Security Operation: azioni preventive

Traccia

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP

2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per la service detection e -o nomefilereport per salvare in un file l'output)

3. Abilitare il Firewall sulla macchina Windows XP

4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.

5. Trovare le eventuali differenze e motivarle.

Requisiti:

- Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150
- Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

Domande alla quale rispondere:

- Che differenze notate?
- E quale può essere la causa del risultato diverso?

Configurazione indirizzo IP della macchina "**Kali Linux**"

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.255
        inet6 fe80::a00:27ff:fe2b:7e2e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2b:7e:2e  txqueuelen 1000  (Ethernet)
        RX packets 67  bytes 7288 (7.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2123  bytes 133742 (130.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Configurazione indirizzo IP della macchina "**WindowsXP**"

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.240.150
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

Scansione e analisi del traffico con wireshark avendo il FireWall attivo

Attivazione **FireWall**.

Scansione tramite il comando "**nmap -sV -oN + nome file salvataggio report + indirizzo IP target**" verso la macchina target "**WIndowsXP**" con il firewall attivo. Come si può ben notare dallo screen, essendoci il firewall attivo, la scansione non ha fornito nessuna informazione.

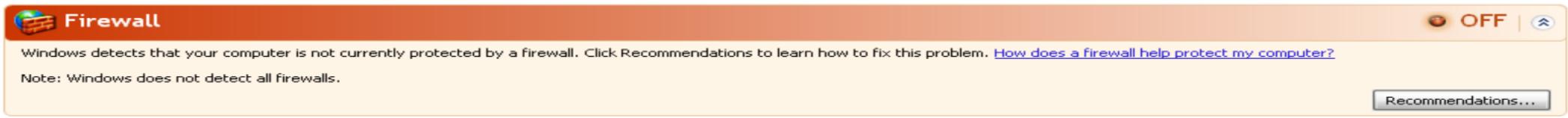
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -oN Scan_result_FWon.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:43 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.21 seconds
```

Analisi traffico di rete catturato con Wireshark e Firewall attivo

1. **Annunci di Rete (BROWSER Protocol)**
   - **Pacchetti 1-3**:
     - **Provenienza**: 192.168.240.150
     - **Destinazione**: 192.168.240.255 (broadcast)
     - **Protocollo**: BROWSER
     - **Descrizione**: Annunci del Master Browser Locale e del Gruppo di Lavoro. Utilizzati per la gestione e l'annuncio di dispositivi di rete in ambienti Windows.
2. **Tentativi di Connessione TCP (SYN)**
   - **Pacchetti 4-8**:
     - **Provenienza**: 192.168.240.150
     - **Destinazione**: 192.168.240.100
     - **Protocollo**: TCP
     - **Descrizione**: Richieste di connessione (SYN) verso le porte HTTP (80) e HTTPS (443). Indicazioni di tentativi di stabilire una connessione TCP.
3. **Ritrasmissioni TCP**
   - **Pacchetti 9-10**:
     - **Provenienza**: 192.168.240.100
     - **Destinazione**: 192.168.240.150
     - **Protocollo**: TCP
     - **Descrizione**: Ritrasmissioni di pacchetti TCP per le porte 80 (HTTP) e 443 (HTTPS), indicando problemi di rete o mancate risposte ai tentativi di connessione iniziali.
4. **Richieste ARP**
   - **Pacchetti 11-12**:
     - **Provenienza**: PCSSystmetec_2b:7e:..., PCSSystmetec_7e:6d:...
     - **Destinazione**: Broadcast (ff:ff:ff:ff:ff
     -)
     - **Protocollo**: ARP
     - **Descrizione**: Richieste di risoluzione indirizzi IP a indirizzi MAC. "Who has 192.168.240.150?" e la risposta corrispondente

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.240.150	192.168.240.255	BROWSER	243	Local Master Announcement WINDOWSXP, Workstation, Server, NT Workstation, Potential Browser, Master Browser
2	77.310404278	192.168.240.150	192.168.240.255	BROWSER	252	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
3	720.204641947	192.168.240.150	192.168.240.255	BROWSER	243	Local Master Announcement WINDOWSXP, Workstation, Server, NT Workstation, Potential Browser, Master Browser
4	838.032328694	192.168.240.100	192.168.240.150	TCP	74	50186 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255135617 TSecr=0 WS=128
5	838.032596457	192.168.240.100	192.168.240.150	TCP	74	33508 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255135617 TSecr=0 WS=128
6	840.034471621	192.168.240.100	192.168.240.150	TCP	74	48604 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255137619 TSecr=0 WS=128
7	840.034782943	192.168.240.100	192.168.240.150	TCP	74	53432 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255137619 TSecr=0 WS=128
8	841.047751372	192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 53432 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255138632 TSecr=0 WS=128
9	841.048614349	192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 48604 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255138633 TSecr=0 WS=128
10	843.253560761	PCSSystemtec_2b:7e:…	PCSSystemtec_7e:6d:…	ARP	42	Who has 192.168.240.150? Tell 192.168.240.100
11	843.255475945	PCSSystemtec_7e:6d:…	PCSSystemtec_2b:7e:…	ARP	60	192.168.240.150 is at 08:00:27:7e:6d:d1

Disattivazione **FireWall**



Scansione tramite il comando "**nmap -sV -oN + nome file salvataggio report + indirizzo IP target**" verso la macchina target "**WIndowsXP**" con il firewall disattivato e identificazione delle porte aperte "**135, 139, 445, 3389**" e dei servizi a loro correlati.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -oN Scan_result_FWoff.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:32 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.0047s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.57 seconds
```

Scansione e analisi del traffico con wireshark avendo il FireWall disattivato

Utilizzo del filtro "**icmp**"per visualizzare solo i pacchetti ICMP e verificare la raggiungibilità della macchina target.

icmp

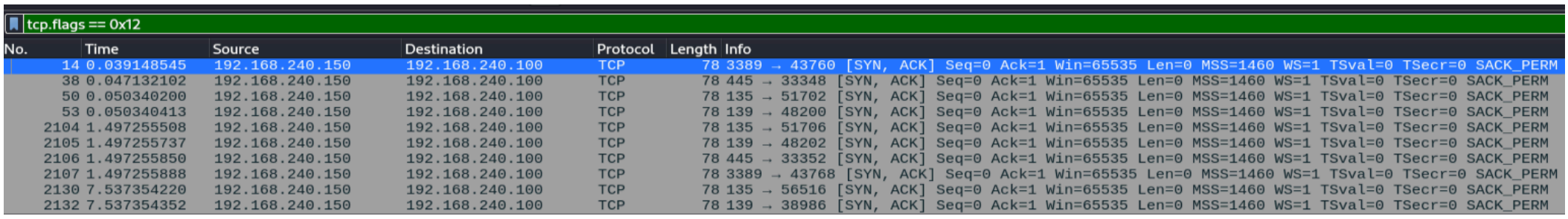
No.	Time	Source	Destination	Protocol	Length	Info
2	0.035898545	192.168.240.100	192.168.240.150	ICMP	98	Echo (ping) request id=0x3edb, seq=1/256, ttl=64 (reply in 3)
3	0.037506120	192.168.240.150	192.168.240.100	ICMP	98	Echo (ping) reply id=0x3edb, seq=1/256, ttl=128 (request in 2)
4	1.037792681	192.168.240.100	192.168.240.150	ICMP	98	Echo (ping) request id=0x3edb, seq=2/512, ttl=64 (reply in 5)
5	1.040112541	192.168.240.150	192.168.240.100	ICMP	98	Echo (ping) reply id=0x3edb, seq=2/512, ttl=128 (request in 4)
6	2.038957778	192.168.240.100	192.168.240.150	ICMP	98	Echo (ping) request id=0x3edb, seq=3/768, ttl=64 (reply in 7)
7	2.040942148	192.168.240.150	192.168.240.100	ICMP	98	Echo (ping) reply id=0x3edb, seq=3/768, ttl=128 (request in 6)
8	3.040305211	192.168.240.100	192.168.240.150	ICMP	98	Echo (ping) request id=0x3edb, seq=4/1024, ttl=64 (reply in 9)
9	3.041892337	192.168.240.150	192.168.240.100	ICMP	98	Echo (ping) reply id=0x3edb, seq=4/1024, ttl=128 (request in 8)

Utilizzo del filtro "**tcp.flags.syn == 1 && tcp.flags.ack == 0**" per vedere tutti i pacchetti SYN inviati e mostrare tutte le richieste di connessione inviate da nmap.

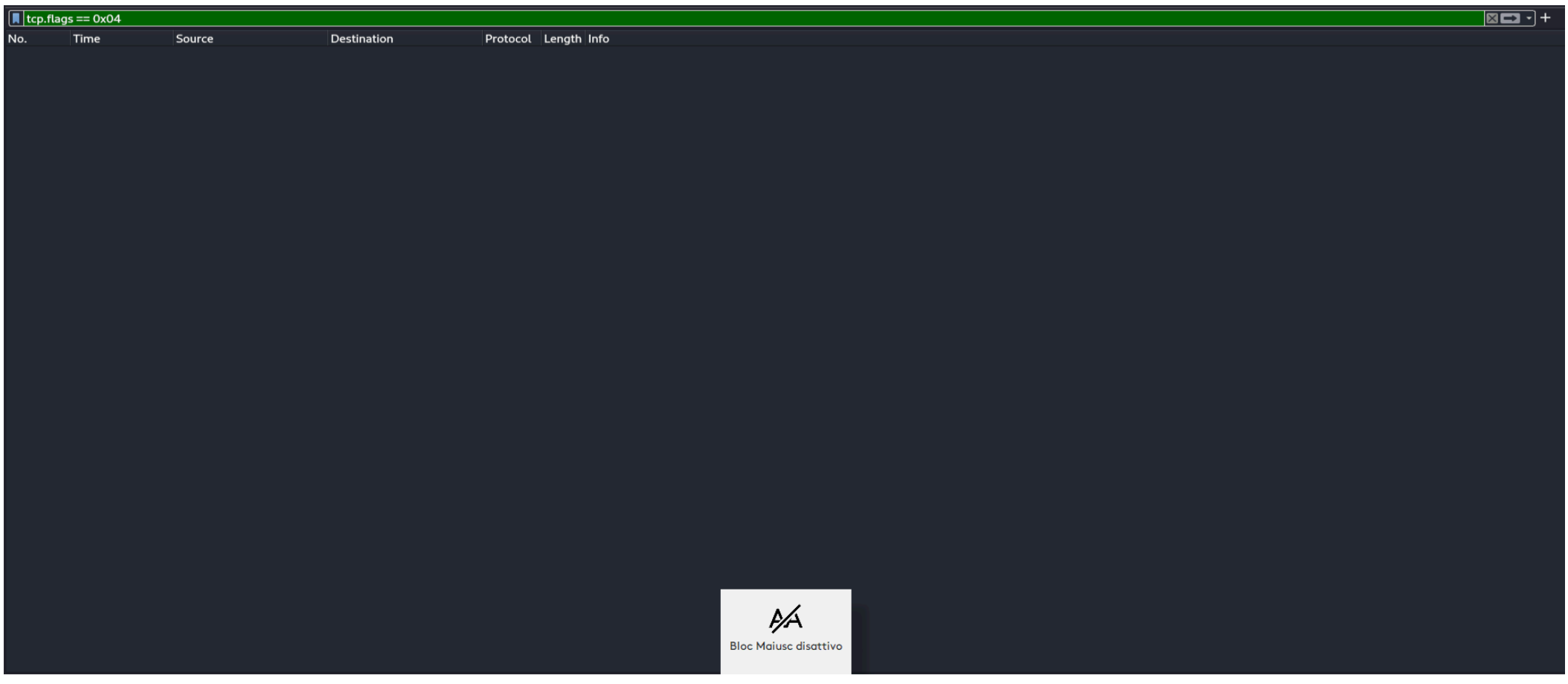
tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.240.100	192.168.240.150	TCP	74	60702 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541778 TSecr=0 WS=128
5	0.030677329	192.168.240.100	192.168.240.150	TCP	74	50150 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541809 TSecr=0 WS=128
7	0.036855123	192.168.240.100	192.168.240.150	TCP	74	33804 → 993 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541815 TSecr=0 WS=128
8	0.037514026	192.168.240.100	192.168.240.150	TCP	74	35002 → 256 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541816 TSecr=0 WS=128
9	0.037928213	192.168.240.100	192.168.240.150	TCP	74	48854 → 53 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541816 TSecr=0 WS=128
10	0.038491174	192.168.240.100	192.168.240.150	TCP	74	43760 → 3389 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541816 TSecr=0 WS=128
16	0.039962310	192.168.240.100	192.168.240.150	TCP	74	60714 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541818 TSecr=0 WS=128
17	0.040380571	192.168.240.100	192.168.240.150	TCP	74	38786 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541818 TSecr=0 WS=128
18	0.040774303	192.168.240.100	192.168.240.150	TCP	74	41586 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541819 TSecr=0 WS=128
22	0.041722644	192.168.240.100	192.168.240.150	TCP	74	43280 → 1720 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541820 TSecr=0 WS=128
23	0.042131289	192.168.240.100	192.168.240.150	TCP	74	51026 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541820 TSecr=0 WS=128
24	0.042874238	192.168.240.100	192.168.240.150	TCP	74	49988 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541821 TSecr=0 WS=128
29	0.044033459	192.168.240.100	192.168.240.150	TCP	74	45542 → 587 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541822 TSecr=0 WS=128
30	0.044515200	192.168.240.100	192.168.240.150	TCP	74	35580 → 199 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541823 TSecr=0 WS=128
31	0.044913664	192.168.240.100	192.168.240.150	TCP	74	57322 → 113 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541823 TSecr=0 WS=128
35	0.045671602	192.168.240.100	192.168.240.150	TCP	74	33348 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541824 TSecr=0 WS=128
36	0.046020358	192.168.240.100	192.168.240.150	TCP	74	50154 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541824 TSecr=0 WS=128
37	0.046571101	192.168.240.100	192.168.240.150	TCP	74	59536 → 110 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541825 TSecr=0 WS=128
42	0.047711167	192.168.240.100	192.168.240.150	TCP	74	59412 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541826 TSecr=0 WS=128
43	0.048073508	192.168.240.100	192.168.240.150	TCP	74	41638 → 143 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541826 TSecr=0 WS=128
46	0.048771993	192.168.240.100	192.168.240.150	TCP	74	51702 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541827 TSecr=0 WS=128
47	0.049145375	192.168.240.100	192.168.240.150	TCP	74	33618 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541827 TSecr=0 WS=128
48	0.049556256	192.168.240.100	192.168.240.150	TCP	74	60972 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541828 TSecr=0 WS=128
49	0.049945679	192.168.240.100	192.168.240.150	TCP	74	48200 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541828 TSecr=0 WS=128
56	0.051439340	192.168.240.100	192.168.240.150	TCP	74	48064 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541829 TSecr=0 WS=128
57	0.051825324	192.168.240.100	192.168.240.150	TCP	74	54360 → 554 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541830 TSecr=0 WS=128
60	0.085310560	192.168.240.100	192.168.240.150	TCP	74	36402 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541863 TSecr=0 WS=128
65	0.102883805	192.168.240.100	192.168.240.150	TCP	74	40312 → 8888 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541881 TSecr=0 WS=128
66	0.103356551	192.168.240.100	192.168.240.150	TCP	74	59942 → 8080 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541881 TSecr=0 WS=128
67	0.103893934	192.168.240.100	192.168.240.150	TCP	74	40478 → 5900 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541882 TSecr=0 WS=128
68	0.104536675	192.168.240.100	192.168.240.150	TCP	74	34044 → 5989 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541883 TSecr=0 WS=128
69	0.105210038	192.168.240.100	192.168.240.150	TCP	74	56300 → 8021 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541883 TSecr=0 WS=128
70	0.105862558	192.168.240.100	192.168.240.150	TCP	74	41956 → 1106 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541884 TSecr=0 WS=128
77	0.108931275	192.168.240.100	192.168.240.150	TCP	74	43926 → 3003 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541887 TSecr=0 WS=128
78	0.109354707	192.168.240.100	192.168.240.150	TCP	74	45878 → 515 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541887 TSecr=0 WS=128
79	0.109754289	192.168.240.100	192.168.240.150	TCP	74	33874 → 19801 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541888 TSecr=0 WS=128
80	0.110284240	192.168.240.100	192.168.240.150	TCP	74	35872 → 16113 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541888 TSecr=0 WS=128
85	0.111541579	192.168.240.100	192.168.240.150	TCP	74	39688 → 20828 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541890 TSecr=0 WS=128
86	0.111957831	192.168.240.100	192.168.240.150	TCP	74	58228 → 32782 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541890 TSecr=0 WS=128
89	0.114491440	192.168.240.100	192.168.240.150	TCP	74	52658 → 900 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541892 TSecr=0 WS=128
90	0.115031521	192.168.240.100	192.168.240.150	TCP	74	41142 → 16018 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541893 TSecr=0 WS=128
91	0.115418359	192.168.240.100	192.168.240.150	TCP	74	60838 → 1840 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541893 TSecr=0 WS=128
95	0.116353632	192.168.240.100	192.168.240.150	TCP	74	56156 → 2046 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541894 TSecr=0 WS=128
96	0.116738487	192.168.240.100	192.168.240.150	TCP	74	48586 → 60020 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541895 TSecr=0 WS=128
97	0.117044560	192.168.240.100	192.168.240.150	TCP	74	41906 → 3920 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541895 TSecr=0 WS=128
98	0.117446855	192.168.240.100	192.168.240.150	TCP	74	55122 → 617 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541895 TSecr=0 WS=128
103	0.118275213	192.168.240.100	192.168.240.150	TCP	74	59622 → 8600 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541896 TSecr=0 WS=128
105	0.133399596	192.168.240.100	192.168.240.150	TCP	74	57632 → 1138 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541911 TSecr=0 WS=128
106	0.133736212	192.168.240.100	192.168.240.150	TCP	74	39152 → 49156 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541912 TSecr=0 WS=128
107	0.133955987	192.168.240.100	192.168.240.150	TCP	74	34684 → 9000 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2255541912 TSecr=0 WS=128

Utilizzo del filtro **“tcp.flags.syn == 1 && tcp.flags.ack == 1**" per vedere tutti i pacchetti SYN-ACK e mostrare tutte le risposte delle porte aperte.



Utilizzo del filtro “**tcp.flags.rst == 1**” per vedere tutte le risposte RST e mostrare le risposte relative alle porte chiuse. Ma come si può ben notare dallo screen sottostante, essendoci il firewall disattivato, non è stata identificata nessuna porta chiusa.



Analisi dei pacchetti:

- **Pacchetto 2112**
  - **Sorgente**: 192.168.240.100
  - **Destinazione**: 192.168.240.150
  - **Protocollo**: TCP
  - **Info**: Pacchetto con PSH, ACK. Indica che i dati sono inviati immediatamente senza buffer aggiuntivo.

- **Pacchetto 2113**
  - **Sorgente**: 192.168.240.150
  - **Destinazione**: 192.168.240.100
  - **Protocollo**: NBSS (NetBIOS Session Service)
  - **Info**: Messaggio di continuazione NBSS.

- **Pacchetto 2114**
  - **Sorgente**: 192.168.240.150
  - **Destinazione**: 192.168.240.100
  - **Protocollo**: SMB (Server Message Block)
  - **Info**: Richiesta di negoziazione del protocollo SMB.

- **Pacchetto 2115**
  - **Sorgente**: 192.168.240.150
  - **Destinazione**: 192.168.240.100

    - **Protocollo**: RDP (Remote Desktop Protocol)
    - **Info**: Richiesta di negoziazione del protocollo RDP.

- **Pacchetto 2116**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: NBSS
    - **Info**: Risposta di sessione negativa NBSS, errore non specificato.

- **Pacchetto 2117**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: COTP (ISO Connection Oriented Transport Protocol)
    - **Info**: TPDU CC inviato con riferimento di origine 0x1234, riferimento di destinazione 0x0000.

- **Pacchetto 2120**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: SMB
    - **Info**: Risposta di negoziazione del protocollo SMB.

- **Pacchetto 2136**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: TCP
    - **Info**: Pacchetto con PSH, ACK. Trasferimento di dati.

- **Pacchetto 2137**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: SMB
    - **Info**: Richiesta di negoziazione del protocollo SMB.

- **Pacchetto 2141**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: NBSS
    - **Info**: Risposta di sessione negativa NBSS, errore non specificato.

- **Pacchetto 2143**
    - **Sorgente**: 192.168.240.150
    - **Destinazione**: 192.168.240.100
    - **Protocollo**: DCERPC (DCE/RPC)
    - **Info**: Bind_nak, motivo: versione del protocollo non supportata.

Osservazioni

- **Traffico TCP con dati**: La maggior parte del traffico consiste in pacchetti TCP che contengono dati di negoziazione del protocollo.
- **Negoziazione del protocollo**: Sono visibili diverse richieste di negoziazione dei protocolli SMB e RDP.
- **Errori**: Ci sono risposte che indicano errori non specificati (NBSS) e negoziazioni non riuscite (DCERPC con versione del protocollo non supportata).

Questa analisi mostra l'interazione di diversi protocolli (NBSS, SMB, RDP, COTP) tra due host sulla rete, con alcune risposte di errore che indicano problemi di compatibilità o configurazione. Wireshark è utile per identificare e risolvere questi problemi analizzando il traffico di rete in dettaglio.

tcp.len > 0

No.	Time	Source	Destination	Protocol	Length	Info
2112	7.504618298	192.168.240.100	192.168.240.150	TCP	98	51706 → 135 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=32 TSval=2255549283 TSecr=0
2113	7.504745860	192.168.240.100	192.168.240.150	NBSS	84	NBSS Continuation Message
2114	7.504901019	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2115	7.505073096	192.168.240.100	192.168.240.150	RDP	108	Cookie: mstshash=nmap, Negotiate Request
2116	7.506642751	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2117	7.506642973	192.168.240.150	192.168.240.100	COTP	77	CC TPDU src-ref: 0x1234 dst-ref: 0x0000
2120	7.508826620	192.168.240.150	192.168.240.100	SMB	187	Negotiate Protocol Response
2136	7.537572199	192.168.240.100	192.168.240.150	TCP	234	56516 → 135 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=168 TSval=2255549316 TSecr=0
2139	7.537980367	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2141	7.539124253	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2143	7.539664385	192.168.240.150	192.168.240.100	DCERPC	90	Bind_nak: call_id: 1073809408, Fragment: Single reason: Protocol version not supported