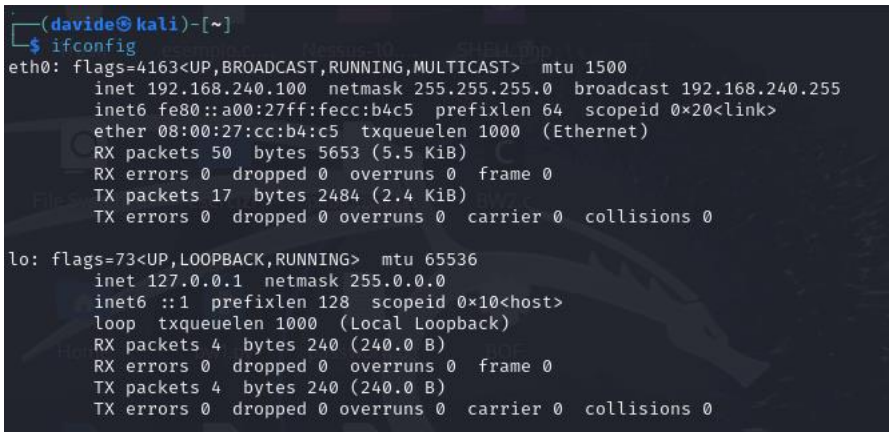
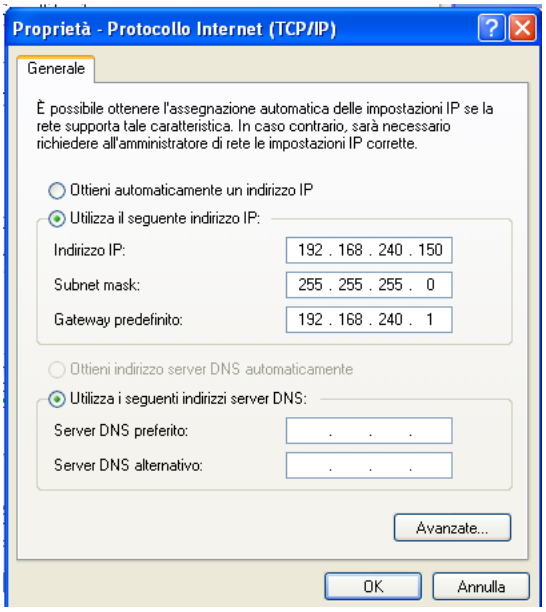
Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. 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. Abilitare il Firewall sulla macchina Windows XP 4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Procediamo col cambio dell'indirizzo IP di Kali Linux; per prima cosa lanciamo da terminale il seguente comando <> per accedere al file che contiene le informazioni della nostra scheda di rete e per modificare le configurazioni di rete. Una volta fatto ciò modifichiamo il contenuto del file in modo che sia identico alle configurazioni in figura. Le configurazioni mostrate conferiscono alla macchina il seguente indirizzo IP statico <<192.168.240.100>> Quando abbiamo modificato il file lo salviamo e lo chiudiamo con <> e <> e premiamo invio. In seguito, riavviamo la macchina col comando <> per applicare le modifiche appena effettuate.

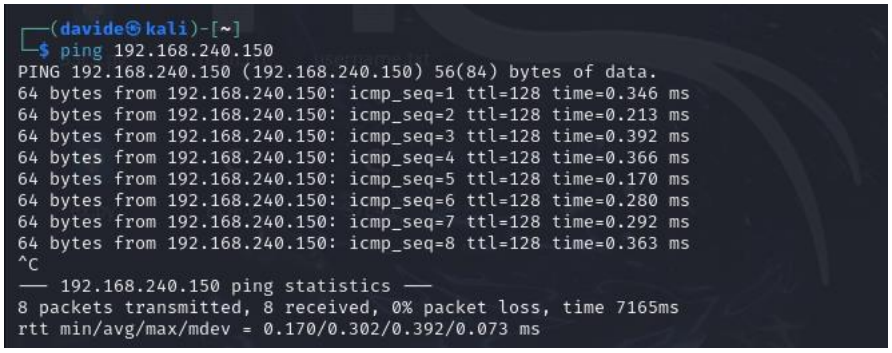
Dopo che la macchina si è riavviata possiamo verificare che le modifiche siano state apportate correttamente digitando da terminale il comando <> che mostra le informazioni sulla scheda di rete. Come possiamo osservare la scheda eth0 ha come indirizzo IP il seguente 192.168.240.100 quindi le modifiche sono state apportate correttamente



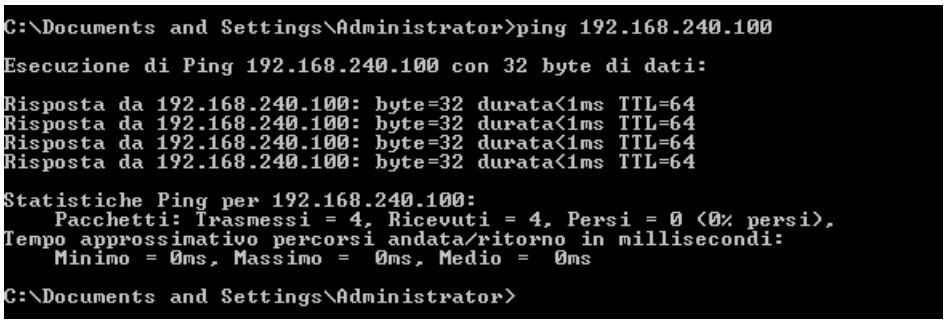
Per modificare l’indirizzo IP della macchina Windows XP bisogna raggiungere la finestra delle impostazioni di sistema corretta. Dopo aver acceso la macchina seguiamo il seguente path per raggiungere la finestra che ci permetterà di modificare l’indirizzo IP della macchina. [Start>Pannello di controllo>Rete e connessioni internet>Connessioni di rete>Tasto destro sulla scheda di rete>proprietà>Tasto sinistro su Protocollo Internet (TCP/UDP)>proprietà] Una volta raggiunta la finestra modifichiamo i valori come in figura per cambiare l’indirizzo IP al seguente <<192.168.240.150>> e riavviamo la macchina per apportare le modifiche.



Dopo aver configurato entrambe le macchine dobbiamo accertarci che riescano a comunicare fra loro, per fare ciò utilizzeremo la funzione <> che ci permette di mandare dei pacchetti ad un indirizzo IP che scegliamo noi per verificare che ci sia comunicazione tra le macchine. Da Kali mandiamo il seguente comando <> per effettuare un ping alla macchina Windows XP. Di 5 pacchetti inviati, 5 sono stati ricevuti confermando che avviene comunicazione tra le due macchine.



eseguiamo la stessa procedura anche nella direzione inversa, ovvero da Windows XP a Kali Linux. Sulla nostra macchina Windows XP apriamo un prompt dei comandi ed inseriamo il seguente comando <> per eseguire un ping verso Kali Linux. Analizzando il risultato del comando possiamo vedere che avviene lo scambio di pacchetti correttamente, confermando l'avvenuta comunicazione tra le due macchine.



Dopo aver configurato correttamente le due macchine ed esserci accertati che comunicano fra loro senza problemi possiamo procedere con le scansioni con nmap da Kali Linux verso Windows XP. Per prima cosa verifichiamo lo stato del firewall di Windows XP, per fare ciò apriamo il pannello di controllo e clicchiamo su Centro Sicurezza PC. Come possiamo osservare il firewall di Windows XP è attualmente disattivato. Preso nota dello stato del firewall torniamo su Kali e procediamo con la scansione.

Da terminale procediamo ad effettuare una scansione con nmap verso la macchina Windows XP che ci elencherà le porte attive sulla macchina target, procediamo col comando <> Osservando il risultato della scansione possiamo osservare che ci sono tre porte aperte sulla macchina Windows e sono rispettivamente la 135, la 139 e la 445. Prendiamo nota di questi risultati e procediamo con la seconda scansione.

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
[sudo] password for davide:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 12:49 CET
Nmap scan report for 192.168.240.150
Host is up (0.00040s latency).
Not shown: 997 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 XP microsoft-ds
MAC Address: 08:00:27:0E:53:2F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:wind
ows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 20.48 seconds
```

Abbiamo appena eseguito una scansione alla macchina Windows XP mentre il suo firewall era disattivato, proviamo adesso a ripetere la scansione dopo aver attivato il firewall per osservare eventuali differenze. Torniamo su Windows alla pagina Centro Sicurezza PC e attiviamo il firewall. Dopo aver attivato il firewall torniamo su Kali e ripetiamo lo scan.

Dopo essere tornati su Kali ripetiamo la scansione col comando <> Osservando il risultato della scansione possiamo notare che delle 1000 porte analizzate da nmap tutte e 1000 appaiono filtrate, di conseguenza possiamo dedurre che il firewall di Windows deve avere qualche regola che dice di droppare i pacchetti quando viene effettuata la scansione. Questa ipotesi è valorizzata dal fatto che se proviamo a ripetere il ping da Kali verso Windows questa volta non andrà a buon fine e ci informerà che i pacchetti non vengono ricevuti dalla macchina Windows

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 12:54 CET
Nmap scan report for 192.168.240.150
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:0E:53:2F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 34.52 seconds

┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150 -Pn
[sudo] password for davide:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 13:18 CET
Nmap scan report for 192.168.240.150
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:0E:53:2F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 34.53 seconds
```