S9L1

SECURITY OPERATION (AZIONI PREVENTIVE)

REQUISITI:
-UNA MACHINA KALI LINUX CON IL SEGUENTE INDIRIZZO IP: 192.168.240.100
-UNA MACCHINA WINDOWS XP CON IL SEGUENTE INDIRIZZO IP: 192.168.240.150

TRACCIA:

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. Disattivare il Firewall sulla macchina Windows XP

2.Effettuate una scansione con nmap sulla macchina target

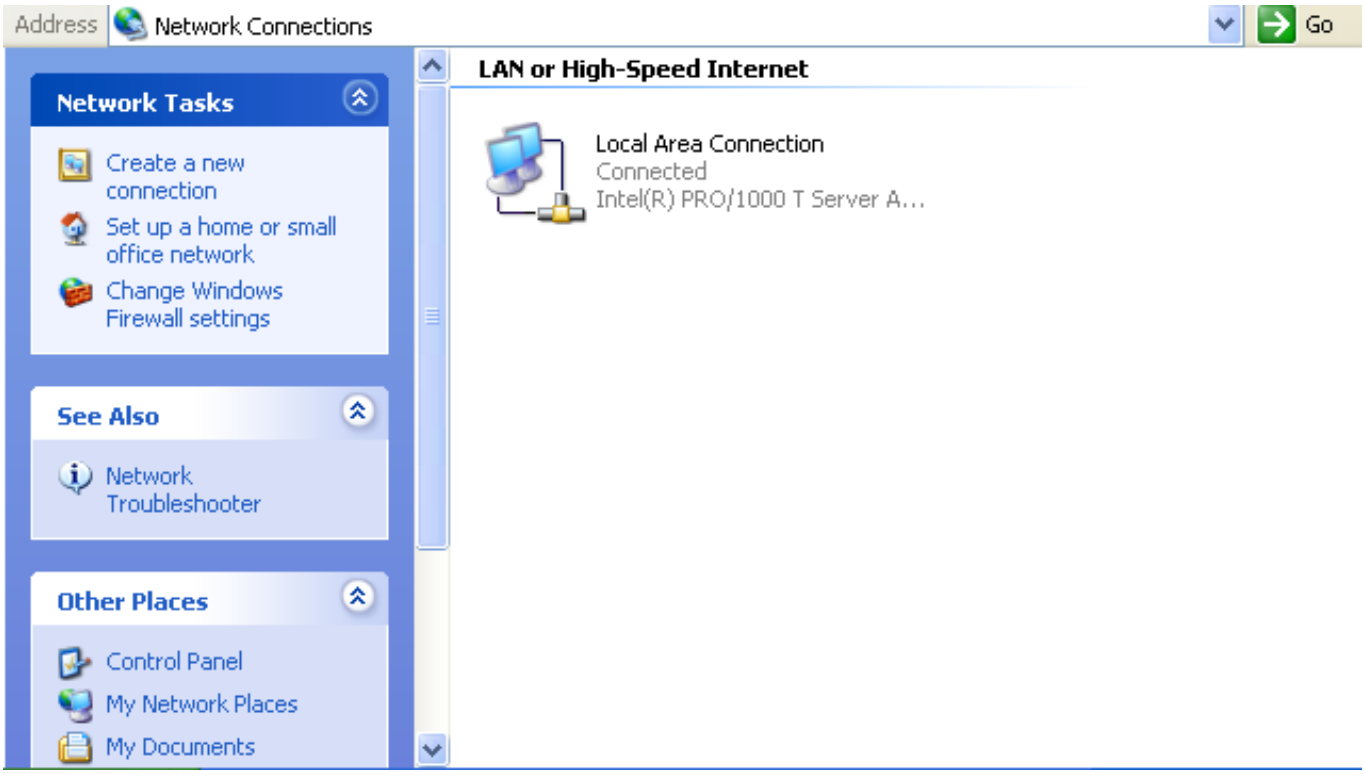
3.Abilitare il Firewall sulla macchina Windows XP

4.Effettuate una seconda scansione con nmap.

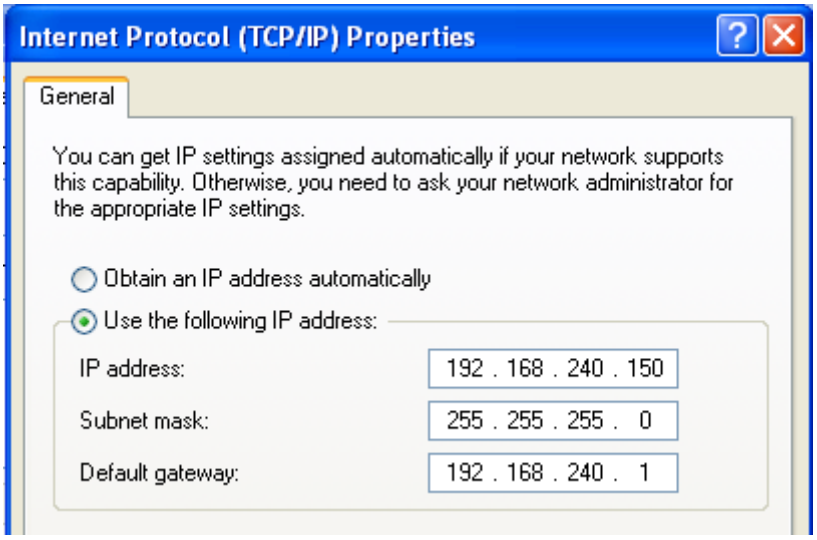
5.Trovare le eventuali differenze e motivarle.

SVOLGIMENTO:

Come prima cosa ci si deve assicurare di aver configurato correttamente le macchine come richiesto dalla consegna. Per poter cambiare indirizzo IP sulla macchina Windows XP bisogna andare sul pannello di controllo per poi selezionare Network and Internet connections > My network places > View network connections, in questa schermata sarà possibile controllare nello specifico le impostazioni di rete della macchina.

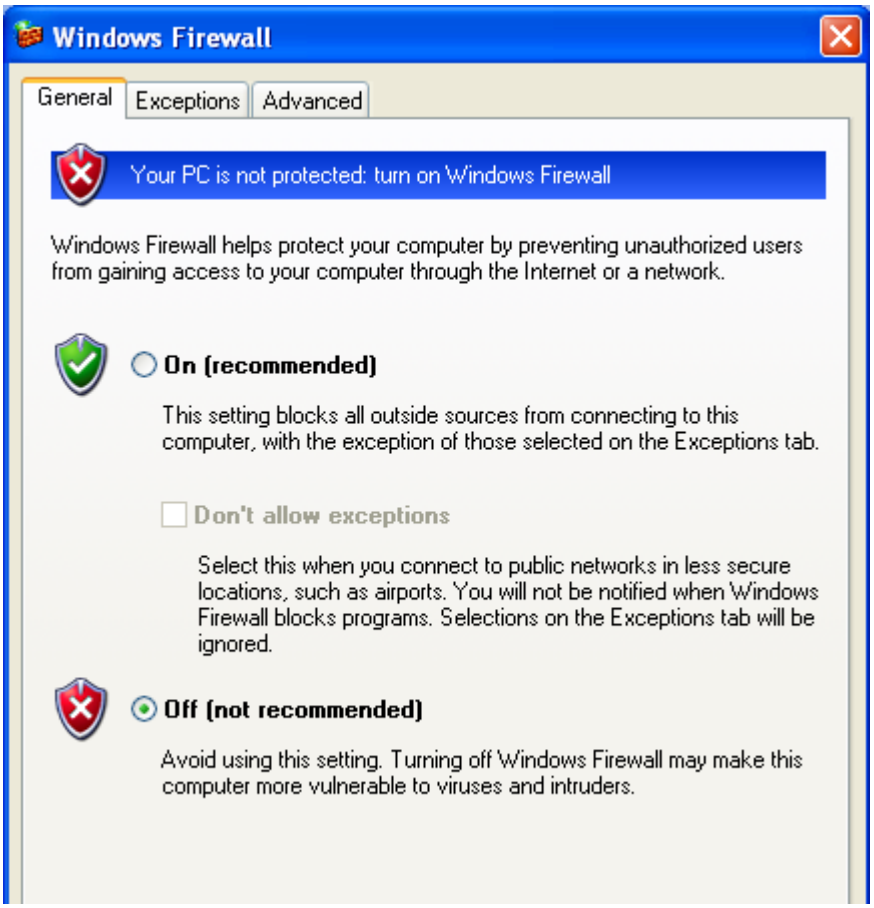


Dopo aver fatto ciò cliccando sul tasto properties sarà possibile modificare l'indirizzo IP di Windows XP come riportato nell'immagine.

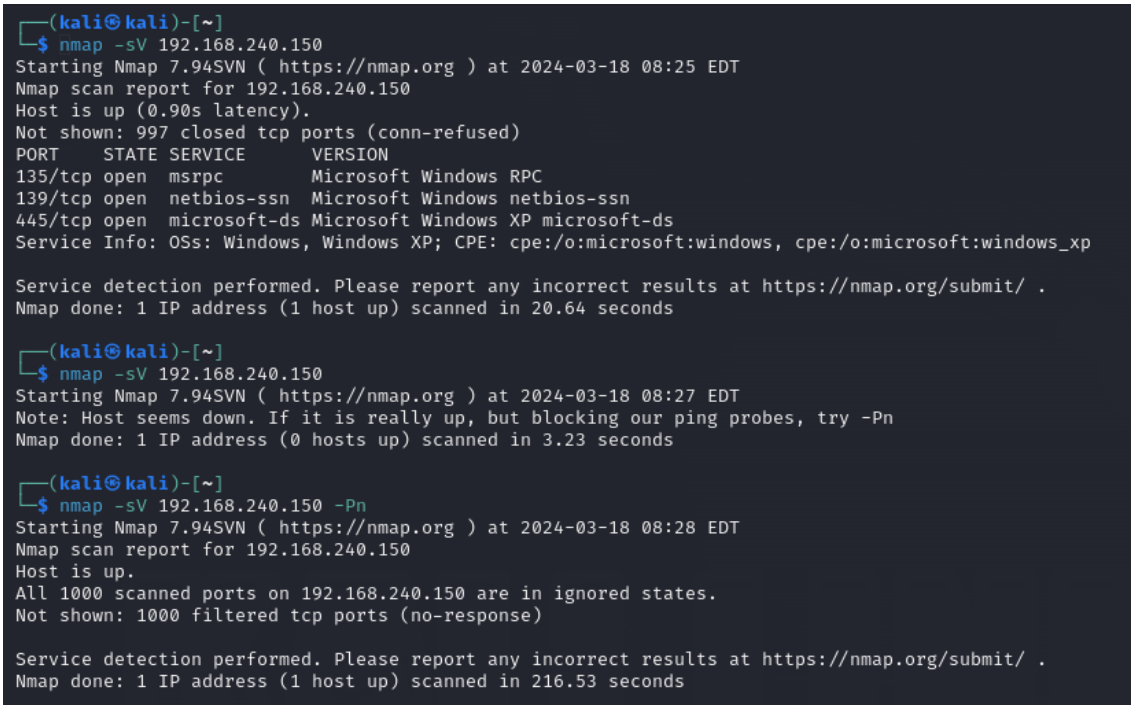


Mentre per cambiare indirizzo IP sulla macchina di Kali basta aprire il documento dove sono presenti le impostazioni di rete tramite la seguente riga di comando, per poi cambiarle come riportato nelle immagini.

Dopo aver configurato correttamente le impostazioni di rete su entrambe le macchine bisogna procedere con la disattivazione del firewall di Windows come illustrato nell'immagine.



La seguente immagine riporta 3 scansioni eseguite con nmap: la prima eseguita senza il firewall di windows, la seconda con il firewall acceso (senza successo), la terza con il firewall acceso, ma senza eseguire il ping per poter andare oltre il firewall.



La principale differenza tra la prima e la terza scansione effettuate è data dal fatto che nella terza il firewall impedisce di far controllare ad nmap lo stato delle porte

*da notare come la seconda scansione non è stata nominata per via del fatto che la terza è la risoluzione della seconda