


# REPORT : AZIONI PREVENTIVE

Parlando di reti, è possibile prevenire e ridurre la possibilità di attacchi provenienti dall'esterno, si può ad esempio attivare/configurare un Firewall per fare in modo che un particolare traffico, potenzialmente dannoso venga bloccato.

In questa simulazione andremo innanzitutto ad impostare gli IP di Kali linux e XP in modo che siano riconoscibili.

```
(kali@kali)-[~]  
$ sudo ifconfig eth0 192.168.240.100
```

Connection status	
	Address Type: Manually Configured
	IP Address: 192.168.240.150
	Subnet Mask: 255.255.255.0
	Default Gateway: 192.168.240.150

Effettuando sempre un ping che verifichi l'effettiva connessione.

```
(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=0.911 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.21 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.36 ms  
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.33 ms  
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=1.32 ms  
^C  
— 192.168.240.150 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4010ms  
rtt min/avg/max/mdev = 0.911/1.224/1.350/0.164 ms
```

Usiamo il tool d'enumerazione servizi Nmap utilizzando switch < -sV > per la service detection e < -o > per salvare in un file in output.

```
(kali@kali)-[~]  
$ nmap -sV -o filexp 192.168.240.150  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:31 EST  
Nmap scan report for 192.168.240.150  
Host is up (0.0018s 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 20.85 seconds
```

Come possiamo notare da figura, lo scan ci restituisce molte informazioni sensibili come porte\servizi\versioni attive sul target, poiché esso non dispone di alcuna misura di sicurezza che impedisca allo scan di venire effettuato con successo.

Ma se il target avesse una misura di sicurezza, che risultato restituirebbe in quel caso nmap?

Abilitiamo quindi il firewall su macchina Windows Xp



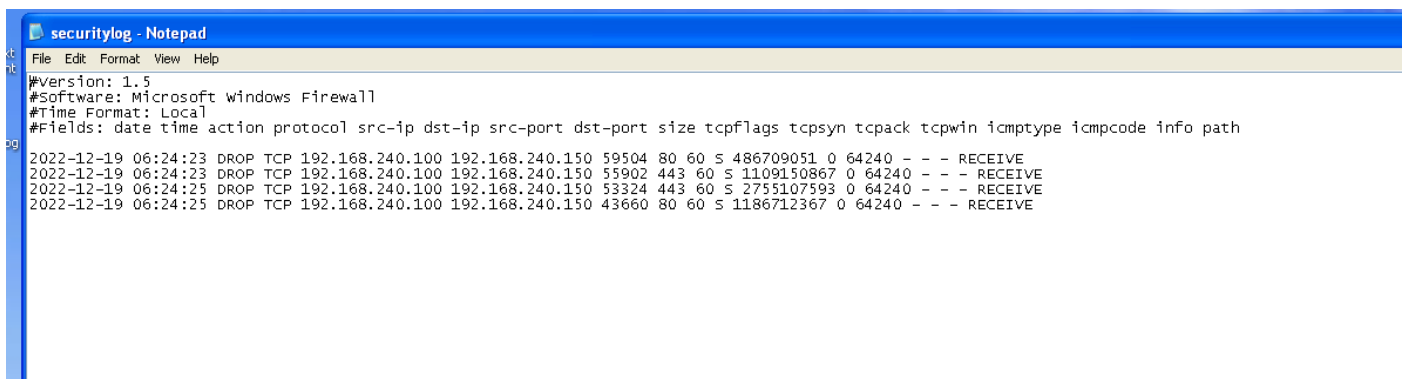
Ed effettuiamo nuovamente la scansione

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:35 EST
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 3.38 seconds
```

Come è possibile notare, lo scan non restituisce nessuna informazione in merito alla macchina target proteggendone i dati sensibili o potenzialmente sfruttabili da utenti malintenzionati.

Degli eventuali scan effettuati da utenti malevoli possono essere rilevati tramite l'event viewer di windows?

Con il Firewall attivato sarà possibile scaricare un documento di testo di firewall logs , che include qualsiasi tentativo da parte di un processo o applicazione che cerchi di stabilire una connessione che contravvenga alle regole stabilite .



Sull'event viewer non avremo risultati rilevanti a meno che non andremo ad attivare i settings dedicati, e soprattutto se verrà effettuato uno scan semplice, uno scan aggressivo invece verrà rilevato restituendoci un messaggio di alert

# Error Properties

## Event

Date: 19/12/2022 Source: TermService  
 Time: 6.38.21 Category: None  
 Type: Error Event ID: 1006  
 User: N/A  
 Computer: BOT-3C4EBAC7DD1

## Description:

The terminal server received large number of incomplete connections.  
 The system may be under attack.

For more information, see Help and Support Center at  
<http://go.microsoft.com/fwlink/events.asp>.

Data: ☒ Bytes ☐ Words

0000: 52 00 44 00 50 00 2d 00 R.D.P.-.  
 0008: 54 00 63 00 70 00 00 00 T.c.p...  
 0010: 00 00 00 00 00 00 00 00 .....

OK

Cancel

Apply

Information	19/12/2022	5.29.09	Browser	None
Error	19/12/2022	5.28.40	W32Time	None
Error	19/12/2022	5.28.40	W32Time	None

Category	Event	User	Computer
System	1006	N/A	BOT-3C4EB...
System	1006	N/A	BOT-3C4EB...
System	50	N/A	BOT-3C4EB...
System	50	N/A	BOT-3C4EB...
System	50	N/A	BOT-3C4EB...
System	7036	N/A	BOT-3C4EB...
System	7035	SYSTEM	BOT-3C4EB...
System	7036	N/A	BOT-3C4EB...
System	7036	N/A	BOT-3C4EB...
System	7035	Epicode_user6	BOT-3C4EB...
System	7036	N/A	BOT-3C4EB...
System	7036	N/A	BOT-3C4EB...
System	7035	Epicode_user6	BOT-3C4EB...
System	29	N/A	BOT-3C4EB...
System	17	N/A	BOT-3C4EB...
System	29	N/A	BOT-3C4EB...
System	17	N/A	BOT-3C4EB...
System	29	N/A	BOT-3C4EB...
System	17	N/A	BOT-3C4EB...
System	29	N/A	BOT-3C4EB...
System	17	N/A	BOT-3C4EB...
System	8033	N/A	BOT-3C4EB...
System	29	N/A	BOT-3C4EB...
System	17	N/A	BOT-3C4EB...