# SVOLGIMENTO TRACCIA S9L1

# CONFIGURAZIONE DEGLI INDIRIZZI IP MACCHINA ''KALI'' - MACCHINA WINDOWS XP

- Attraverso il seguente comando andremo a settare l'indirizzo ip della macchina kali linux:
  - apertura del terminale
  - Inserimento del comando : <sudo nano /etc/network/interfaces
  - Configurazione del parametro <address : 192,168,240,100>
  - Ctrl+c – INVIO – ''Y''

- Attraverso i seguenti passaggi configureremo la macchina WINDOWS XP
  - Accedere alla local area network cliccando sui due comuter visibili sulla barra di start
  - Cliccare su properties
  - Selezionare la voce TCP/IP
  - Selezionare properties
  - Modificare l'IP address in base alle nostre esigenze

# TRACCIA S9/L1

EPICODE

Esercizio
Le azioni preventive

**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 che abbiamo utilizzato 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 le eventuali differenze e motivarle.

PHANTOM
IMPOSSIBLE IS OUR TARGET

# SVOLGIMENTO DELLA TRACCIA
# CASO IN CUI IL FIREWALL SIA DISATTIVATO

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p- --min-rate 1000 -sV -T3 192.168.240.150 -oN report1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:22 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00026s latency).
Not shown: 65531 closed tcp ports (reset)
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: MSHOME)
1027/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:16:2B:30 (Oracle VirtualBox virtual NIC)
Service Info: Host: LUCA; 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 39.61 seconds
```

- Come possiamo vedere dopo aver inserito una scansione nmap (*nmap ci permette di visionare la mappa di rete con le relative porte aperte sulla rete target e i suioi demoni di servizio in ascolto sulle porte) possiamo vedere che le porte 135-139-445-1027 sono porte aperte.
- **IN PARTICOLARE LA PORTA 139 CHE ATTRAVERSO UN ATTACCO POTREBBE PORTARCI ALL'INTERNO DEL NET BIOS DEL PC DANDOCI ACCESSO COMPLETO ALLA MACCHINA.**

# SOLUZIONE SECONDO CASO CON FIREWALL WINDOWS ACCESO

- Come possiamo vedere dall’immagine al di sopra attivando il firewall le porte che prima potevano risultare una minaccia in termini di sicurezza ora risultano non più in ascolto.
- **Da questo possiamo dedurre che l’utilizzo di un firewall e di una corretta configurazione del medesimo provoca una riduzione dei rischi di attacchi in quanto va a limitare le vulnerabilità sfruttabili da un’attaccante.**