

WINDOWS XP SCAN:

#NMAP

#KALI LINUX

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 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 LA SERVICE DETECTION E **-O** NOMEFILEREPORT PER SALVARE IN UN FILE L'OUTPUT)
 3. **ABILITARE IL FIREWALL** SULLA MACCHINA WINDOWS XP
 4. EFFETTUATE UNA **SECONDA SCANSIONE CON NMAP**, UTILIZZANDO ANCORA UNA VOLTA LO SWITCH **-SV**.
 5. TROVARE EVENTUALI DIFFERENZE E MOTIVARLE.
- CHE DIFFERENZE NOTATE? E QUALE PUÒ ESSERE LA CAUSA DEL RISULTATO DIVERSO?

REQUISITI:

CONFIGURATE L'INDIRIZZO DI WINDOWS XP COME DI SEGUITO:
192.168.240.150

CONFIGURATE L'INDIRIZZO DELLA MACCHINA KALI COME DI SEGUITO: 192.168.240.100

SUGGERIMENTO:

SE NON SIETE CERTI DI COME ABILITARE IL FIREWALL SU WINDOWS XP, SEGUITE LE ISTRUZIONI DI SEGUITO.

1. CLICcate SULL'ICONA IN BASSO A DESTRA ALL'INTERNO DEL RETTANGOLO ROSSO IN FIGURA
2. CLICcate SU WINDOWS FIREWALL (RETTANGOLO BLU IN FIGURA)
3. SELEZIONATE «DISATTIVATO» COME IN FIGURA E CLICcate SU «OK»

BONUS:

MONITORARE I LOG DI WINDOWS DURANTE QUESTE OPERAZIONI.

1. QUALI LOG VENGONO MODIFICATI? (SE VENGONO MODIFICATI)
2. COSA SI RIESCE A TROVARE?

COME DA ACCORDI COL PROFESSORE I REQUISITI DI MODIFICA IP AL FINE DELL'ESERCIZIO POSSONO ESSERE IGNORATI.

PROCEDO QUINDI ALLA SCANSIONE DI **WINDOWS XP** PRIMA CON IL FIREWALL DISATTIVATO E POI CON IL FIREWALL ABILITATO CON **NMAP** DA **KALI LINUX** UTILIZZANDO GLI SWITCH SUGGERITI NELLA TRACCIA **-sV** E **-o** PER SALVARE IL FILE IN OUTPUT.

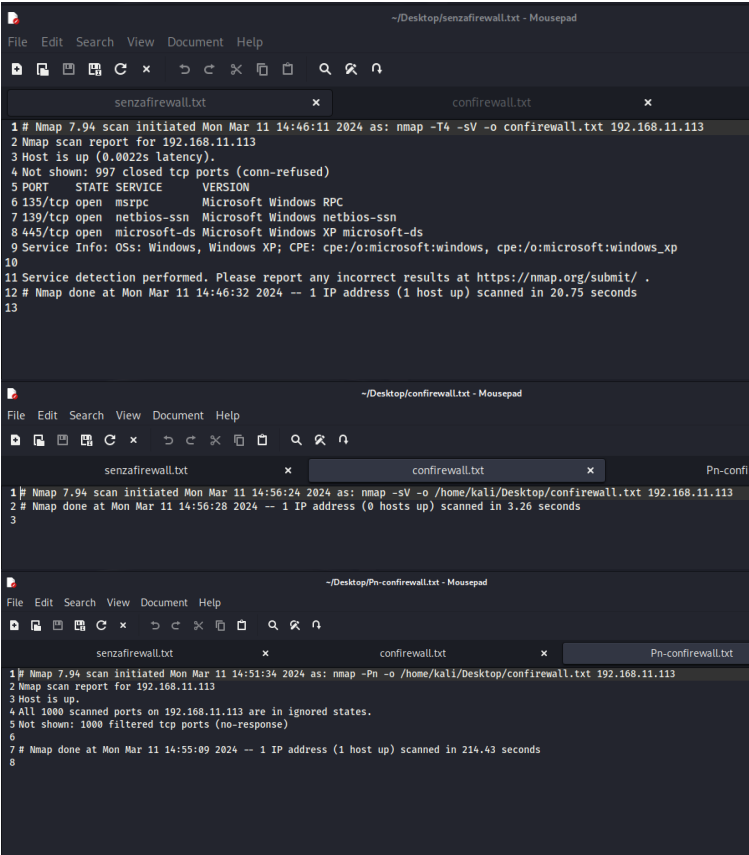
```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -T4 -sV 192.168.11.113 -o confirewall.txt  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-11 14:46 CET  
Nmap scan report for 192.168.11.113  
Host is up (0.0022s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE 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 20.75 seconds
```

#SCAN SERVIZI CON **-Pn** / FIREWALL WINDOWS ATTIVO

```
(kali@kali)~  
└─$ nmap -T4 -sV 192.168.11.113 -o ~/Desktop/confirewall.txt  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-11 14:51 CET  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap scan report for 192.168.11.113  
Host is up.  
All 1000 scanned ports on 192.168.11.113 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 214.43 seconds
```

VISUALIZZO E PARAGONO DI SEGUITO I TRE FILE ACQUISITI:

- 1) SENZAFIREWALL.TXT
- 2) CONFIREWALL.TXT
- 3) Pn-CONFIREWALL.TXT

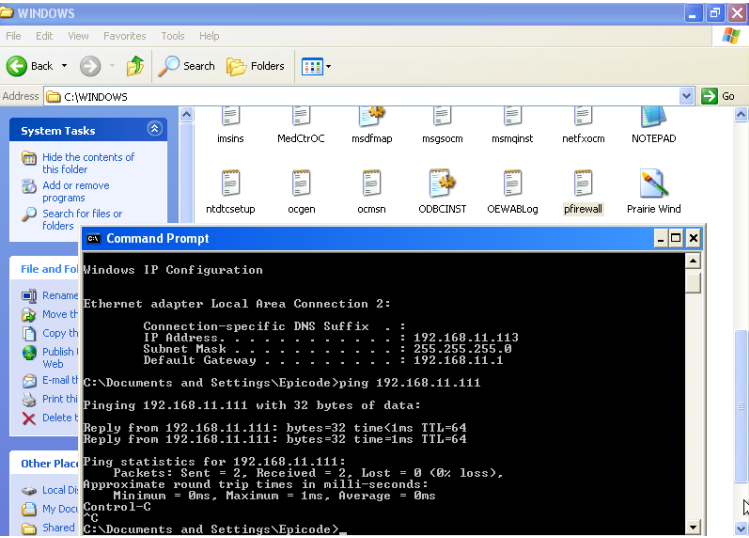
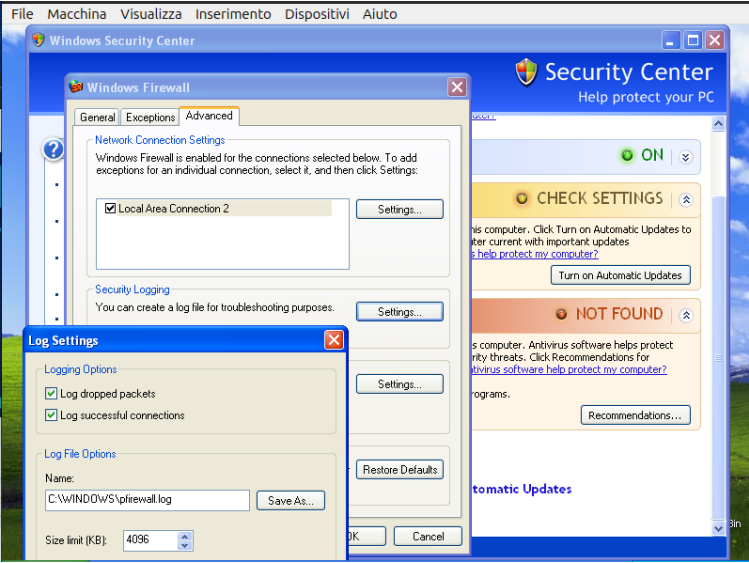


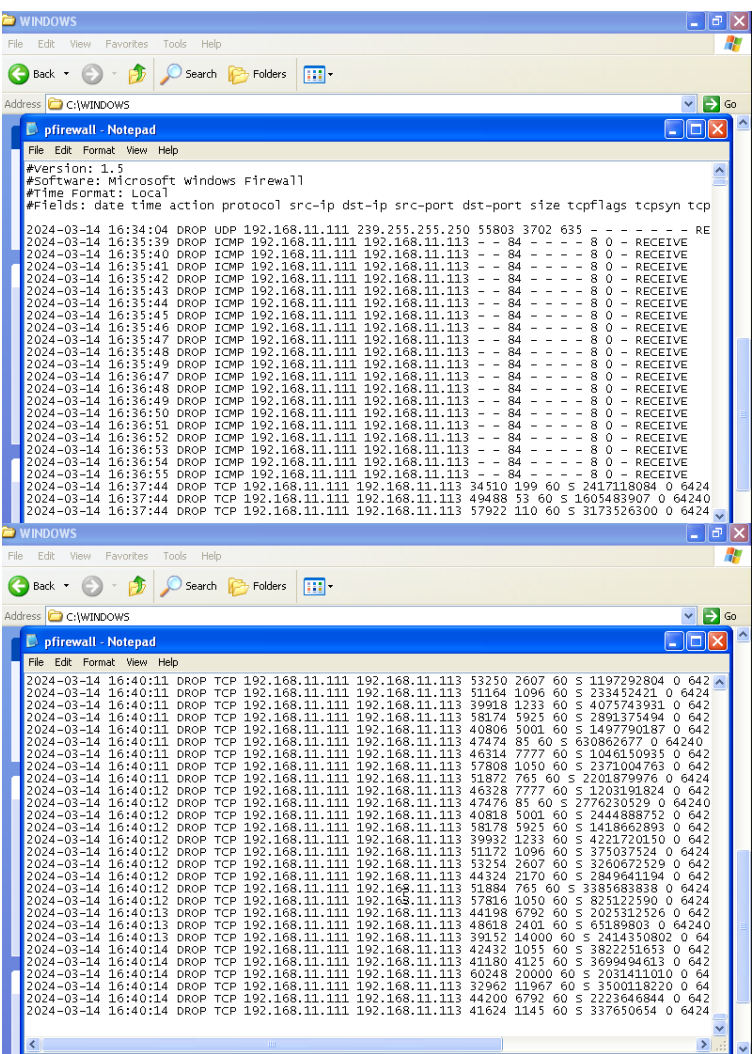
POSSO NOTARE COME NEL PRIMO CASO, SENZA FIREWALL, VENGONO RILEVATI L'OS E TRE SERVIZI TCP NOTI:

- 1) MSRPC SULLA PORTA 135/TCP
 - 2) NETBIOS-SSN SULLA PORTA 139/TCP
 - 3) MICROSOFT-DS SULLA PORTA 445/TCP
- E 997 PORTE CHIUSE.

NEL SECONDO CASO, CON FIREWALL ATTIVO, NON VIENE RILEVATO ALCUN SERVIZIO E VIENE SUGGERITO DI FARE UN NO-PING SCAN IN CASO CIA SIA CERTEZZA O SOSPETTO CHE L'HOST SIA UP. SEGUO IL SUGGERIMENTO RILEVANDO 1000 PORTE FILTRATE.

AVENDO ATTIVATO I LOG DALLE IMPOSTAZIONI DEL FIREWALL DI WINDOWS XP, NE RIPORTO GLI EVENTI CATTURATI NEL FILE PFIREWALL.LOG CHE SI TROVA IN C:\WINDOWS; POSSO NOTARE QUANTI PACCHETTI VENGONO DROPPATI DAL FIREWALL CHE BLOCCA LE RICHIESTE IN INGRESSO A PARTIRE DA UN SEMPLICE PINGE PROSEGUENDO CON LA MIA SCANSIONE.





POSSO CONSULTARE ALTRI LOG DALL'**EVENT VIEWER** CHE SI TROVA NEL **PANNELLO DI CONTROLLO -> PERFORMANCE AND MAINTENANCE -> ADMINISTRATIVE TOOLS**.

- QUI TROVO LOG DI TRE TIPI:
- 1) APPLICATION
 - 2) SECURITY
 - 3) SYSTEM

PRENDO COME ESEMPIO UN LOG A CASO DELLA CATEGORIA "APPLICATION" CHE MI NOTIFICA IL MOMENTO IN CUI VIENE ATTIVATO IL SERVIZIO DI "EVENT LOG".

