

Convezione o normalita' la presenza dei firewall?

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 / 7
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 / 7
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch **-sV**.
5. Provare eventuale ulteriore **scansione differente** sempre con firewall attivato.
6. Trovare le eventuali differenze e motivarle

Configurazione delle macchine

Come primo passaggio, configuriamo le macchine con l'ip scelto e verifichiamo che il ping vada a buon fine:

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:e6:d5:f9 brd ff:ff:ff:ff:ff:ff
   inet 192.168.240.100/24 brd 192.168.240.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
   inet6 fe80::1c51:23f5:630f:711d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ping -c4 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.539 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.519 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.375 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.605 ms

— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.375/0.509/0.605/0.083 ms
```

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

Suffisso DNS specifico per connessione:

Indirizzo IP. : 192.168.240.150
Subnet mask : 255.255.255.0
Gateway predefinito : 192.168.240.1

C:\Documents and Settings\Administrator>ping 192.168.240.100

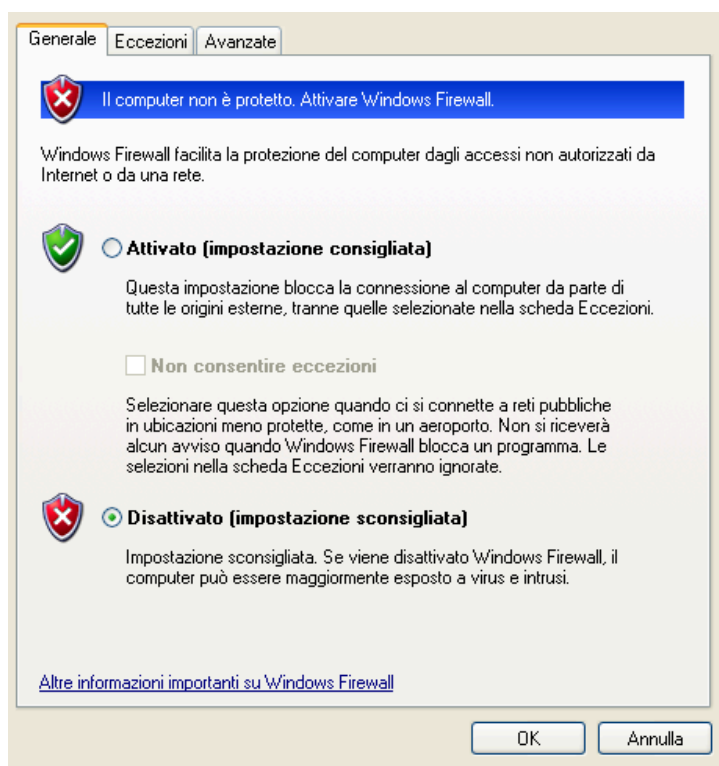
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.240.100:

Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 1ms, Medio = 0ms

Come seconda cosa verifichiamo che sia disattivo il firewall della macchina vittima, in questo caso windows XP:



Scansione senza firewall

Adesso possiamo mandare una scansione tramite **nmap** per ottenere informazioni:

```
(kali㉿kali)-[~]
$ nmap -sV -o dati.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 11:52 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00036s latency).
Not shown: 997 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
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 7.49 seconds
```

ove **-sV** sta per **service detection** che permette una scansione piu' approfondita, permette di ottenere dati sul tipo di servizio attivo e **-o** che sta per **output** per salvare tutto in un file output.

Possiamo notare che in assenza di firewall, nmap ha notato 3 porte aperte e buone informazioni sull'**OS**.

In contemporanea ho lasciato **Wireshark** attivo a sniffare il traffico:

No.	Time	Source	Destination	Protocol	Length	Info
2063	1.151317062	192.168.240.100	192.168.240.150	TCP	74	57202 → 3546 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2064	1.151341929	192.168.240.100	192.168.240.150	TCP	74	54046 → 3809 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2065	1.151355900	192.168.240.100	192.168.240.150	TCP	74	56368 → 49999 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2066	1.151369748	192.168.240.100	192.168.240.150	TCP	74	55974 → 5906 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2067	1.151381959	192.168.240.100	192.168.240.150	TCP	74	37296 → 783 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2068	1.151405770	192.168.240.100	192.168.240.150	TCP	74	51200 → 6580 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2069	1.151440380	192.168.240.100	192.168.240.150	TCP	74	42084 → 427 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2070	1.151450434	192.168.240.150	192.168.240.100	TCP	60	5226 → 34798 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2071	1.151450545	192.168.240.150	192.168.240.100	TCP	60	32783 → 55546 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2072	1.151507828	192.168.240.150	192.168.240.100	TCP	60	3546 → 57202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2073	1.151507887	192.168.240.150	192.168.240.100	TCP	60	3809 → 54046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2074	1.151507913	192.168.240.150	192.168.240.100	TCP	60	49999 → 56368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2075	1.151507941	192.168.240.150	192.168.240.100	TCP	60	5906 → 55974 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2076	1.151507970	192.168.240.150	192.168.240.100	TCP	60	783 → 37296 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2077	1.151507999	192.168.240.150	192.168.240.100	TCP	60	6580 → 51200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2078	1.151508027	192.168.240.150	192.168.240.100	TCP	60	427 → 42084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2079	1.151539785	192.168.240.100	192.168.240.150	TCP	74	49574 → 1594 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2080	1.151565858	192.168.240.100	192.168.240.150	TCP	74	39388 → 5100 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2081	1.151582634	192.168.240.100	192.168.240.150	TCP	74	60888 → 5959 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2082	1.151600216	192.168.240.100	192.168.240.150	TCP	74	57060 → 44442 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2083	1.151621283	192.168.240.100	192.168.240.150	TCP	74	45398 → 3268 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2084	1.151626318	192.168.240.150	192.168.240.100	TCP	60	1594 → 49574 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2085	1.151626390	192.168.240.150	192.168.240.100	TCP	60	5100 → 39388 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2086	1.151626413	192.168.240.150	192.168.240.100	TCP	60	5959 → 60888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2087	1.151635732	192.168.240.100	192.168.240.150	TCP	74	44378 → 1183 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2088	1.151647319	192.168.240.100	192.168.240.150	TCP	74	36684 → 9010 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453606 TSecr=0 WS=128
2089	1.151758176	192.168.240.150	192.168.240.100	TCP	60	44442 → 57060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2090	1.151758261	192.168.240.150	192.168.240.100	TCP	60	3268 → 45398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2091	1.151758286	192.168.240.150	192.168.240.100	TCP	60	1183 → 44378 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2092	1.151758310	192.168.240.150	192.168.240.100	TCP	60	9010 → 36684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2093	1.231908214	192.168.240.100	192.168.240.150	TCP	74	35280 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453687 TSecr=0 WS=128
2094	1.231852031	192.168.240.100	192.168.240.150	TCP	74	38794 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453687 TSecr=0 WS=128
2095	1.231866780	192.168.240.100	192.168.240.150	TCP	74	36252 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929453687 TSecr=0 WS=128

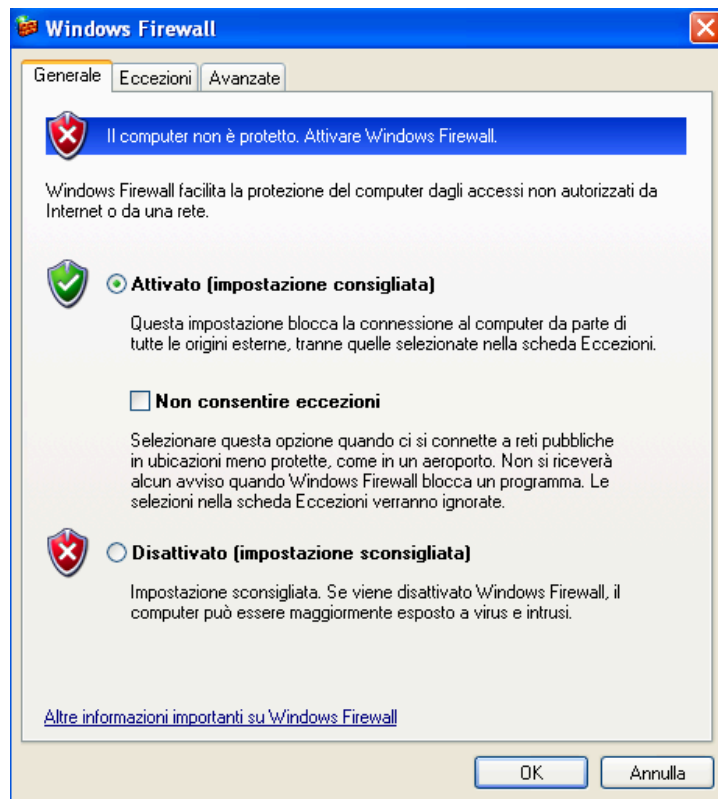
No.	Time	Source	Destination	Protocol	Length	Info
2102	7.247932334	192.168.240.100	192.168.240.150	TCP	98	35280 → 135 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=32 TSval=3929459703 TSecr=0
2103	7.248084071	192.168.240.100	192.168.240.150	NBSS	84	NBSS Continuation Message
2104	7.24829161	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2105	7.248961564	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2106	7.249460396	192.168.240.150	192.168.240.100	TCP	66	135 → 35280 [FIN, ACK] Seq=1 Ack=33 Win=64208 Len=0 TSval=25708 TSecr=3929459703
2107	7.249460642	192.168.240.150	192.168.240.100	SMB	187	Negotiate Protocol Response
2108	7.249498395	192.168.240.100	192.168.240.150	TCP	66	36252 → 445 [ACK] Seq=169 Ack=122 Win=32128 Len=0 TSval=3929459704 TSecr=25708
2109	7.258238161	192.168.240.100	192.168.240.150	TCP	66	35280 → 135 [ACK] Seq=33 Ack=2 Win=32128 Len=0 TSval=3929459713 TSecr=25708
2110	7.295762668	192.168.240.100	192.168.240.150	TCP	66	38794 → 139 [ACK] Seq=19 Ack=7 Win=32128 Len=0 TSval=3929459750 TSecr=25708
2111	7.321331344	192.168.240.100	192.168.240.150	TCP	66	35280 → 135 [FIN, ACK] Seq=33 Ack=2 Win=32128 Len=0 TSval=3929459776 TSecr=25708
2112	7.321393013	192.168.240.100	192.168.240.150	TCP	74	37914 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929459776 TSecr=0 WS=128
2113	7.321472978	192.168.240.100	192.168.240.150	TCP	66	36252 → 445 [FIN, ACK] Seq=169 Ack=122 Win=32128 Len=0 TSval=3929459776 TSecr=25708
2114	7.321495471	192.168.240.100	192.168.240.150	TCP	66	38794 → 139 [FIN, ACK] Seq=19 Ack=7 Win=32128 Len=0 TSval=3929459776 TSecr=25708
2115	7.321514161	192.168.240.100	192.168.240.150	TCP	74	35186 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929459776 TSecr=0 WS=128
2116	7.321788905	192.168.240.150	192.168.240.100	TCP	66	135 → 35280 [ACK] Seq=2 Ack=34 Win=64208 Len=0 TSval=25709 TSecr=3929459776
2117	7.321789075	192.168.240.150	192.168.240.100	TCP	78	135 → 37914 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2118	7.321789105	192.168.240.150	192.168.240.100	TCP	66	139 → 38794 [ACK] Seq=7 Ack=20 Win=64222 Len=0 TSval=25709 TSecr=3929459776
2119	7.321789127	192.168.240.150	192.168.240.100	TCP	78	139 → 35186 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2120	7.321789152	192.168.240.150	192.168.240.100	TCP	66	445 → 36252 [FIN, ACK] Seq=122 Ack=170 Win=64072 Len=0 TSval=25709 TSecr=3929459776
2121	7.321817732	192.168.240.100	192.168.240.150	TCP	66	37914 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929459777 TSecr=0
2122	7.321828507	192.168.240.100	192.168.240.150	TCP	66	35186 → 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929459777 TSecr=0
2123	7.321834511	192.168.240.100	192.168.240.150	TCP	66	36252 → 445 [ACK] Seq=170 Ack=123 Win=32128 Len=0 TSval=3929459777 TSecr=25709
2124	7.321879646	192.168.240.100	192.168.240.150	TCP	234	37914 → 135 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=168 TSval=3929459777 TSecr=0
2125	7.321944328	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2126	7.322159976	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2127	7.322305089	192.168.240.100	192.168.240.150	TCP	66	35186 → 139 [FIN, ACK] Seq=169 Ack=7 Win=32128 Len=0 TSval=3929459777 TSecr=25709
2128	7.322303459	192.168.240.150	192.168.240.100	DCERPC	90	Bind nak: call_id: 1073809408, Fragment: Single reason: Protocol version not supported
2129	7.322303553	192.168.240.150	192.168.240.100	TCP	66	135 → 37914 [FIN, ACK] Seq=25 Ack=169 Win=64072 Len=0 TSval=25709 TSecr=3929459777
2130	7.322405465	192.168.240.100	192.168.240.150	TCP	66	37914 → 135 [ACK] Seq=169 Ack=25 Win=32128 Len=0 TSval=3929459777 TSecr=25709
2131	7.322479883	192.168.240.100	192.168.240.150	TCP	66	37914 → 135 [FIN, ACK] Seq=169 Ack=26 Win=32128 Len=0 TSval=3929459777 TSecr=25709
2132	7.322544324	192.168.240.150	192.168.240.100	TCP	66	139 → 35186 [ACK] Seq=7 Ack=170 Win=64072 Len=0 TSval=25709 TSecr=3929459777
2133	7.322785922	192.168.240.150	192.168.240.100	TCP	66	135 → 37914 [ACK] Seq=26 Ack=170 Win=64072 Len=0 TSval=25709 TSecr=3929459777

Possiamo notare che ci sono principalmente 3 tipi risposte alle domande **TCP [SYN]** (Synchronize):

1. **Risposta vuota;** la mancata risposta puo' avvenire per vari motivi, per la perdita del pacchetto, per la chiusura della porta, per un errore di connessione, oppure i sistemi possono essere configurati in modo tale da non destare segnali.
2. **Risposta rifiutata [RST, ACK];** questo implica che la macchina vittima ha ricevuto il pacchetto di richiesta ma non essendoci un servizio attivo in ascolto sulla determinata porta, rifiuta la connessione (rammentiamo che **[RST, ACK]** sta per Reset Acknowledgment).
3. **Risposta accettata [ACK];** in questo caso se la richiesta viene accettata, allora significa che abbiamo ricevuto un pacchetto **[ACK]** dal servizio attivo, questo implica che la porta e aperta.

Scansione in presenza del firewall

Attiviamo il firewall di WindowsXP:



Mandiamo nuovamente la scansione tramite **nmap**:

```
(kali㉿kali)-[~]
$ nmap -sV -o dati.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:01 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 3.14 seconds

(kali㉿kali)-[~]
$ nmap -Pn -sV -o dati.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:02 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
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 11.50 seconds
```

Possiamo notare che con la stessa scansione, **nmap** non trova nessun host. Questo perché la strutturazione di **nmap** è fatta in modo tale da mandare una scansione solo dopo avere ottenuto dei pacchetti **ICMP** (Internet Control Message Protocol) o chiamata anche richiesta ping, ma dato che il firewall di Windows è configurato per ignorare le richieste **ICMP**, giustamente **nmap** non manda la scansione.

Per risolvere questo problema, bisogna aggiungere un sotto comando di **nmap**, il **-Pn** che permette di avviare la scansione senza controllare i pacchetti **ICMP**.

Infatti possiamo notare che in questo modo ha trovato l'host, seppur con servizi in meno.

Osserviamo ora i due casi con **Wireshark**:

Capturing from eth1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.240.100	192.168.240.150	TCP	74	42746 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929745529 TSecr=0 WS=128
2	0.000037749	192.168.240.100	192.168.240.150	TCP	74	45132 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929745529 TSecr=0 WS=128
3	2.001717696	192.168.240.100	192.168.240.150	TCP	74	57214 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929747531 TSecr=0 WS=128
4	2.001882604	192.168.240.100	192.168.240.150	TCP	74	54948 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929747531 TSecr=0 WS=128
5	3.036947592	192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 54948 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929748566 TSecr=0 WS=128
6	3.037116854	192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 57214 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929748567 TSecr=0 WS=128
7	5.168717478	PCSSystemtec_e6:d5::...	PCSSystemtec_5c:8d::...	ARP	42	Who has 192.168.240.150? Tell 192.168.240.100
8	5.169384342	PCSSystemtec_5c:8d::...	PCSSystemtec_e6:d5::...	ARP	60	192.168.240.150 is at 08:09:27:5c:8d:1c

eth1: <live capture in progress> Packets: 8 · Displayed: 8 (100.0%) Profile: Default

Capturing from eth1

No.	Time	Source	Destination	Protocol	Length	Info
2008	5.074681734	192.168.240.100	192.168.240.150	TCP	74	56568 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851541 TSecr=0 WS=128
2009	5.074706642	192.168.240.100	192.168.240.150	TCP	74	58310 → 254 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851541 TSecr=0 WS=128
2010	5.074731543	192.168.240.100	192.168.240.150	TCP	74	35756 → 911 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851541 TSecr=0 WS=128
2011	5.074751777	192.168.240.100	192.168.240.150	TCP	74	33950 → 4445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851541 TSecr=0 WS=128
2012	5.074778560	192.168.240.100	192.168.240.150	TCP	74	55274 → 3052 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851541 TSecr=0 WS=128
2013	5.210015621	192.168.240.100	192.168.240.150	TCP	74	56080 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851676 TSecr=0 WS=128
2014	5.211171853	192.168.240.100	192.168.240.150	TCP	78	445 → 56080 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2015	5.211236141	192.168.240.100	192.168.240.150	TCP	66	56080 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929851677 TSecr=0
2016	5.211525382	192.168.240.100	192.168.240.150	TCP	66	56080 → 445 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929851678 TSecr=0
2017	5.308160142	192.168.240.100	192.168.240.150	TCP	74	37492 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851774 TSecr=0 WS=128
2018	5.308184456	192.168.240.100	192.168.240.150	TCP	74	56094 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929851774 TSecr=0 WS=128
2019	5.308511005	192.168.240.100	192.168.240.150	TCP	78	139 → 37492 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2020	5.308511196	192.168.240.100	192.168.240.150	TCP	78	445 → 56094 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2021	5.308546520	192.168.240.100	192.168.240.150	TCP	66	37492 → 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929851775 TSecr=0
2022	5.308557028	192.168.240.100	192.168.240.150	TCP	66	56094 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929851775 TSecr=0
2023	11.349737245	192.168.240.100	192.168.240.150	NBSS	84	NBSS Continuation Message
2024	11.349840005	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2025	11.350979449	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2026	11.350979806	192.168.240.150	192.168.240.100	SMB	187	Negotiate Protocol Response
2027	11.351063282	192.168.240.100	192.168.240.150	TCP	66	56094 → 445 [ACK] Seq=169 Ack=122 Win=32128 Len=0 TSval=3929857817 TSecr=29686
2028	11.381199470	192.168.240.100	192.168.240.150	TCP	66	56094 → 445 [FIN, ACK] Seq=169 Ack=122 Win=32128 Len=0 TSval=3929857847 TSecr=29686
2029	11.381290216	192.168.240.100	192.168.240.150	TCP	66	37492 → 139 [FIN, ACK] Seq=19 Ack=7 Win=32128 Len=0 TSval=3929857847 TSecr=29686
2030	11.381394895	192.168.240.100	192.168.240.150	TCP	74	38968 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3929857848 TSecr=0 WS=128
2031	11.381796953	192.168.240.150	192.168.240.100	TCP	66	139 → 37492 [ACK] Seq=7 Ack=20 Win=64222 Len=0 TSval=29687 TSecr=3929857847
2032	11.381797117	192.168.240.150	192.168.240.100	TCP	78	139 → 38968 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2033	11.381797170	192.168.240.150	192.168.240.100	TCP	66	445 → 56094 [FIN, ACK] Seq=122 Ack=170 Win=64072 Len=0 TSval=29687 TSecr=3929857847
2034	11.381840708	192.168.240.100	192.168.240.150	TCP	66	38968 → 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3929857848 TSecr=0
2035	11.381859261	192.168.240.100	192.168.240.150	TCP	66	56094 → 445 [ACK] Seq=170 Ack=123 Win=32128 Len=0 TSval=3929857848 TSecr=29687
2036	11.381916668	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2037	11.382322481	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2038	11.382521571	192.168.240.100	192.168.240.150	TCP	66	38968 → 139 [FIN, ACK] Seq=169 Ack=7 Win=32128 Len=0 TSval=3929857849 TSecr=29687
2039	11.383017561	192.168.240.150	192.168.240.100	TCP	66	139 → 38968 [ACK] Seq=7 Ack=170 Win=64072 Len=0 TSval=29687 TSecr=3929857849

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
eth1: <live capture in progress> Packets: 2039 · Displayed: 2039 (100.0%) Profile: Default

Notiamo nel primo caso che **wireshark** riceve pochissimi pacchetti proprio dovuto al fatto che **nmap** non ha trovato l'host, mentre nel secondo caso, possiamo notare invece la quantita' di pacchetti e quasi tutti contenenti richieste ignorate.

In particolare abbiamo ottenuto poche risposte **[ACK]**, pochissime **[RST, ACK]**, e tante 'non risposte', cioe' lasciate richieste **[SYN]**.

Questo in realta' ha senso, perche' dimostra che il firewall ha il compito di ignorare quante piu' possibili risposte per lasciare il dubbio all'attaccante.

Conclusione:

Questo breve esercizio dimostra che la presenza di un firewall, può fare la differenza in ambito sicurezza.

Lasciare sistemi in balia di possibili attacchi, non ha alcun senso a meno che non lo si fa per uso didattico, perciò consiglio di mantenere sempre attivi i firewall di sistema e mantenerli aggiornati.