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:

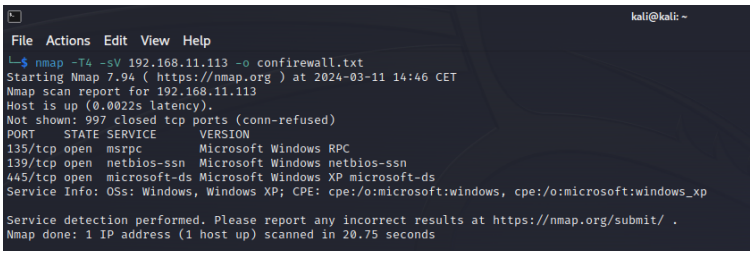
SE NON SIETE CERTI DI COME ABILITARE IL FIREWALL SU WINDOWS XP, SEGUITE LE ISTRUZIONI DI SEGUITO.
1. CLICCATE SULL'ICONA IN BASSO A DESTRA ALL'INTERNO DEL RETTANGOLO ROSSO IN FIGURA
2. CLICCATE SU WINDOWS FIREWALL (RETTANGOLO BLU IN FIGURA)
3. SELEZIONATE «DISATTIVATO» COME IN FIGURA E CLICCATE SU «OK»

BONUS:

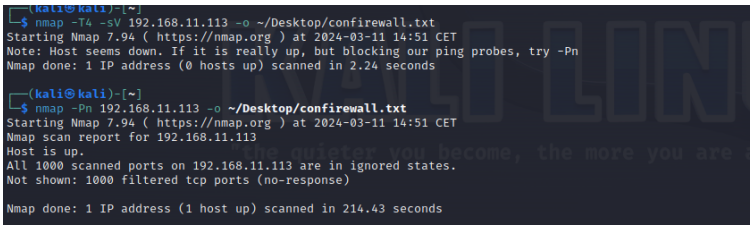
MONITORARE I LOG DI WINDOWS DURANTE QUESTE OPERAZIONI.
1. QUALI LOG VENGONO MODIFICATI? (SE VENGONO MODIFICATI)
2. COSA SI RIESCE A TROVARE?

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.



#SCAN SERVIZI CON -Pn / FIREWALL WINDOWS ATTIVO



VISUALIZZO E PARAGONO DI SEGUITO I TRE FILE ACQUISITI:
1) SENZAFIREWALL.TXT
2) CONFIREWALL.TXT
3) Pn-CONFIREWALL.TXT

~/Desktop/senzafirewall.txt - Mousepad

File Edit Search View Document Help

senzafirewall.txt | confirewall.txt

```
1 # Nmap 7.94 scan initiated Mon Mar 11 14:46:11 2024 as: nmap -T4 -sV -o confirewall.txt 192.168.11.113
2 Nmap scan report for 192.168.11.113
3 Host is up (0.0022s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT    STATE SERVICE      VERSION
6 135/tcp open  msrpc        Microsoft Windows RPC
7 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Mar 11 14:46:32 2024 -- 1 IP address (1 host up) scanned in 20.75 seconds
13
```

~/Desktop/confirewall.txt - Mousepad

File Edit Search View Document Help

senzafirewall.txt | confirewall.txt | Pn-confi

```
1 # Nmap 7.94 scan initiated Mon Mar 11 14:56:24 2024 as: nmap -sV -o /home/kali/Desktop/confirewall.txt 192.168.11.113
2 # Nmap done at Mon Mar 11 14:56:28 2024 -- 1 IP address (0 hosts up) scanned in 3.26 seconds
3
```

~/Desktop/Pn-confirewall.txt - Mousepad

File Edit Search View Document Help

senzafirewall.txt | confirewall.txt | Pn-confirewall.txt

```
1 # Nmap 7.94 scan initiated Mon Mar 11 14:51:34 2024 as: nmap -Pn -o /home/kali/Desktop/confirewall.txt 192.168.11.113
2 Nmap scan report for 192.168.11.113
3 Host is up.
4 All 1000 scanned ports on 192.168.11.113 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6
7 # Nmap done at Mon Mar 11 14:55:09 2024 -- 1 IP address (1 host up) scanned in 214.43 seconds
8
```

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.

I LOG SONO UNA MISURA DI SICUREZZA MOLTO IMPORTANTE A LIVELLO ORGANIZZATIVO; SERVONO SIA IN MANIERA PREVENTIVA PER VEDERE COSA STA ACCADENDO, SIA PER VEDERE SE MAGARI CI POTREBBERO ESSERE DEI TIPI DI SCANSIONE CHE VENGONO FATTE PRIMA DI UNA POSSIBILE FASE DI EXPLOITATION, MA ANCHE DURANTE L'ATTACCO E NELLA FARE POST ATTACCO. QUANDO C'È L'INCIDENTE NOI RACCOGLIAMO I LOG, E SONO USATI IN FASE DI ANALISI PER CAPIRE QUAL'È L'INCIDENTE. VEDIAMO E CAPIAMO DA LÌ COME COMPORTARCI E COME PRENDERE LE CORRETTE CONTROMISURE.

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

SU WINDOWS XP QUI TROVO LOG DI TRE TIPI:

1) APPLICATION: REGISTRA EVENTI SEGNALATI DALLE APPLICAZIONI O DAI PROGRAMMI. PUÒ ESSERE UTILE PER IDENTIFICARE PROBLEMI CON SPECIFICHE APPLICAZIONI.
2) SECURITY: CONTIENE EVENTI RELATIVI ALLA SICUREZZA, COME L'ACCESSO DEGLI UTENTI E LE OPERAZIONI RELATIVE ALLA SICUREZZA. È IMPORTANTE PER L'AUDIT E LA CONFORMITÀ.
3) SYSTEM: REGISTRA EVENTI RELATIVI A COMPONENTI DEL SISTEMA WINDOWS, COME DRIVER DI DISPOSITIVI E SERVIZI DI SISTEMA. È UTILE PER DIAGNOSTICARE PROBLEMI RELATIVI AL SISTEMA OPERATIVO.

INOLTRE CI SAREBBERO ANCHE:

- LOG DI INSTALLAZIONE: SPECIFICO PER LE VERSIONI SERVER DI WINDOWS, REGISTRA EVENTI RELATIVI ALL'INSTALLAZIONE DI APPLICAZIONI E SERVIZI.
- LOG FORWARDED EVENTS: VIENE UTILIZZATO IN AMBIENTI DI RETE PER CENTRALIZZARE GLI EVENTI RACCOLTI DA PIÙ COMPUTER IN UN UNICO VISUALIZZATORE EVENTI.

CE NE SONO ANCHE ALTRI; LA MAGGIOR PARTE DI QUESTI LOG PUÒ ESSERE TROVATA UTILIZZANDO L'EVENT VIEWER, MA ALCUNI POSSONO RICHIEDERE STRUMENTI O COMANDI SPECIFICI (COME POWERSHELL PER IL LOG DI WINDOWS UPDATE) O L'ACCESSO TRAMITE LE IMPOSTAZIONI DELL'APPLICAZIONE SPECIFICA (COME IL CENTRO SICUREZZA DI WINDOWS PER I LOG DI DEFENDER).

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