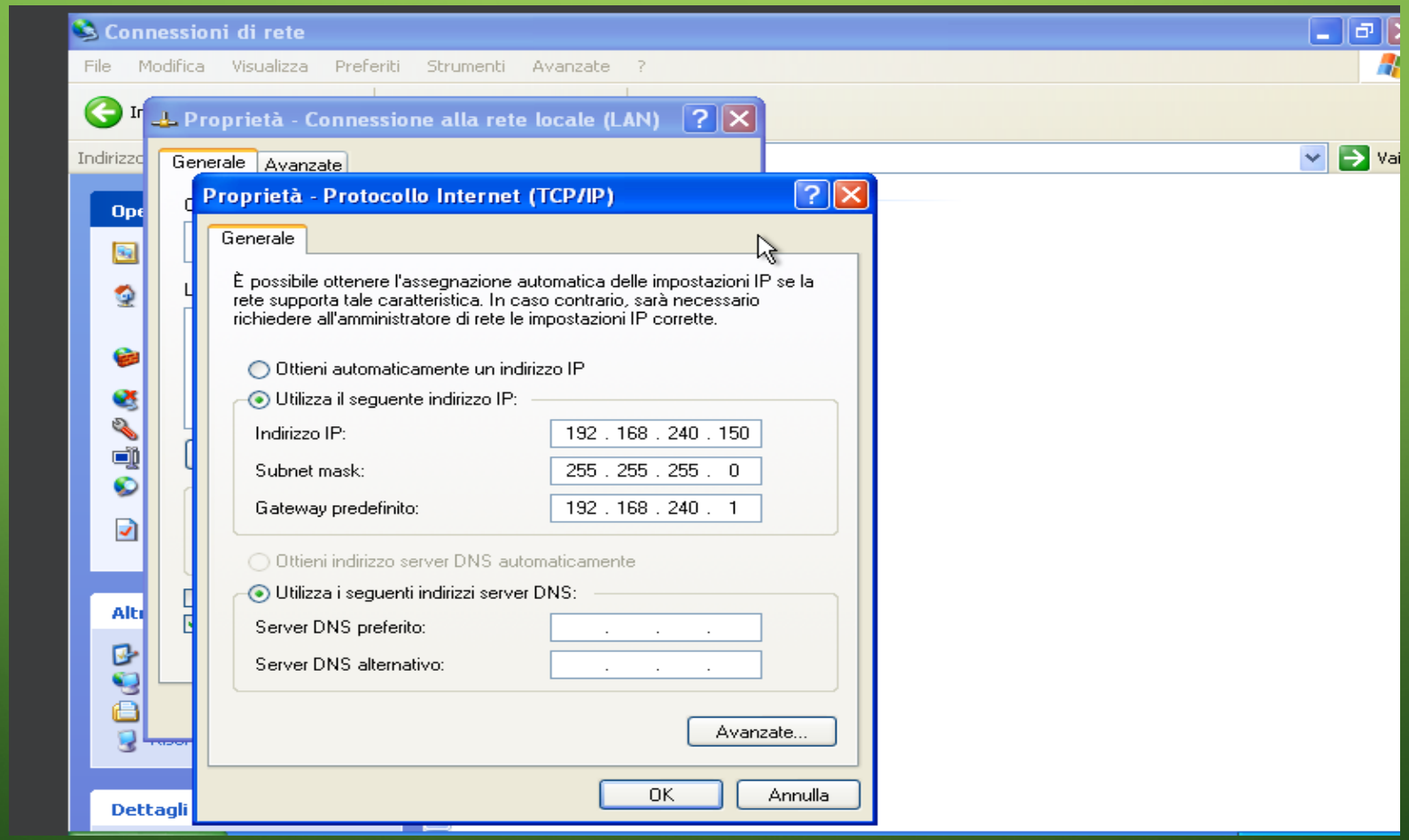
S9L1

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)
3. 3. ABILITARE IL FIREWALL SULLA MACCHINA WINDOWS XP 4. EFFETTUATE UNA SECONDA SCANSIONE CON NMAP, UTILIZZANDO ANCORA UNA VOLTA LO SWITCH –SV.

INIZIALMENTE SIAMO ANDATI A CONFIGURARE I SEGUENTI IP 1) IL PRIMO DI WINDOWS XK CON QUELLO RIPORTATO PER LA TRACCIA CON IL REGUENTE PERCORSO: PANNELLO DI CONTROLLO>CONNESSIONI DI RETE>PROPRIETA CONNESSIONI ALLA RETE LAN>TASTO DX DEL MOUSE PROTOCOLLO INTERNET (TCP/IP)V4



MENTRE PER L' IP DI KALI DA TERMINALE IN ALTO A SINISTRA DELLA SCHERMATA CON IL SEGUENTE COMANDO DA : **SUDO NANO /ETC/NETWORK/INTERFACES**

ADESSO UTILIZZEREMO NMAP CHE È UNO STRUMENTO PER ANALIZZARE LE RETI INFORMATICHE ED I SERVIZI E PROTOCOLLI DI RETE IN QUESTO CASO È STATO UTILIZZATO SULL'IP DI WINDOWS XP **192.168.240.150** CON IL FIREWALL DISABILITATO MOSTRANDO LE PORTE

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 11:15 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.240.150
Host is up (0.11s 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.66 seconds
```

MENTRE NEL SECONDO CASO CON IL FIREWALL ABILITATO SU WINDOWS XP CI VIENE RIPORTATO QUESTO CHE STA A SIGNIFICARE CON L'OUTPUT **"HOST SEEMS DOWN"** INDICA CHE NMAP NON È RIUSCITO A RILEVARE L'HOST SPECIFICATO COME ATTIVO SULLA RETE. QUESTO E' DOVUTO A DIVERSE, CONFIGURAZIONI FIREWALL CHE BLOCCANO I PACCHETTI ICMP (UTILIZZATI PER IL PING) O ALTRE FORME DI FILTRAGGIO CHE POSSONO IMPEDIRE A NMAP DI RAGGIUNGERE E INTERROGARE L'HOST.
FIREWALL: SE HAI UN FIREWALL ATTIVO SUL TUO INDIRIZZO IP, È PROBABILE CHE STIA BLOCCANDO LE RICHIESTE DI PING INVIATE DA NMAP PER DETERMINARE SE L'HOST È RAGGIUNGIBILE. L'AVVISO **"UNABLE TO DETERMINE ANY DNS SERVERS"** INDICA CHE NMAP NON È STATO IN GRADO DI TROVARE I SERVER DNS CONFIGURATI NEL SISTEMA. QUESTO NON È DIRETTAMENTE CORRELATO AL FALLIMENTO DELLA SCANSIONE, MA POTREBBE INFLUENZARE LA CAPACITÀ DI NMAP DI RISOLVERE I NOMI HOST IN INDIRIZZI IP.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 11:18 CET
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 11:18 (0:00:02 remaining)
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 3.27 seconds
```