

# SECURITY OPERATION: Azioni preventive

## CS - Operation

### TRACCIA:

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi preventivi all'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 in formato OVA che abbiamo utilizzato nella Unit 2 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 service detection e -o nomefilereport per salvare in un file l'output)
- 3) Abilitate 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
  - Che differenza notate? E quale può essere la causa del risultato diverso?

### REQUISITI

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

### BONUS:

- Monitorare i log durante queste operazioni
- Cosa si riesce a trovare?

---

## CONFIGURAZIONE IP DELLE DUE MACCHINE

I) Configurare l'indirizzo di Kali con IP 192.168.240.100:

- dal terminal: andiamo ad aprire il file 'network 'interfaces' utilizzando il comando 'sudo nano /etc/network/interfaces'
- modifico il file come segue:

```
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
#address 192.168.13.10/24
address 192.168.240.100/24
#gateway 192.168.13.1
```

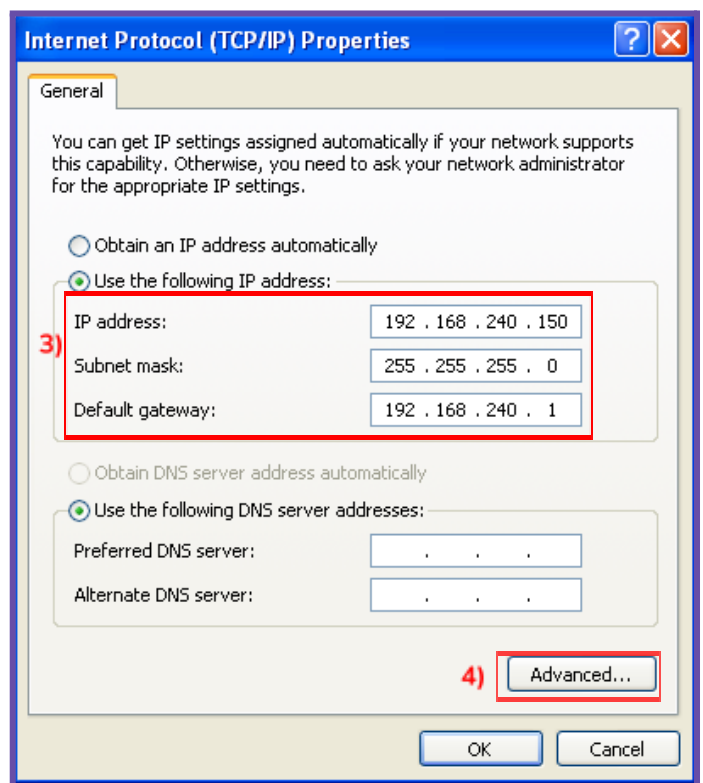
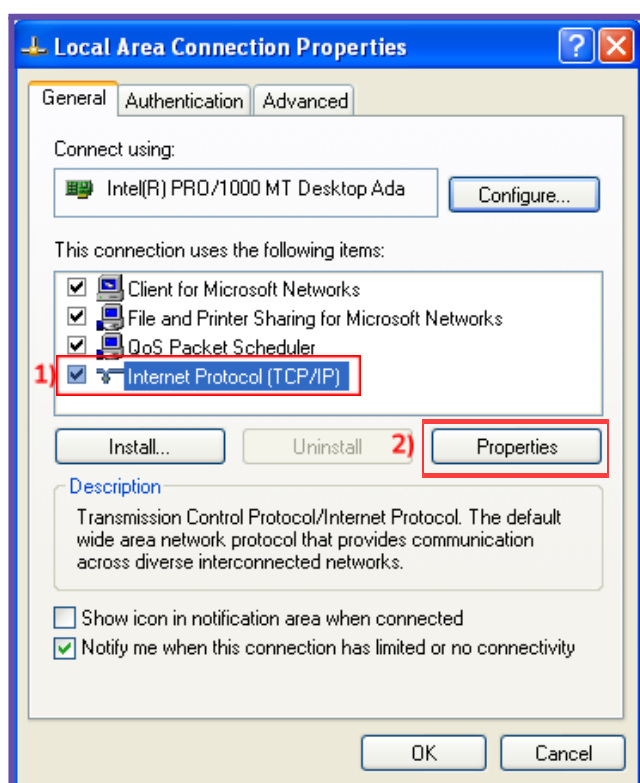
```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::a00:27ff:fe06:7605 prefixlen 64 scopeid 0<link>
    ether 08:00:27:06:76:05 txqueuelen 1000 (Ethernet)
    RX packets 104 bytes 15138 (14.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 74 bytes 11838 (11.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## II) Configurare la macchina Windows XP con IP 192.168.240.150

Per configurare l'indirizzo IP sulla macchina Windows XP:

- da Start: apro il Apro il 'Pannello di controllo'
- clicco su 'Network Connections'
- clicco su 'Local Area Connection'
- mi si apre una scheda delle proprietà della Local Area Connection, da questa scheda, faccio doppio click su 'Internet Protocol (TCP/IP)'
- mi si apre la scheda delle proprietà dell'Internet Protocol
- clicco sull'opzione 'Use the following IP address:' e configuro l'indirizzo IP della macchina Windows XP
- clicco su 'okay'



Verifico che la configurazione dell'IP sia stato salvato correttamente, aprendo il command prompt (cmd) e digitando:

`'ipconfig'`

Come possiamo vedere dalla seguente immagine, la configurazione dell'IP è stata effettuata correttamente.

```
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
```

## VERIFICO LA CONNETTIVITA' TRA LE DUE MACCHINE:

Dalla macchina Kali a Windows 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=1.57 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.33 ms
^C
— 192.168.240.150 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.570/1.947/2.325/0.377 ms
```

Dalla macchina Windows XP a Kali:

```
C:\Documents and Settings\Administrator>ping 192.168.240.100

Pinging 192.168.240.100 with 32 bytes of data:

Reply from 192.168.240.100: bytes=32 time=2ms 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=2ms 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 = 2ms, Average = 1ms
```

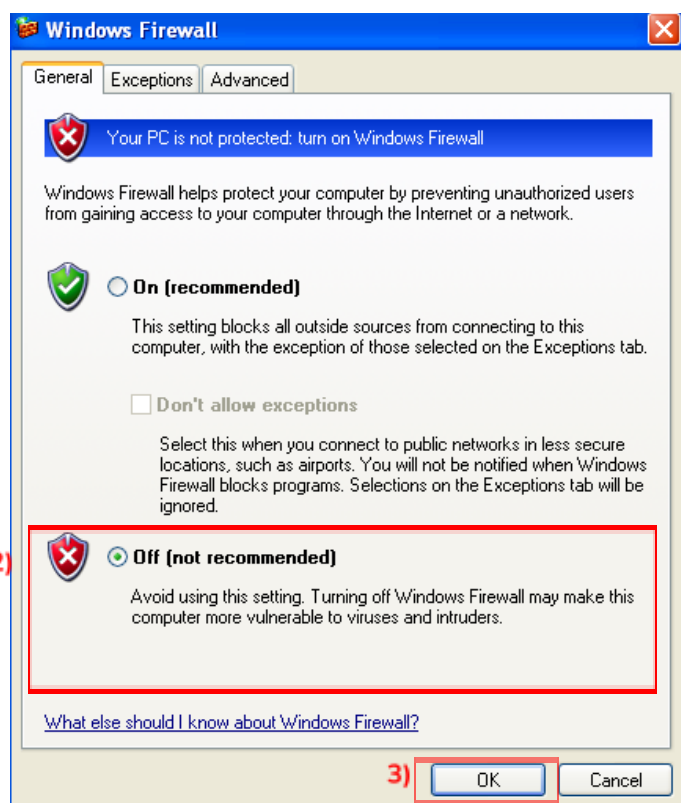
## SVOLGIMENTO ESERCIZIO

### 1) Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP

Per disattivare il Firewall su Windows XP, dobbiamo:

- andare sul pannello di controllo
- cliccare su 'Security Center'
- cliccare su 'Windows Firewall'
- cliccare su 'Off (not recommended)'

Manage security settings for:



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

Effettuo una scansione con nmap sulla macchina target utilizzando lo switch -sV (per service detection) e -o 'nomefilereport' (per salvare in un file l'output)

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -o xpreportscan.txt  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:40 CEST  
Nmap scan report for 192.168.240.150  
Host is up (0.0035s 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 Vista Embedded microsoft-ds (workgroup: WORKGROUP)  
1025/tcp  open  msrpc        Microsoft Windows RPC  
Service Info: Host: WINDOWSXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.08 seconds
```

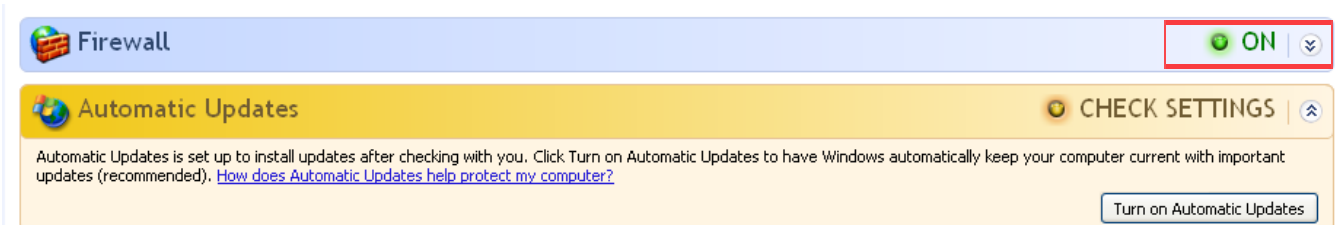
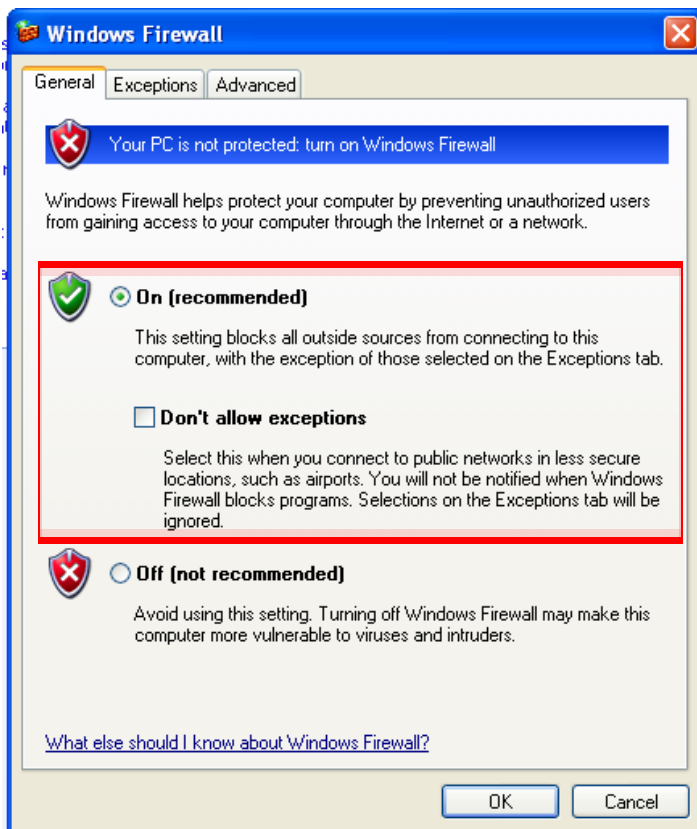
Apri il file 'xpreportscan.txt' per poter visualizzare il contenuto di tale file, che ci restituisce le porte aperte e i servizi attivi

```
(kali㉿kali)-[~]  
$ cat xpreportscan.txt  
# Nmap 7.94 scan initiated Thu Oct 26 14:40:08 2023 as: nmap -sV -o xpreportscan.txt 192.168.240.150  
Nmap scan report for 192.168.240.150  
Host is up (0.0035s 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 Vista Embedded microsoft-ds (workgroup: WORKGROUP)  
1025/tcp  open  msrpc        Microsoft Windows RPC  
Service Info: Host: WINDOWSXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
# Nmap done at Thu Oct 26 14:40:29 2023 -- 1 IP address (1 host up) scanned in 21.08 seconds
```

### 3 ) Abilitate il Firewall sulla macchina Windows XP

Per abilitare il Firewall sulla macchina Windows XP dobbiamo:

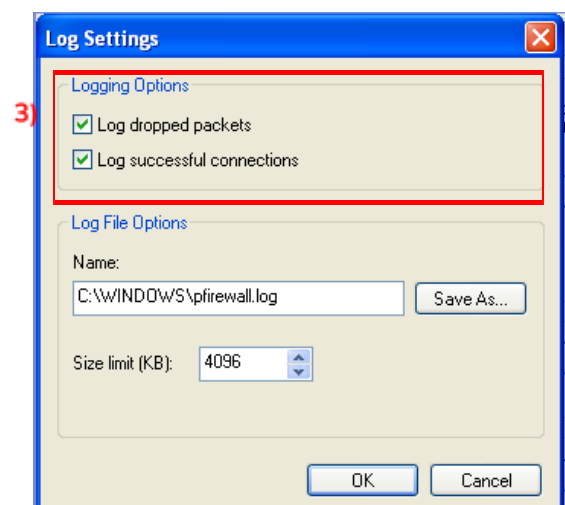
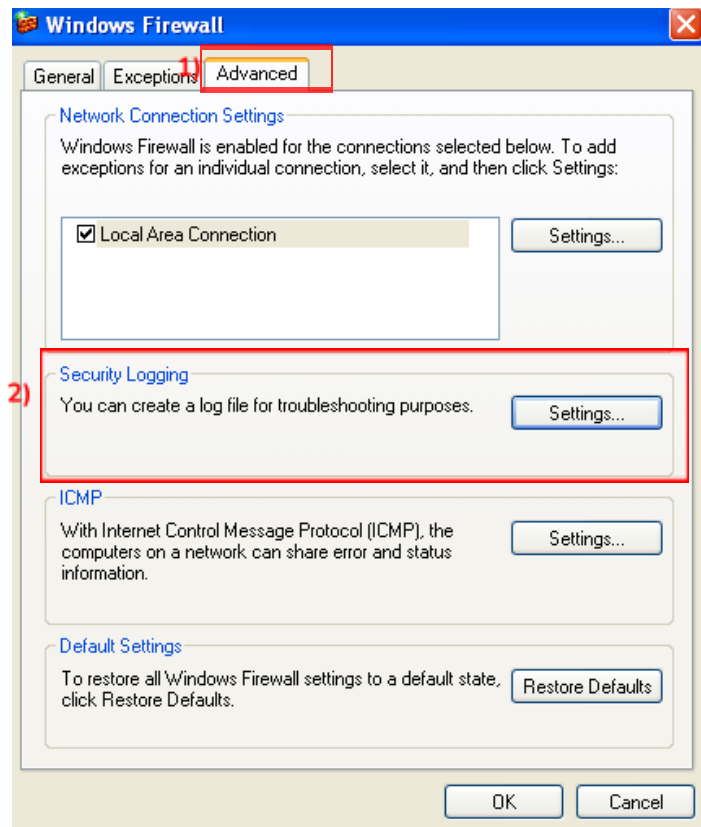
- andare sul pannello di controllo
- cliccare su 'Security Center'
- cliccare su 'Windows Firewall'
- cliccare su 'On (recommended)'



## Monitorare i log durante queste operazioni

Per poter monitorare i log durante le operazioni di scansione, dobbiamo abilitare i log del Firewall su Windows XP, per farlo dobbiamo:

- andare su 'Windows Firewall'
- andare sulla scheda 'Advanced'
- cliccare sulle impostazioni di 'Security Logging'
- abilitare le due opzioni di Log dropped Packets e Log successful connections



## 4) Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV.

Effettuo nuovamente la scansione con nmap sulla macchina target utilizzando ancora una volta lo switch -sV (per service detection) e -o 'nomefilereport' (per salvare in un file l'output)

```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150 -o xpreportscan.txt  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:50 CEST  
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 3.34 seconds
```

Visualizzo di nuovo il report e ci riporta il fatto che sia le porte aperte che i servizi attivi non siano stati rilevati con la scansione precedentemente effettuata

```
(kali㉿kali)-[~]  
$ cat xpreportscan.txt  
# Nmap 7.94 scan initiated Thu Oct 26 14:50:37 2023 as: nmap -sV -o xpreportscan.txt 192.168.240.150  
# Nmap done at Thu Oct 26 14:50:41 2023 -- 1 IP address (0 hosts up) scanned in 3.34 seconds
```

## 5) Trovare le eventuali differenze e motivarle

Nella scansione con il Firewall disattivato ha rilevato che le rispettive porte, di seguito evidenziate, fossero aperte e che i servizi fossero attivi

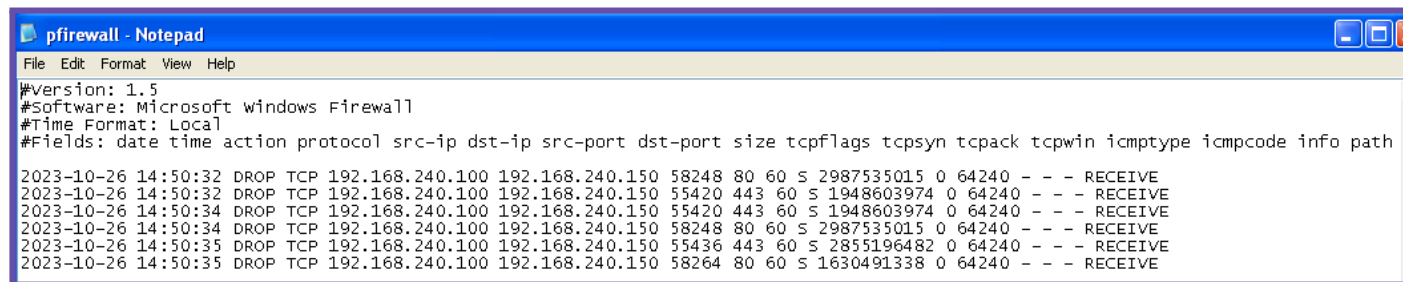
```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -o xpreportscan.txt  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:40 CEST  
Nmap scan report for 192.168.240.150  
Host is up (0.0035s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE          VERSION  
135/tcp   open  msrpc            Microsoft Windows RPC  
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds    Microsoft Windows Vista Embedded microsoft-ds (workgroup: WORKGROUP)  
1025/tcp  open  msrpc            Microsoft Windows RPC  
Service Info: Host: WINDOWSXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.08 seconds
```

Mentre nella scansione con Firewall attivato, la macchina non è riuscita a rilevare propriamente l'host:

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -o xpreportscan.txt  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:50 CEST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pr  
Nmap done: 1 IP address (0 hosts up) scanned in 3.34 seconds
```



Questo implica che il Firewall di Windows XP, ha impedito il rilevamento sia delle porte che dei servizi, infatti se andiamo ad analizzare il file di log, ci riporta (nella data e ora della scansione) i risultati effettuati dall'IP di Kali:



```
pfirewall - 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 icmpcode info path
2023-10-26 14:50:32 DROP TCP 192.168.240.100 192.168.240.150 58248 80 60 S 2987535015 0 64240 - - - RECEIVE
2023-10-26 14:50:32 DROP TCP 192.168.240.100 192.168.240.150 55420 443 60 S 1948603974 0 64240 - - - RECEIVE
2023-10-26 14:50:34 DROP TCP 192.168.240.100 192.168.240.150 55420 443 60 S 1948603974 0 64240 - - - RECEIVE
2023-10-26 14:50:34 DROP TCP 192.168.240.100 192.168.240.150 58248 80 60 S 2987535015 0 64240 - - - RECEIVE
2023-10-26 14:50:35 DROP TCP 192.168.240.100 192.168.240.150 55436 443 60 S 2855196482 0 64240 - - - RECEIVE
2023-10-26 14:50:35 DROP TCP 192.168.240.100 192.168.240.150 58264 80 60 S 1630491338 0 64240 - - - RECEIVE
```

Nello specifico:

DROP = i pacchetti in entrata sono stati bloccati

TCP = specifica il protocollo utilizzato per le richieste

src-ip = la sorgente dell'IP, che sarebbe l'IP di Kali che abbiamo configurato (192.168.240.100)

dst-ip = l'IP di destinazione, quindi l'IP di Windows XP (192.168.240.150)

src-port = riguarda la porta di origine, quindi quelle porte utilizzate durante la scansione nmap da Kali

dst-port = si riferisce alla porta di destinazione, alle quali nmap ha inviato il pacchetto

size = riguarda la dimensione del pacchetto trasmessi in byte

tcpflags tcpsyn = contrassegnato nel nostro caso da 'S', significa che nmap ha inviato pacchetti SYN

tcpack = contrassegnato da '0' significa che la risposta al three-way-handshake è stata rifiutata

tcpwin = utilizza un protocollo per mitigare i problemi con client e server che tentano di condividere segmenti di dati troppo grandi o piccoli e quindi non possono essere trasmessi in modo efficace.

icmptype icmpcode info = sono campi contrassegnati dal tratteggio in quanto non è stato effettuato questa tipo di richiesta

path = contrassegnato da 'RECEIVE', e riguarda il percorso del pacchetto e nel nostro caso sono pacchetti in ricezione