80 → 57628 [SYN,
192.168.50.101	192.168.50.102	TCP	66	[TCP Dup ACK 2045#1] 57628 → 80 [ACK]
192.168.50.101	192.168.50.102	HTTP	84	GET / HTTP/1.0
192.168.50.102	192.168.50.101	TCP	66	80 → 57628 [ACK] Seq=1 Ack=19 Win=588
192.168.50.102	192.168.50.101	TCP	1131	80 → 57628 [PSH, ACK] Seq=1 Ack=19 Wi
192.168.50.101	192.168.50.102	TCP	66	57628 → 80 [ACK] Seq=19 Ack=1066 Win=
192.168.50.102	192.168.50.101	HTTP	66	HTTP/1.1 200 OK (text/html)
192.168.50.101	192.168.50.102	TCP	66	57628 → 80 [FIN, ACK] Seq=19 Ack=1067
192.168.50.102	192.168.50.101	TCP	66	80 → 57628 [ACK] Seq=1067 Ack=20 Win=
192.168.50.101	192.168.50.102	TCP	74	38540 → 80 [SYN] Seq=0 Win=64240 Len=
192.168.50.102	192.168.50.101	TCP	74	80 → 38540 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	66	38540 → 80 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.101	192.168.50.102	TCP	74	38546 → 80 [SYN] Seq=0 Win=64240 Len=
192.168.50.102	192.168.50.101	TCP	74	80 → 38546 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	66	38546 → 80 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.101	192.168.50.102	TCP	74	38556 → 80 [SYN] Seq=0 Win=64240 Len=
192.168.50.102	192.168.50.101	TCP	74	80 → 38556 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	66	38556 → 80 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.101	192.168.50.102	TCP	74	38562 → 80 [SYN] Seq=0 Win=64240 Len=
192.168.50.102	192.168.50.101	TCP	74	80 → 38562 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	66	38562 → 80 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.101	192.168.50.102	TCP	74	38574 → 80 [SYN] Seq=0 Win=64240 Len=
192.168.50.102	192.168.50.101	TCP	74	80 → 38574 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.101	192.168.50.102	TCP	66	38574 → 80 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.101	192.168.50.102	HTTP	376	POST / HTTP/1.1 (application/x-www-f
192.168.50.101	192.168.50.102	HTTP	84	GET / HTTP/1.0
192.168.50.101	192.168.50.102	HTTP	284	GET / HTTP/1.1 , NTLMSSP_NEGOTIATE
192.168.50.102	192.168.50.101	TCP	66	80 → 38546 [ACK] Seq=1 Ack=311 Win=69
192.168.50.101	192.168.50.102	HTTP	227	GET /.git/HEAD HTTP/1.1
192.168.50.101	192.168.50.102	HTTP	228	GET /robots.txt HTTP/1.1
192.168.50.102	192.168.50.101	TCP	66	80 → 38556 [ACK] Seq=1 Ack=19 Win=588
192.168.50.102	192.168.50.101	TCP	66	80 → 38562 [ACK] Seq=1 Ack=219 Win=69
192.168.50.102	192.168.50.101	TCP	66	80 → 38574 [ACK] Seq=1 Ack=162 Win=69
192.168.50.102	192.168.50.101	TCP	66	80 → 38540 [ACK] Seq=1 Ack=163 Win=69
192.168.50.102	192.168.50.101	HTTP	543	HTTP/1.1 404 Not Found (text/html)
192.168.50.101	192.168.50.102	TCP	66	38574 → 80 [ACK] Seq=162 Ack=478 Win=
192.168.50.102	192.168.50.101	TCP	66	80 → 38574 [FIN, ACK] Seq=478 Ack=162
192.168.50.102	192.168.50.101	HTTP	544	HTTP/1.1 404 Not Found (text/html)

Le tre scansioni presentano differenze significative in termini di rilevabilità e dettagli ottenuti. La scelta della scansione dipende dagli obiettivi specifici e dal livello di intrusività consentito.

Francesco Rinaldi