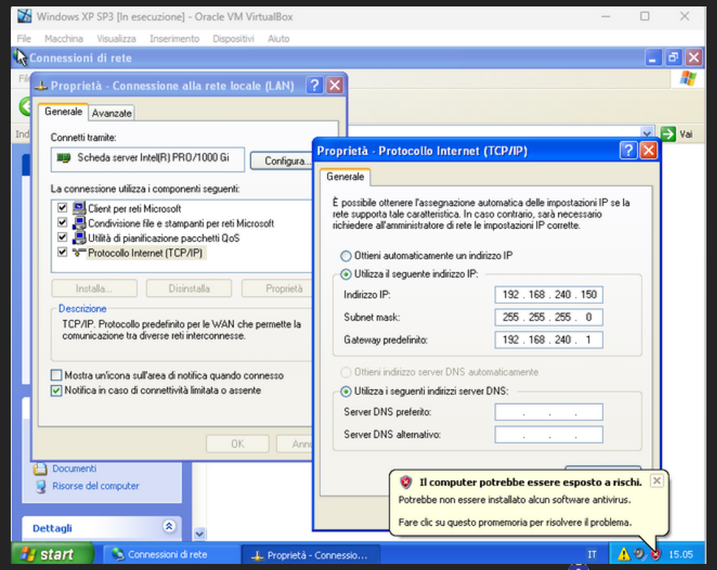
Home Work: SOC intro

EPICODE

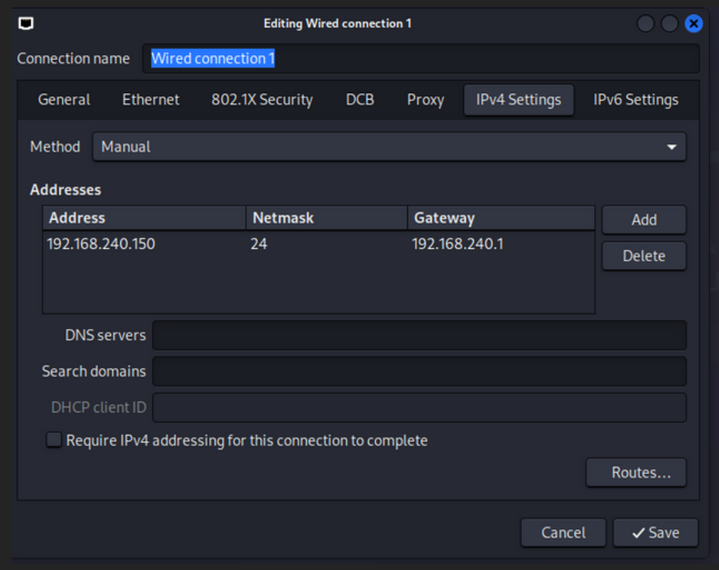
Giovanni Pisapia

CAMBIO INDIRIZZO IP META-WINDOWS

- Clicco sul pulsante "Start" e seleziono "Pannello di controllo".
- Faccio doppio clic su "Connessioni di rete".
- Clicco destro sulla connessione di rete attiva e seleziono "Proprietà".
- Faccio doppio clic su "Protocollo Internet (TCP/IP)".
- Imposto l'indirizzo IP, 192.168.240.150, la maschera di sottorete e il gateway predefinito desiderati.
- Clicco su "OK" per salvare le modifiche.



- Vado in alto a destra dove c'è un simbolo che assomiglia ad un entrata ethernet
- Tasto destro edit connection
- Mi sposto su ipv4 settings
- Cambio indirizzo ip 192.168.240.100



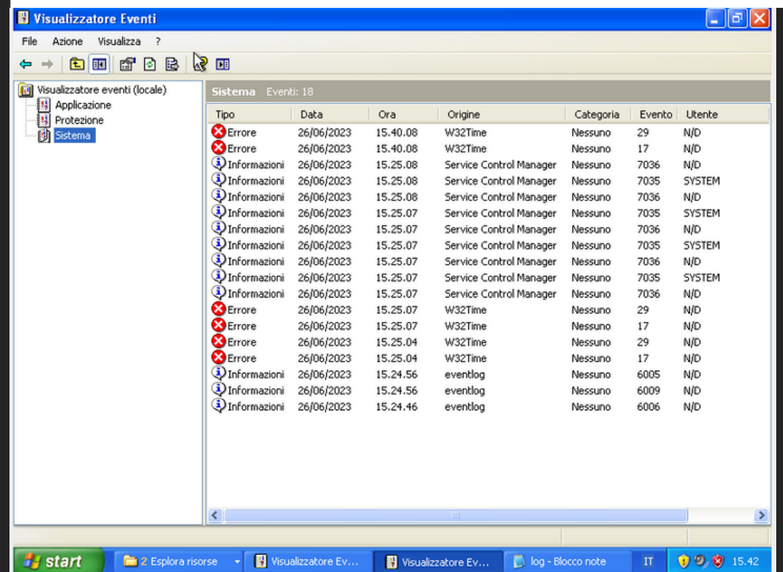
SCANSIONE NMAP SENZA FIREWALL

- Prima di tutto, eseguo una scansione di tutte le porte utilizzando il comando "nmap -sV 192.168.240.150 -o /home/kali/Desktop/report1.txt" per verificare quali porte sono attive e quali servizi sono presenti su di esse, con il risultato salvato in un file di testo.
- Notiamo che riusciamo a individuare le porte aperte senza il firewall.
- Una volta completata la scansione, passo a Windows per verificare eventuali modifiche nei registri degli eventi. Tuttavia, notiamo che non vi è alcuna modifica anche dopo aver premuto il pulsante di aggiornamento.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o /home/kali/Desktop/report1.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 09:11 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.240.150
Host is up (0.00042s 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 7.44 seconds
```

```
1 # Nmap 7.93 scan initiated Mon Jun 26 09:11:56 2023 as: nmap -sV -o /home/kali/Desktop/report1.txt 192.168.240.150
2 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
3 Nmap scan report for 192.168.240.150
4 Host is up (0.00042s latency).
5 Not shown: 996 closed tcp ports (conn-refused)
6 PORT     STATE SERVICE       VERSION
7 135/tcp  open  msrpc         Microsoft Windows RPC
8 139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
9 445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
10 3389/tcp open  ms-wbt-server Microsoft Terminal Services
11 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
12
13 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
14 # Nmap done at Mon Jun 26 09:12:03 2023 -- 1 IP address (1 host up) scanned in 7.44 seconds
15
```



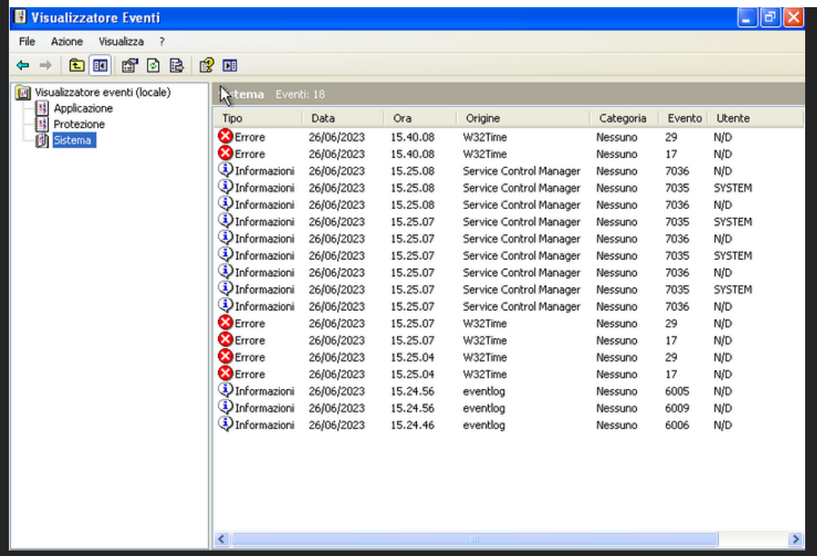
SCANSIONE NMAP CON FIREWALL

- Eseguo di nuovo la scansione "nmap -sV 192.168.240.150 -o /home/kali/Desktop/report2.txt" per verificare quali porte sono attive e quali servizi sono presenti su di esse, con il risultato salvato in un file di testo.
- Con l'attivazione del firewall notiamo che l'host scansionato non risponde alle richieste di ping inviate da Nmap, indicando che potrebbe non essere online o che la connessione di rete potrebbe essere disattiva.
- Una volta completata la scansione, passo a Windows per verificare eventuali modifiche nei registri degli eventi. Tuttavia, notiamo che neache in questo casa nulla è cambiato nella registrazione degli eventi.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o /home/kali/Desktop/report2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 09:13 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 3.20 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150 -o /home/kali/Desktop/report3.txt
```

```
# Nmap 7.93 scan initiated Mon Jun 26 09:13:41 2023 as: nmap -sV -o /home/kali/Desktop/report2.txt 192.168.240.150
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
# Nmap done at Mon Jun 26 09:13:44 2023 -- 1 IP address (0 hosts up) scanned in 3.20 seconds
```



CONCLUSIONI

Dopo accurate ricerche, ho scoperto che su Windows XP non esiste una funzionalità specifica per individuare i log di una scansione Nmap direttamente dal sistema operativo stesso.
Windows XP non dispone di strumenti di registrazione avanzati o di monitoraggio di rete integrati per identificare o registrare specificamente le scansioni Nmap.
Tuttavia, è possibile registrare i log delle scansioni Nmap attivando una funzionalità sul firewall che salva le informazioni su un file di testo, come quello mostrato nello screen. Questo file di log contiene l'indirizzo IP della scansione, l'orario di rilevamento e i dettagli del pacchetto ricevuto.