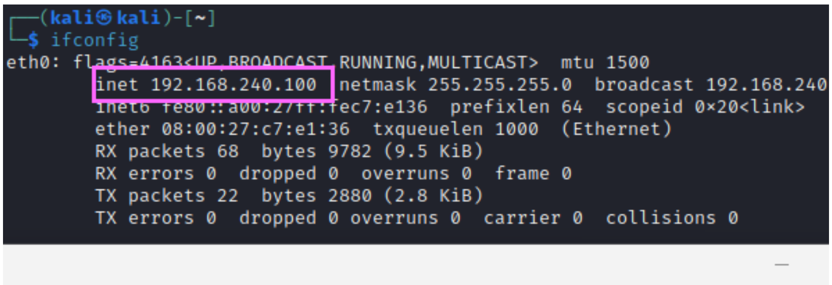
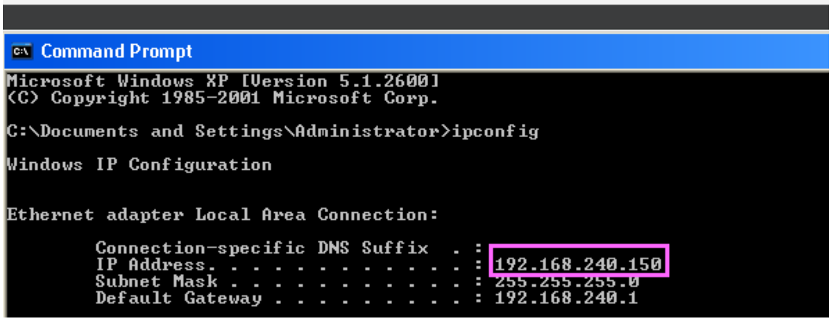
Report UNIT 3 WEEK 9

Azioni preventive

Impostazione indirizzi IP macchina Kali e Windows XP su rete interna.



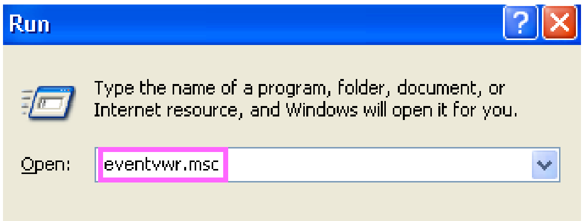
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240
        inet6 fe80::a00:27ff:fec7:e136  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 68  bytes 9782 (9.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2880 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



Command Prompt

```
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 . . . . . . . . . : 192.168.240.1
```

Con il tasto windows+R vado ad aprire l’event manager digitando “**eventvwr.msc**”.



Run

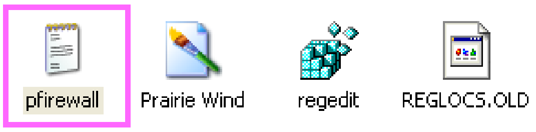
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

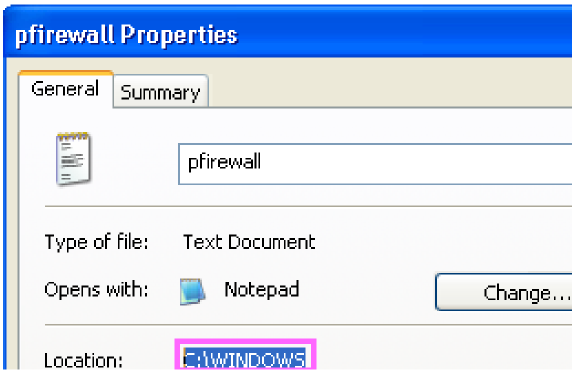
Open: eventvwr.msc

Su Windows XP, per visualizzare i log del firewall è necessario utilizzare un file di log specifico chiamato **PFirewall.log**. A differenza delle versioni più recenti di Windows, il firewall integrato di Windows XP (Windows Firewall) non registra gli eventi direttamente nell'Event Viewer.

Per abilitare la registrazione degli eventi del firewall su Windows XP, è possibile utilizzare PFirewall. Questo file registra le attività del firewall, inclusi i blocchi e i consensi delle connessioni in ingresso e in uscita.

Per accedere ai log del firewall, è possibile trovare il file PFirewall.log nella directory C:\WINDOWS





pfirewall Properties

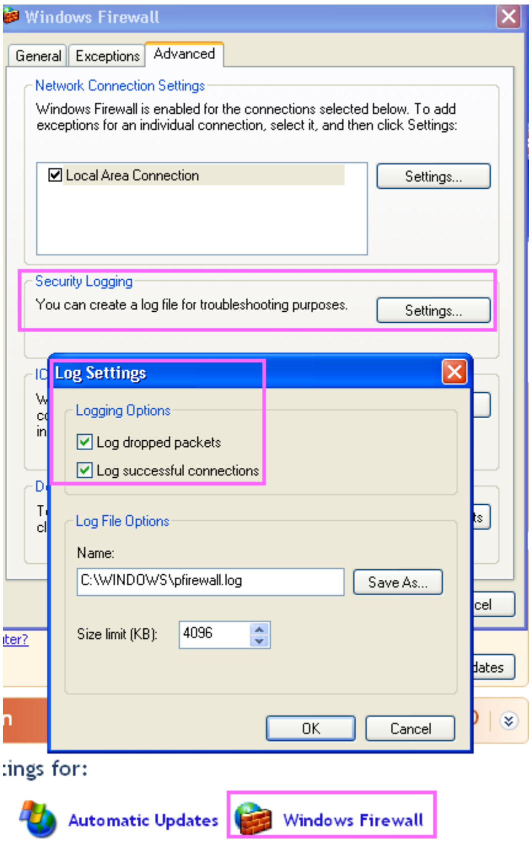
pfirewall

Type of file: Text Document

Opens with: Notepad

Location: C:\WINDOWS

Per abilitarlo è possibile selezionare Windows Firewall, Security Logging Settings e spuntare le opzioni per i log.



Network Connection Settings

Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:

☑ Local Area Connection

Security Logging

You can create a log file for troubleshooting purposes.

Logging Options

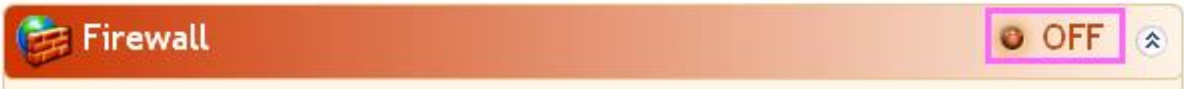
☑ Log dropped packets

☑ Log successful connections

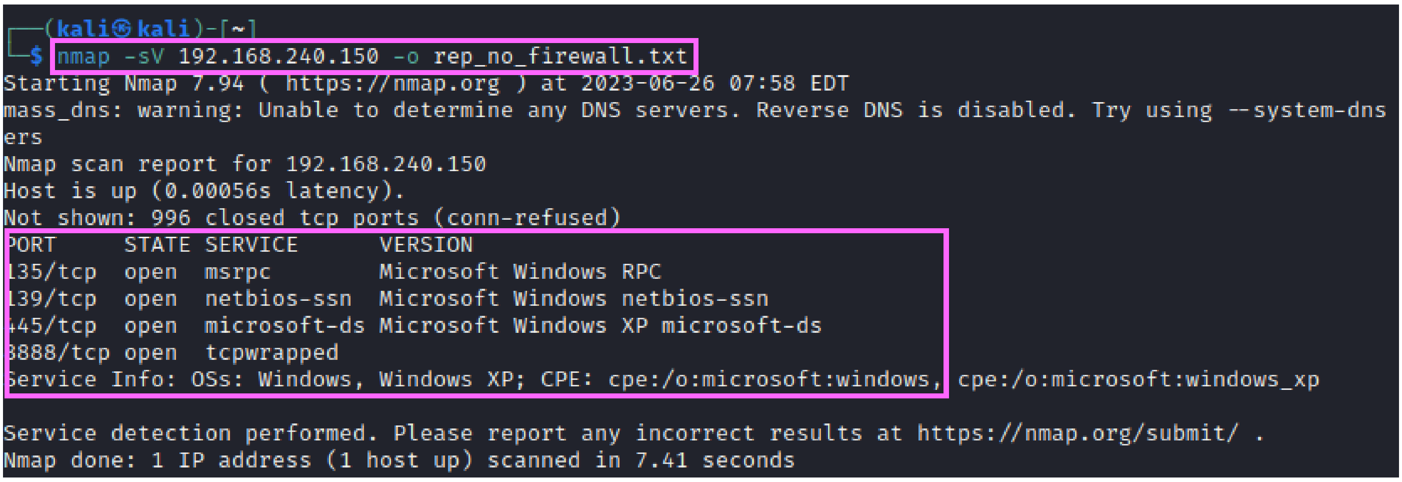
Log File Options

Name: C:\WINDOWS\pfirewall.log

Size limit (KB): 4096

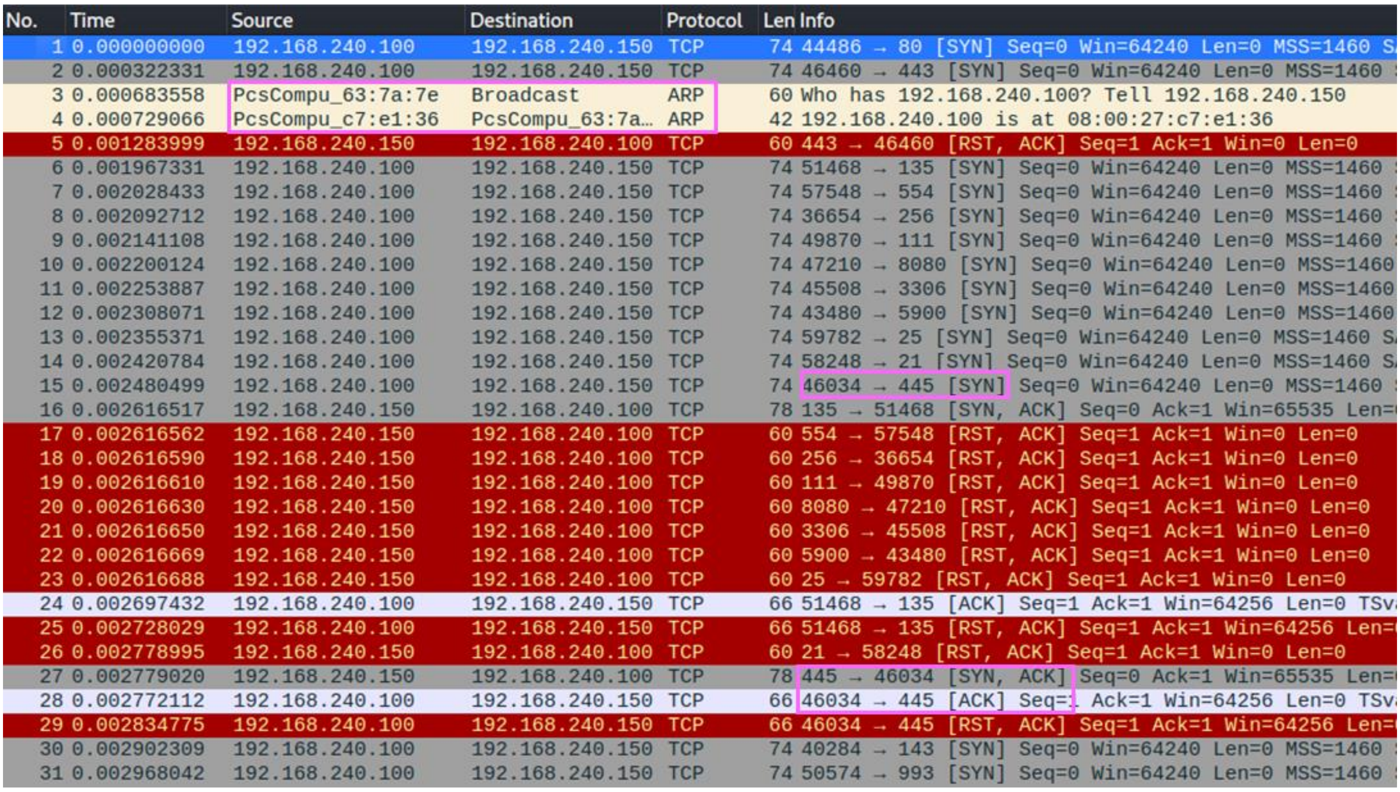


Faccio una scansione nmap da kali salvando il report in un file, intercettando con wireshark.



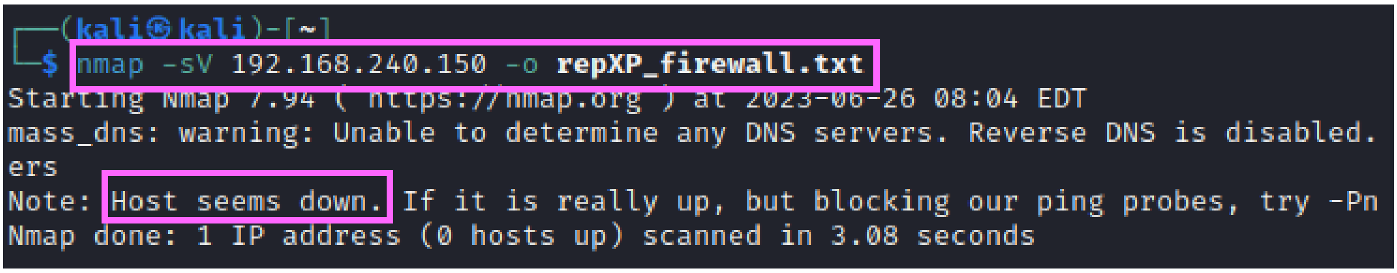
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o rep_no_firewall.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-26 07:58 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
ers
Nmap scan report for 192.168.240.150
Host is up (0.00056s 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
3888/tcp open  tcpwrapped
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 7.41 seconds
```

In questo caso abbiamo eseguito **nmap -sV**, per cui possiamo vedere come nmap invii pacchetti **SYN** alle porte di XP per determinarne lo stato (aperto, chiuso o filtrato) e tentare di identificare la versione dei servizi in esecuzione sulle porte. Se la porta è **aperta**, XP risponderà con **SYN-ACK**. Se la porta è **chiusa**, XP risponderà con **RST**, mentre se la porta è filtrata, XP potrebbe non inviare alcuna risposta.



```
No. Time        Source               Destination          Protocol Len Info
  1 0.000000000 192.168.240.100      192.168.240.150      TCP      74 44486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
  2 0.000322331 192.168.240.100      192.168.240.150      TCP      74 46460 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  3 0.000683558 PcsCompu_63:7a:7e    Broadcast            ARP      60 Who has 192.168.240.100? Tell 192.168.240.150
  4 0.000729066 PcsCompu_c7:e1:36    PcsCompu_63:7a…      ARP      42 192.168.240.100 is at 08:00:27:c7:e1:36
  5 0.001283999 192.168.240.150      192.168.240.100      TCP      60 443 → 46460 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  6 0.001967331 192.168.240.100      192.168.240.150      TCP      74 51468 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  7 0.002028433 192.168.240.100      192.168.240.150      TCP      74 57548 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  8 0.002092712 192.168.240.100      192.168.240.150      TCP      74 36654 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  9 0.002141108 192.168.240.100      192.168.240.150      TCP      74 49870 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 10 0.002200124 192.168.240.100      192.168.240.150      TCP      74 47210 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 11 0.002253887 192.168.240.100      192.168.240.150      TCP      74 45508 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 12 0.002308071 192.168.240.100      192.168.240.150      TCP      74 43480 → 5900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 13 0.002355371 192.168.240.100      192.168.240.150      TCP      74 59782 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
 14 0.002420784 192.168.240.100      192.168.240.150      TCP      74 58248 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
 15 0.002480499 192.168.240.100      192.168.240.150      TCP      74 46034 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 16 0.002616517 192.168.240.150      192.168.240.100      TCP      78 135 → 51468 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
 17 0.002616562 192.168.240.150      192.168.240.100      TCP      60 554 → 57548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 18 0.002616590 192.168.240.150      192.168.240.100      TCP      60 256 → 36654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 19 0.002616610 192.168.240.150      192.168.240.100      TCP      60 111 → 49870 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 20 0.002616630 192.168.240.150      192.168.240.100      TCP      60 8080 → 47210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 21 0.002616650 192.168.240.150      192.168.240.100      TCP      60 3306 → 45508 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 22 0.002616669 192.168.240.150      192.168.240.100      TCP      60 5900 → 43480 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 23 0.002616688 192.168.240.150      192.168.240.100      TCP      60 25 → 59782 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 24 0.002697432 192.168.240.100      192.168.240.150      TCP      66 51468 → 135 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
 25 0.002728029 192.168.240.100      192.168.240.150      TCP      66 51468 → 135 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=
 26 0.002778995 192.168.240.150      192.168.240.100      TCP      60 21 → 58248 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 27 0.002779020 192.168.240.150      192.168.240.100      TCP      78 445 → 46034 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
 28 0.002772112 192.168.240.100      192.168.240.150      TCP      66 46034 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
 29 0.002834775 192.168.240.100      192.168.240.150      TCP      66 46034 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=
 30 0.002902309 192.168.240.100      192.168.240.150      TCP      74 40284 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 31 0.002968042 192.168.240.100      192.168.240.150      TCP      74 50574 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
```

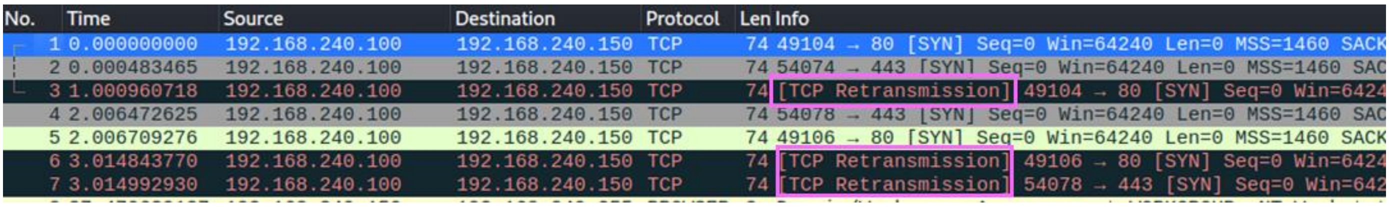
Ripeto la scansione attivando il firewall su windows XP ed intercettando nuovamente con wireshark e pfirewall.



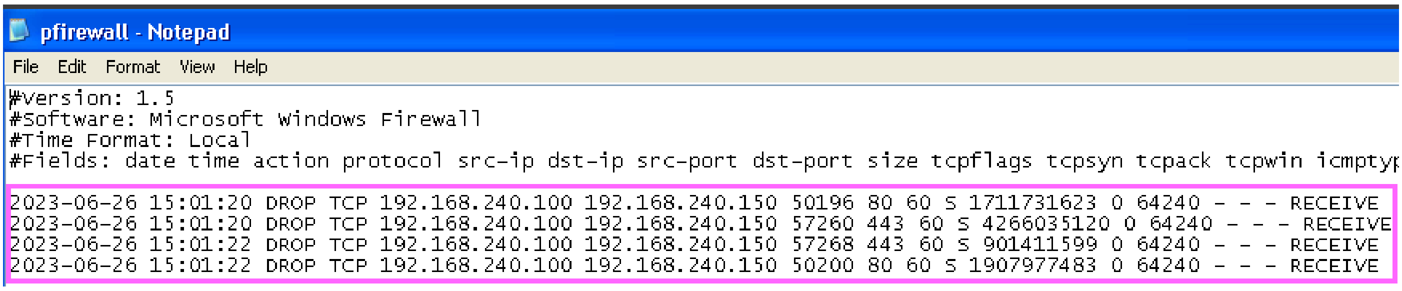
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o repXP_firewall.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-26 08:04 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
ers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds
```

In questo caso XP blocca i pacchetti SYN inviati da Kali, nmap interpreta la mancanza di risposta come se l'host fosse down. Con **TCP Retransmission** possiamo notare come Kali stia tentando di rieffettuare la connessione ed inviare nuovamente i pacchetti SYN, ma senza successo a causa delle politiche del firewall di XP.

Su pfirewall invece possiamo notare come sia visibile **DROP TCP --- RECEIVE**, ovvero il firewall sta bloccando i pacchetti inviati da Kali durante la scansione.

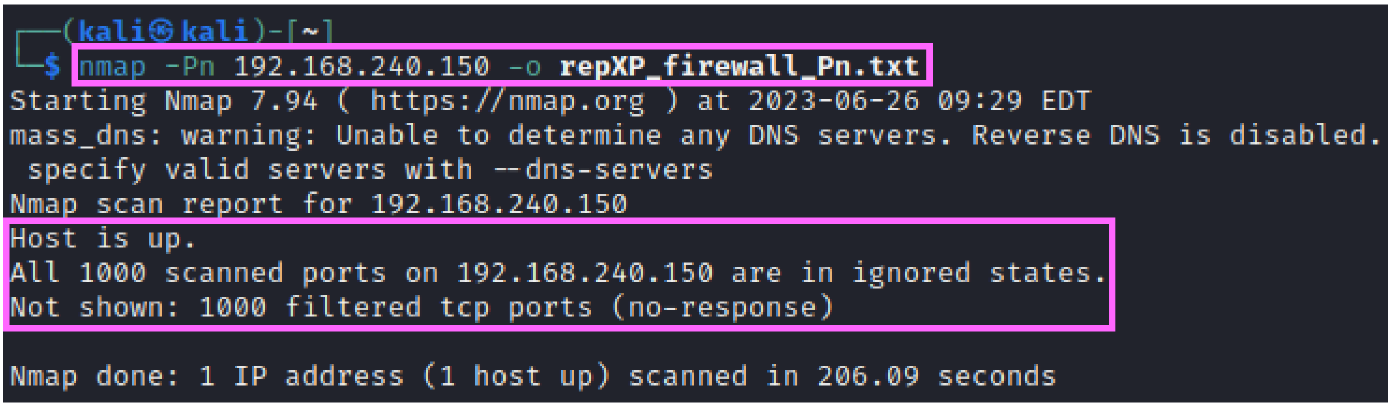


```
No. Time        Source               Destination          Protocol Len Info
  1 0.000000000 192.168.240.100      192.168.240.150      TCP      74 49104 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
  2 0.000483465 192.168.240.100      192.168.240.150      TCP      74 54074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
  3 1.000960718 192.168.240.100      192.168.240.150      TCP      74 [TCP Retransmission] 49104 → 80 [SYN] Seq=0 Win=6424
  4 2.006472625 192.168.240.100      192.168.240.150      TCP      74 54078 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
  5 2.006709276 192.168.240.100      192.168.240.150      TCP      74 49106 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
  6 3.014843770 192.168.240.100      192.168.240.150      TCP      74 [TCP Retransmission] 49106 → 80 [SYN] Seq=0 Win=6424
  7 3.014992930 192.168.240.100      192.168.240.150      TCP      74 [TCP Retransmission] 54078 → 443 [SYN] Seq=0 Win=642
```



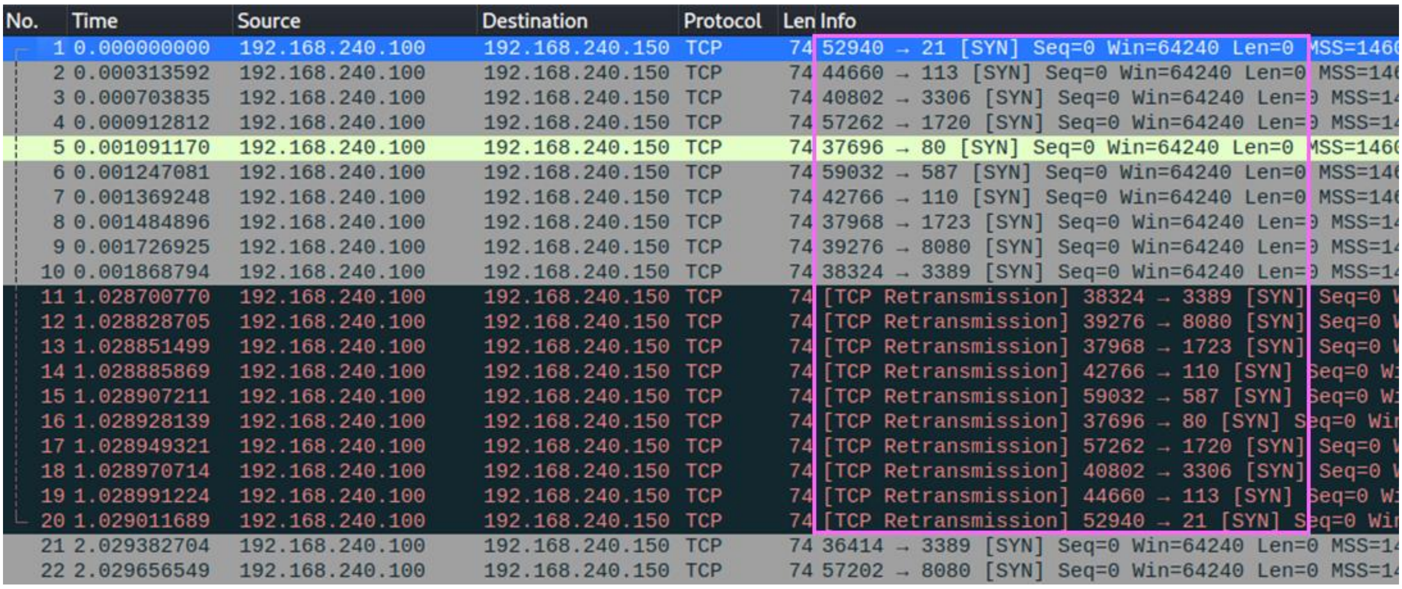
```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptyp

2023-06-26 15:01:20 DROP TCP 192.168.240.100 192.168.240.150 50196 80 60 S 1711731623 0 64240 - - - RECEIVE
2023-06-26 15:01:20 DROP TCP 192.168.240.100 192.168.240.150 57260 443 60 S 4266035120 0 64240 - - - RECEIVE
2023-06-26 15:01:22 DROP TCP 192.168.240.100 192.168.240.150 57268 443 60 S 901411599 0 64240 - - - RECEIVE
2023-06-26 15:01:22 DROP TCP 192.168.240.100 192.168.240.150 50200 80 60 S 1907977483 0 64240 - - - RECEIVE
```

Scansione **-Pn** con firewall on, wireshark e pfirewall.

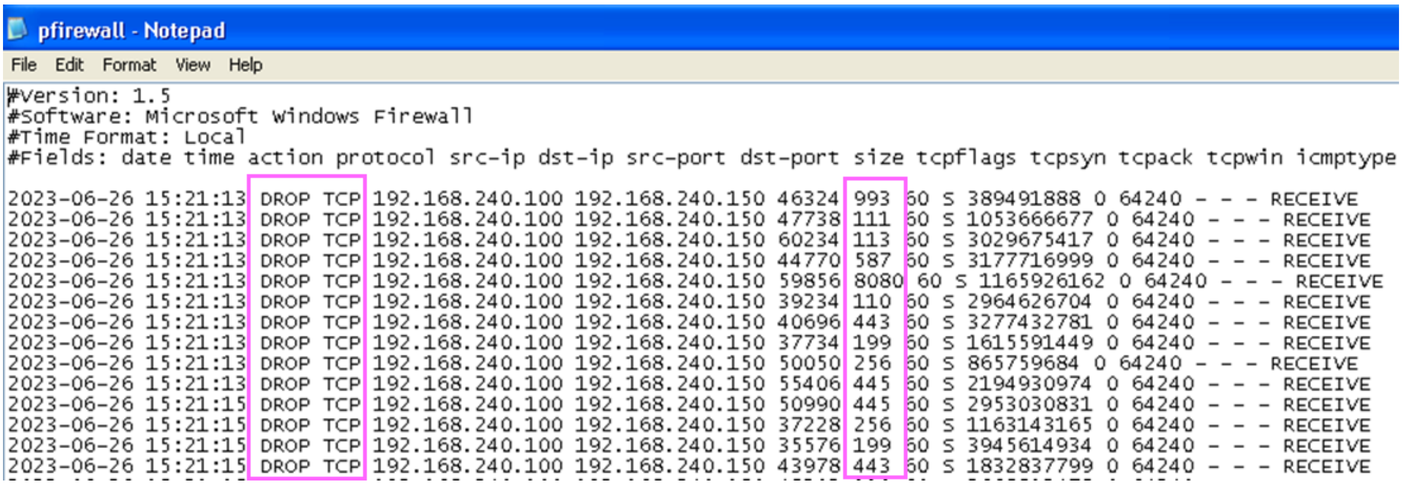


```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.240.150 -o repXP_firewall_Pn.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-26 09:29 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 specify valid servers with --dns-servers
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 206.09 seconds
```

Questa volta la scansione -Pn considera XP attivo senza fare affidamento sulla risposta al ping, saltando la fase preliminare di host discovery. Anche in questo caso Kali continua ad inviare pacchetti SYN senza successo, dal momento che il firewall di XP li blocca.



```
No. Time        Source          Destination     Protocol Len Info
  1 0.000000000 192.168.240.100 192.168.240.150 TCP       74 52940 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  2 0.000313592 192.168.240.100 192.168.240.150 TCP       74 44660 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=146
  3 0.000703835 192.168.240.100 192.168.240.150 TCP       74 40802 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=14
  4 0.000912812 192.168.240.100 192.168.240.150 TCP       74 57262 → 1720 [SYN] Seq=0 Win=64240 Len=0 MSS=14
  5 0.001091170 192.168.240.100 192.168.240.150 TCP       74 37696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  6 0.001247081 192.168.240.100 192.168.240.150 TCP       74 59032 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=146
  7 0.001369248 192.168.240.100 192.168.240.150 TCP       74 42766 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=146
  8 0.001484896 192.168.240.100 192.168.240.150 TCP       74 37968 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=14
  9 0.001726925 192.168.240.100 192.168.240.150 TCP       74 39276 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=14
 10 0.001868794 192.168.240.100 192.168.240.150 TCP       74 38324 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=14
 11 1.028700770 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 38324 → 3389 [SYN] Seq=0 W
 12 1.028828705 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 39276 → 8080 [SYN] Seq=0 W
 13 1.028851499 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 37968 → 1723 [SYN] Seq=0 W
 14 1.028885869 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 42766 → 110 [SYN] Seq=0 Wi
 15 1.028907211 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 59032 → 587 [SYN] Seq=0 Wi
 16 1.028928139 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 37696 → 80 [SYN] Seq=0 Win
 17 1.028949321 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 57262 → 1720 [SYN] Seq=0 W
 18 1.028970714 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 40802 → 3306 [SYN] Seq=0 W
 19 1.028991224 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 44660 → 113 [SYN] Seq=0 Wi
 20 1.029011689 192.168.240.100 192.168.240.150 TCP       74 [TCP Retransmission] 52940 → 21 [SYN] Seq=0 Win
 21 2.029382704 192.168.240.100 192.168.240.150 TCP       74 36414 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=14
 22 2.029656549 192.168.240.100 192.168.240.150 TCP       74 57202 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=14
```



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype

2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 46324 993 60 S 389491888 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 47738 111 60 S 1053666677 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 60234 113 60 S 3029675417 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 44770 587 60 S 3177716999 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 59856 8080 60 S 1165926162 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 39234 110 60 S 2964626704 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 40696 443 60 S 3277432781 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 37734 199 60 S 1615591449 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 50050 256 60 S 865759684 0 64240 - - - RECEIVE
2023-06-26 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 55406 445 60 S 2194930974 0 64240 - - - RECEIVE
2023-06-26 15:21:15 DROP TCP 192.168.240.100 192.168.240.150 50990 445 60 S 2953030831 0 64240 - - - RECEIVE
2023-06-26 15:21:15 DROP TCP 192.168.240.100 192.168.240.150 37228 256 60 S 1163143165 0 64240 - - - RECEIVE
2023-06-26 15:21:15 DROP TCP 192.168.240.100 192.168.240.150 35576 199 60 S 3945614934 0 64240 - - - RECEIVE
2023-06-26 15:21:15 DROP TCP 192.168.240.100 192.168.240.150 43978 443 60 S 1832837799 0 64240 - - - RECEIVE
```