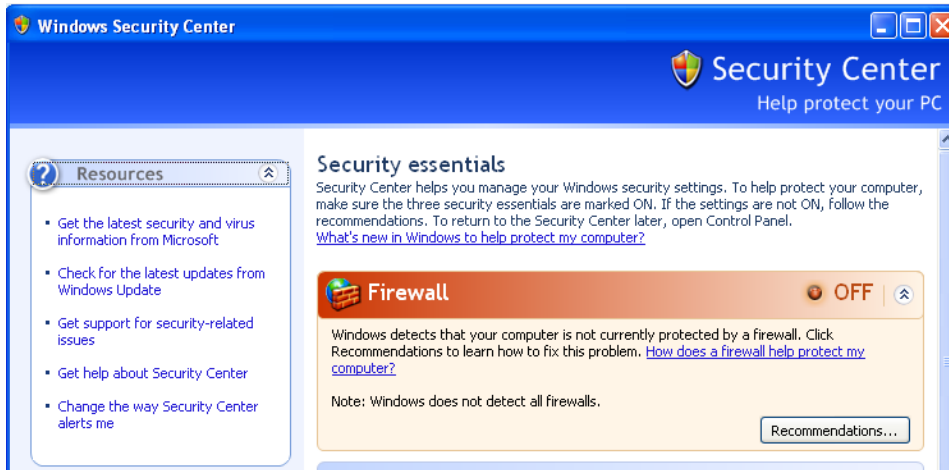
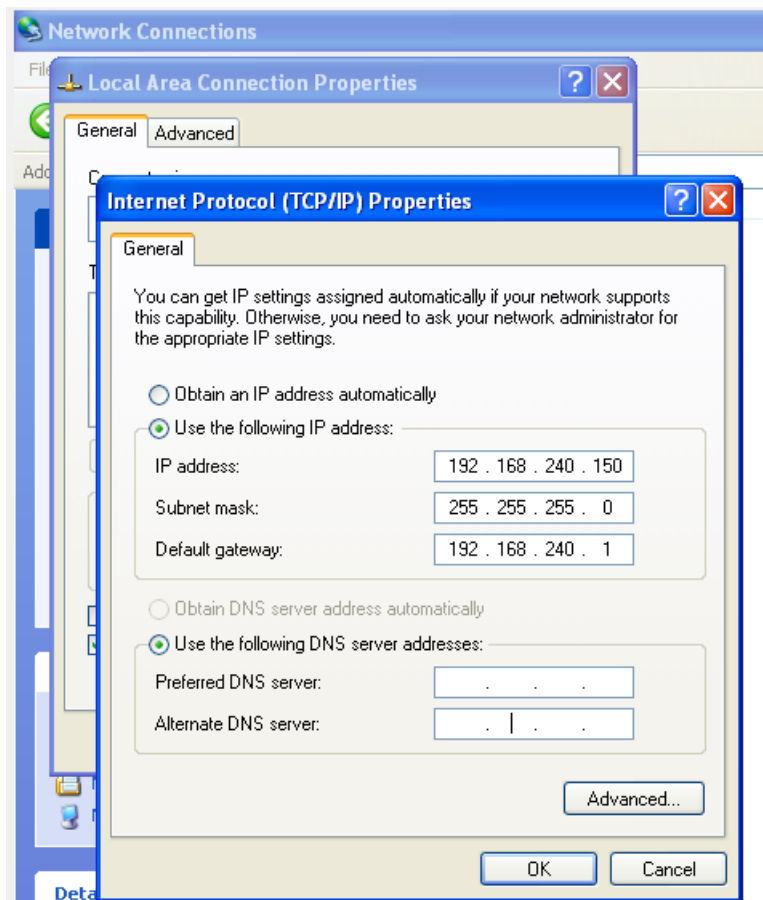


## Security Operations

**Verifica che la macchina virtuale Windows XP abbia il Firewall disabilitato:**



**Configurazione indirizzo IP 192.168.240.150 su Windows XP:**



Verifica con ipconfig:

```
C:\Documents and Settings\A>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

C:\Documents and Settings\A>_
```

### **Configurazione indirizzo IP 192.168.240.100 su Kali Linux:**

```
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
#address 192.168.1.10/24
address 192.168.240.100/24
#gateway 192.168.1.1
```

Restart dei servizi di rete e verifica con ifconfig:

```
(kali㉿kali)-[~]
$ sudo service networking restart

(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:fe53:cba prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:53:0c:ba txqueuelen 1000 (Ethernet)
    RX packets 1153 bytes 80564 (78.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1113 bytes 84080 (82.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Ping da Kali a XP

```
(kali@kali)-[~]
$ ping 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=0.611 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.916 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.683 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.27 ms
^C
— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.611/0.869/1.269/0.256 ms
```

## Ping da XP a Kali

```
Pinging 192.168.240.100 with 32 bytes of data:
Reply from 192.168.240.100: bytes=32 time<1ms TTL=64
Reply from 192.168.240.100: bytes=32 time<1ms TTL=64
Reply from 192.168.240.100: bytes=32 time<1ms TTL=64
Reply from 192.168.240.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.240.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## Scansione con nmap -sV della macchina Windows XP con output nel file xpreportscan.txt

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -o xpreportscan.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 14:49 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00079s 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

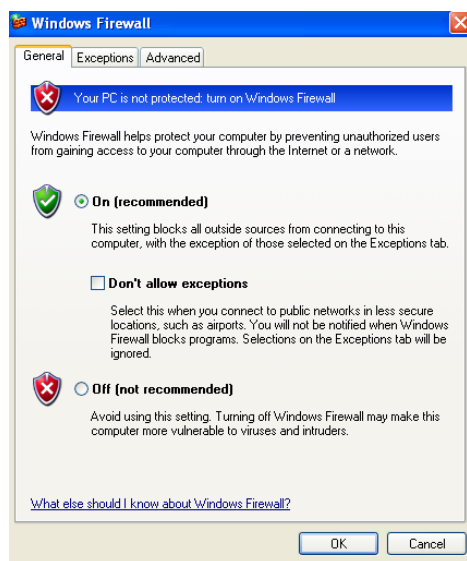
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.64 seconds
```

Visualizzazione del report. Vediamo che lo scan ha restituito le porte aperte e i servizi attivi con relative informazioni:

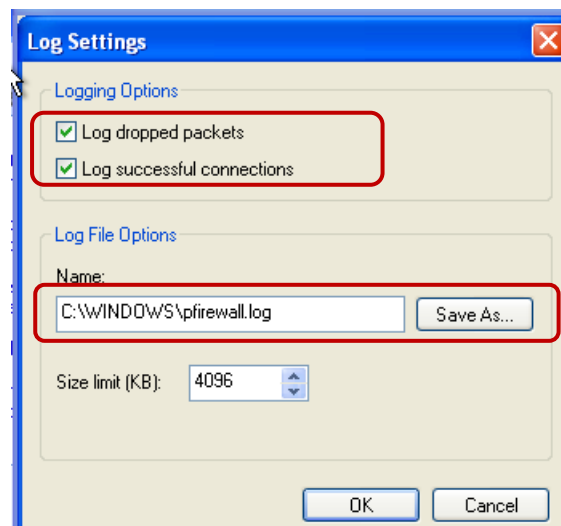
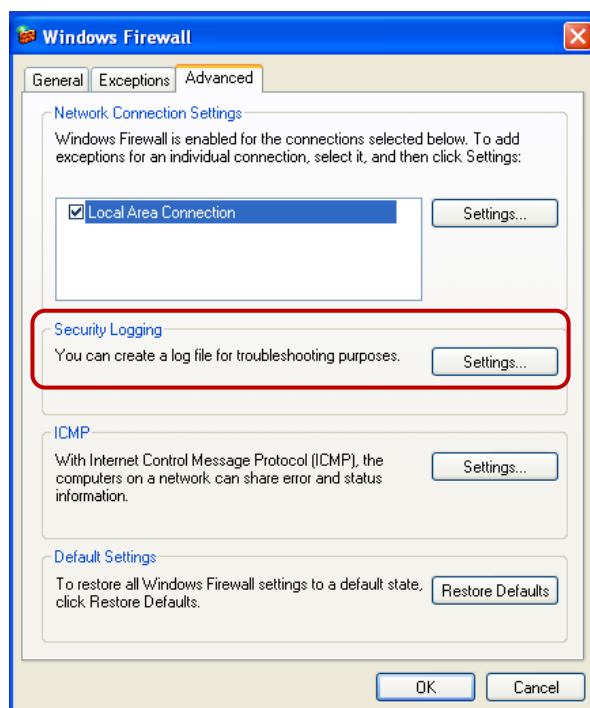
```
(kali@kali)-[~]
$ cat xpreportscan.txt
# Nmap 7.93 scan initiated Tue Oct  3 14:49:36 2023 as: nmap -sV -o xpreportscan.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.00079s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp   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 at Tue Oct  3 14:49:56 2023 -- 1 IP address (1 host up) scanned in 20.64 seconds
```

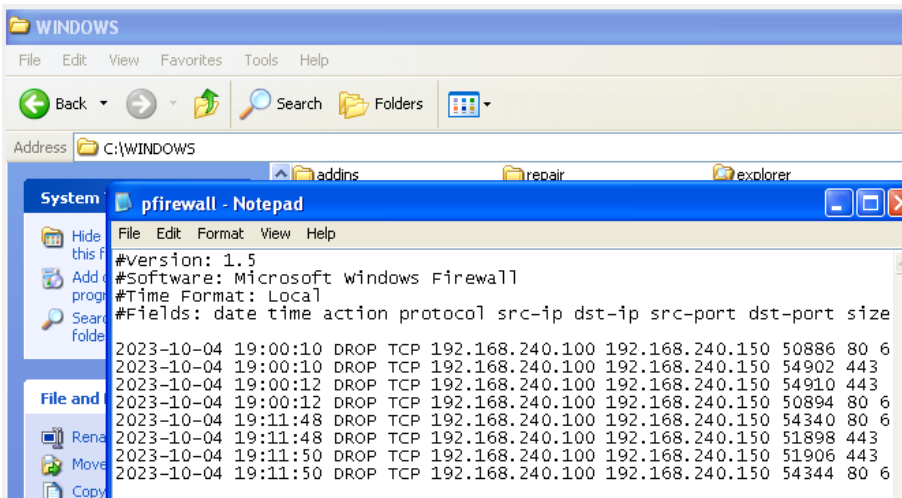
## Abilitazione del Firewall su Windows XP



## Abilitazione dei log del Firewall su Windows XP



Come indicato nella impostazioni di abilitazione del log, i log del Firewall sono salvati nel file `pfirewall.log` nella cartella `C:\WINDOWS`:



**Seconda scansione con `nmap -sV` della macchina Windows XP (con Firewall abilitato) con output nel file `xpreportscan2.txt`**

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -o xpreportscan2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-08 10:09 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 3.15 seconds
```

Visualizzazione del report. Questa volta la scansione indica che l'host sembra down. Le porte aperte e i servizi attivi non sono stati rilevati:

```
(kali@kali)-[~]
$ cat xpreportscan2.txt
# Nmap 7.93 scan initiated Sun Oct  8 10:09:44 2023 as: nmap -sV -o xpreportscan2.txt 192.168.240.150
# Nmap done at Sun Oct  8 10:09:47 2023 -- 1 IP address (0 hosts up) scanned in 3.15 seconds
```

## DIFFERENZE TRA SCANSIONE CON FIREWALL DISABILITATO E FIREWALL ABILITATO:

La scansione 1 ha rilevato le porte TCP 135, 139 e 445 aperte e i relativi servizi in esecuzione. Vediamo il primo report:

```
└─$ cat xpreportscan.txt
# Nmap 7.93 scan initiated Tue Oct  3 14:49:36 2023 as: nmap -sV -o xpreportscan.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.00079s 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

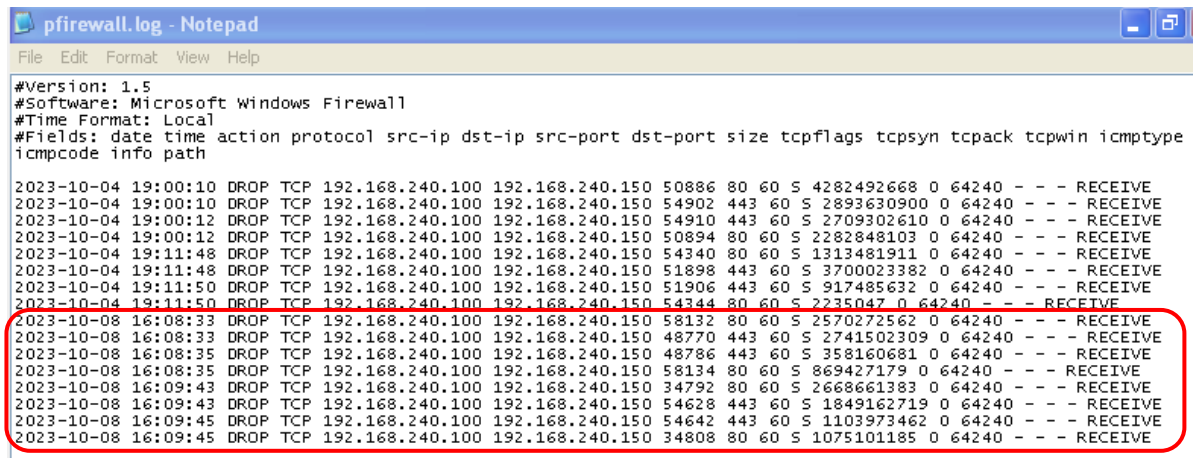
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct  3 14:49:56 2023 -- 1 IP address (1 host up) scanned in 20.64 seconds
```

## La scansione 2 non è riuscita a rilevare l'host. Vediamo il secondo report:

```
└─$ cat xpreportscan2.txt
# Nmap 7.93 scan initiated Sun Oct  8 10:09:44 2023 as: nmap -sV -o xpreportscan2.txt 192.168.240.150
# Nmap done at Sun Oct  8 10:09:47 2023 -- 1 IP address (0 hosts up) scanned in 3.15 seconds
```

Questo significa che il Firewall di Windows XP ha impedito il rilevamento delle porte aperte e servizi sull'host. Vediamo il file di log per maggiori informazioni.

Dal file di log, nella data e ora della scansione risultano in effetti delle richieste ricevute dall'IP di Kali 192.168.240.100.



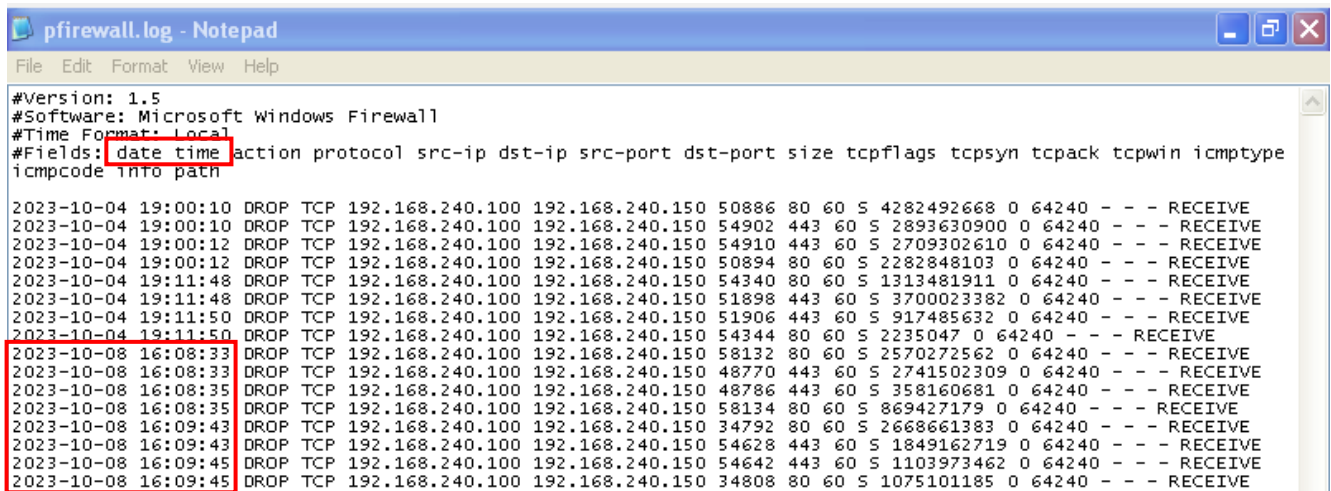
```
pfirewall.log - Notepad
File Edit Format View Help

#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

Analizzando il file di log più in dettaglio, vediamo:

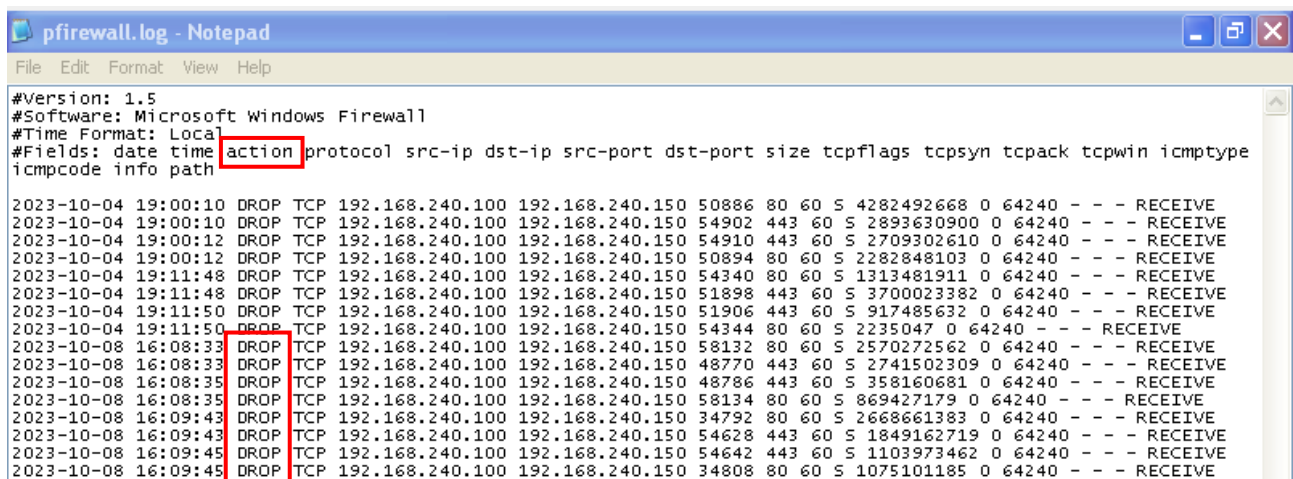
### Data e ora dell'evento:



```
#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

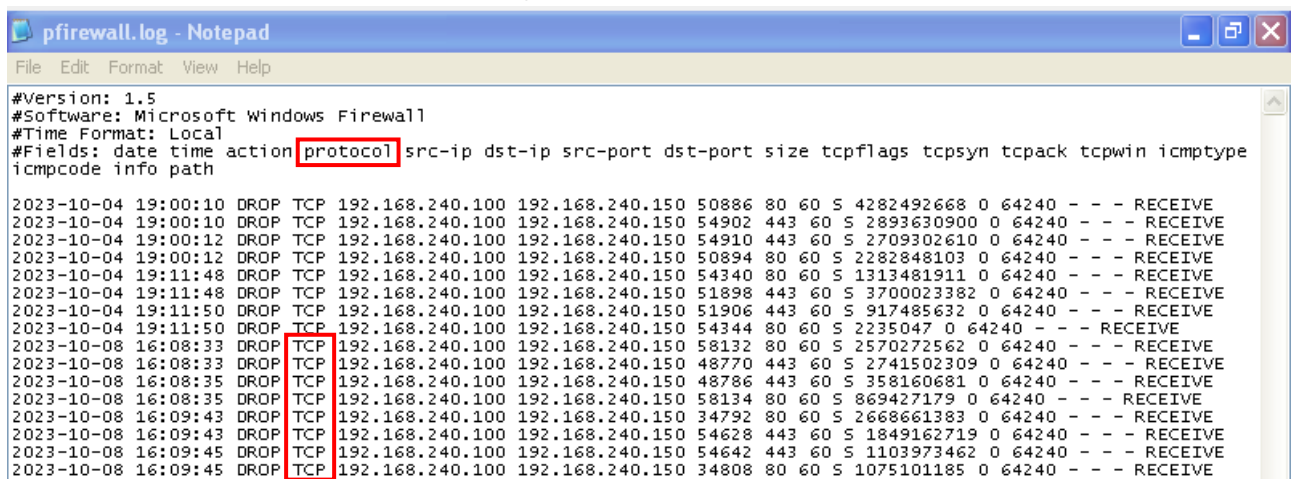
### Azione compiuta dal Firewall (in questo caso DROP, i pacchetti in entrata sono stati bloccati):



```
#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

### Protocollo utilizzato dalle richieste (in questo caso TCP):



```
#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```



Indirizzo IP di origine delle richieste (in questo caso l'IP di Kali, 192.168.240.100):

```
pfirewall.log - Notepad
File Edit Format View Help

#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 tcppack tcpwin icmptype
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

Indirizzo IP di destinazione delle richieste (in questo caso l'IP di Windows XP, 192.168.240.150):

```
pfirewall.log - Notepad
File Edit Format View Help

#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 tcppack tcpwin icmptype
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

Porte di origine delle richieste (le porte di Kali utilizzate da nmap per inviare il pacchetto):

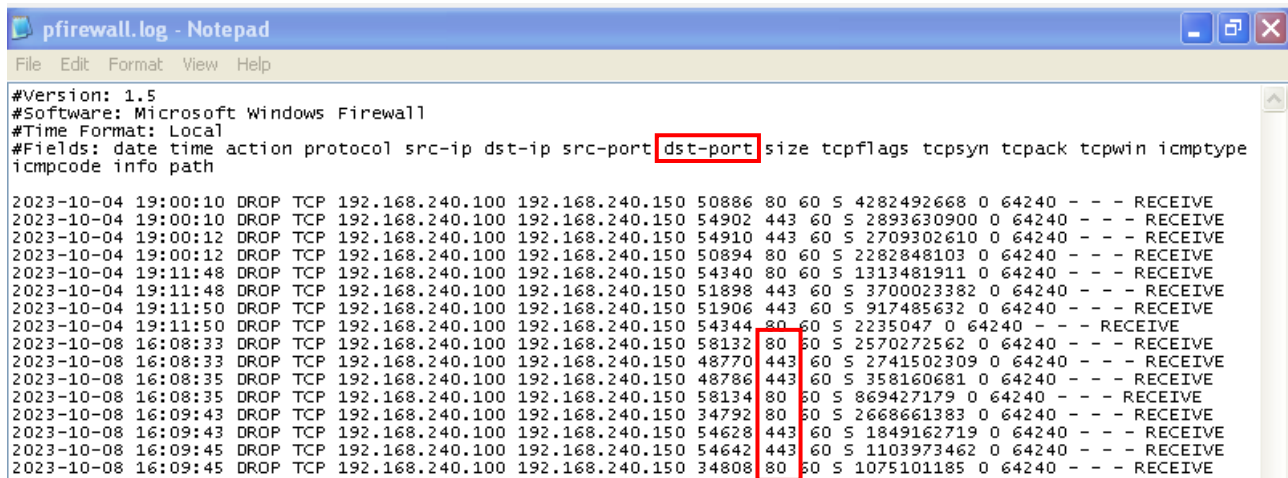
```
pfirewall.log - Notepad
File Edit Format View Help

#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 tcppack tcpwin icmptype
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```



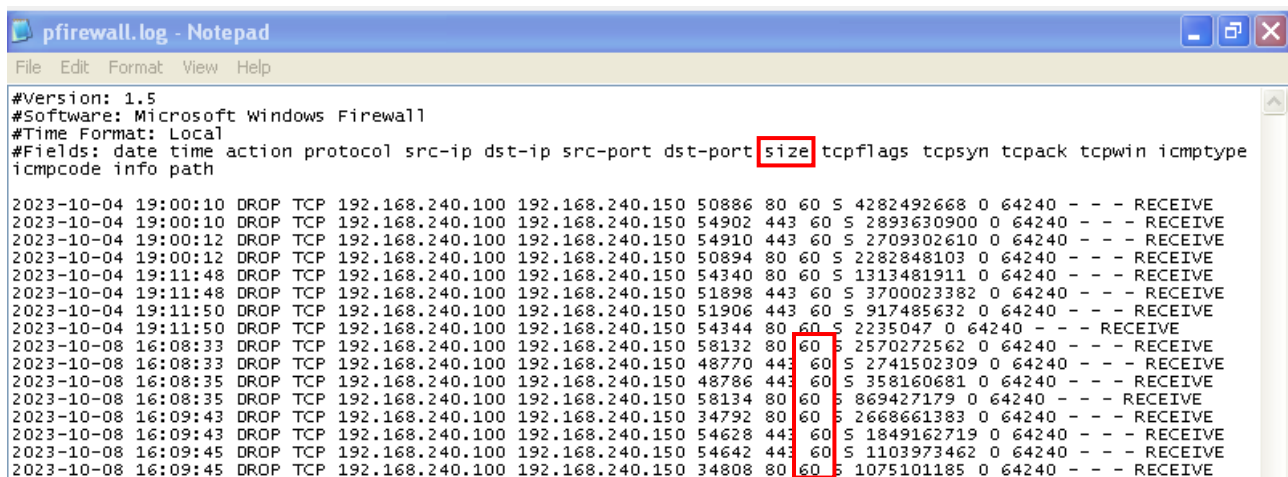
Porte di destinazione delle richieste (le porte Windows XP alle quali nmap ha inviato il pacchetto, in questo caso la 80 e la 443):



```
#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

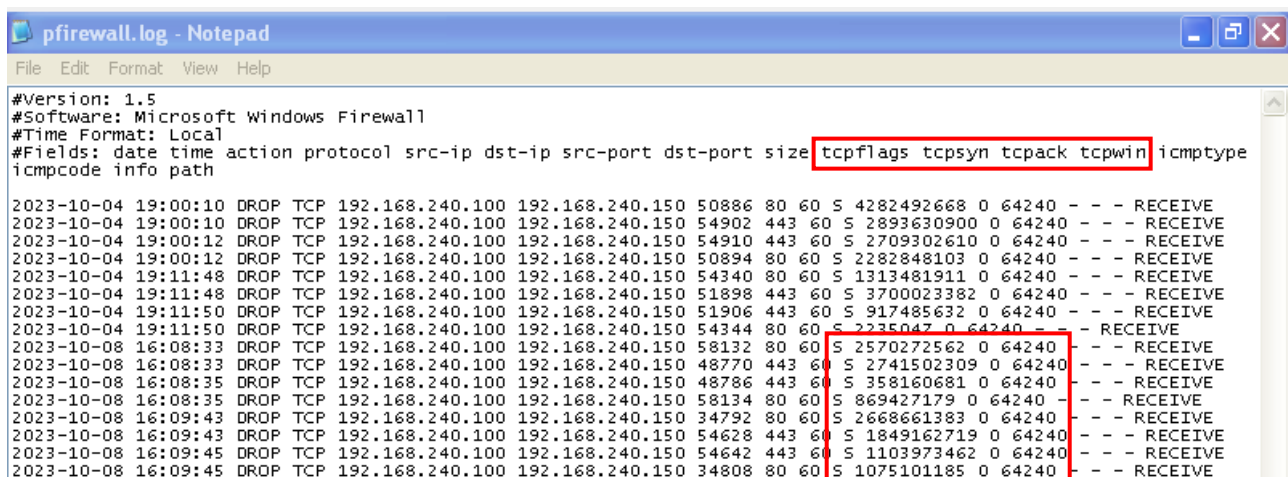
Dimensione dei pacchetti trasmessi (in byte, in questo caso 60):



```
#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

**Dettagli sulla comunicazione TCP.** Il campo `tcpflags` è valorizzato a "s", significa che nmap ha inviato pacchetti SYN per iniziare il three-way handshake. In corrispondenza del campo `tcpack` vediamo che la risposta al three-way handshake è sempre 0 in quanto si tratta di connessioni rifiutate:



```
#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
icmptype info path

2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

**Dettagli sulla comunicazione ICMP (ping).** I campi `icmpcode`, `icmpcode` e `info`, di dettaglio sul protocollo ICMP - o di informazioni aggiuntive nel caso del campo `info` - sono vuoti perché non è stato effettuato questo tipo di richiesta:

```
pfirewall.log - Notepad
File Edit Format View Help

#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 icmpcode info path
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```

Percorso del pacchetto, in questo caso sono pacchetti in ricezione e quindi è "RECEIVE".

```
pfirewall.log - Notepad
File Edit Format View Help

#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 icmpcode info path
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 50886 80 60 S 4282492668 0 64240 - - - RECEIVE
2023-10-04 19:00:10 DROP TCP 192.168.240.100 192.168.240.150 54902 443 60 S 2893630900 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 54910 443 60 S 2709302610 0 64240 - - - RECEIVE
2023-10-04 19:00:12 DROP TCP 192.168.240.100 192.168.240.150 50894 80 60 S 2282848103 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 54340 80 60 S 1313481911 0 64240 - - - RECEIVE
2023-10-04 19:11:48 DROP TCP 192.168.240.100 192.168.240.150 51898 443 60 S 3700023382 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 51906 443 60 S 917485632 0 64240 - - - RECEIVE
2023-10-04 19:11:50 DROP TCP 192.168.240.100 192.168.240.150 54344 80 60 S 2235047 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 58132 80 60 S 2570272562 0 64240 - - - RECEIVE
2023-10-08 16:08:33 DROP TCP 192.168.240.100 192.168.240.150 48770 443 60 S 2741502309 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 48786 443 60 S 358160681 0 64240 - - - RECEIVE
2023-10-08 16:08:35 DROP TCP 192.168.240.100 192.168.240.150 58134 80 60 S 869427179 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 34792 80 60 S 2668661383 0 64240 - - - RECEIVE
2023-10-08 16:09:43 DROP TCP 192.168.240.100 192.168.240.150 54628 443 60 S 1849162719 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 54642 443 60 S 1103973462 0 64240 - - - RECEIVE
2023-10-08 16:09:45 DROP TCP 192.168.240.100 192.168.240.150 34808 80 60 S 1075101185 0 64240 - - - RECEIVE
```