

Report

**Pignatello
Giuseppe**



Prepared For
EPIC EDUCATION SRL

Requisiti

Configurate l'indirizzo di Windows XP come di seguito:

192.168.240.150

Configurate l'indirizzo della macchina Kali come di
seguito: 192.168.240.100

Configurazione Kali

Per modificare il suo indirizzo IP
utilizziamo il seguente comando:
`sudo nano /etc/network/interfaces`

Il comando `sudo` (Super User DO,
ovvero il comando esegui come
amministratore) serve a darci i
permessi necessari per poter
modificare i file, `nano` invece è il
nostro editor di testo.

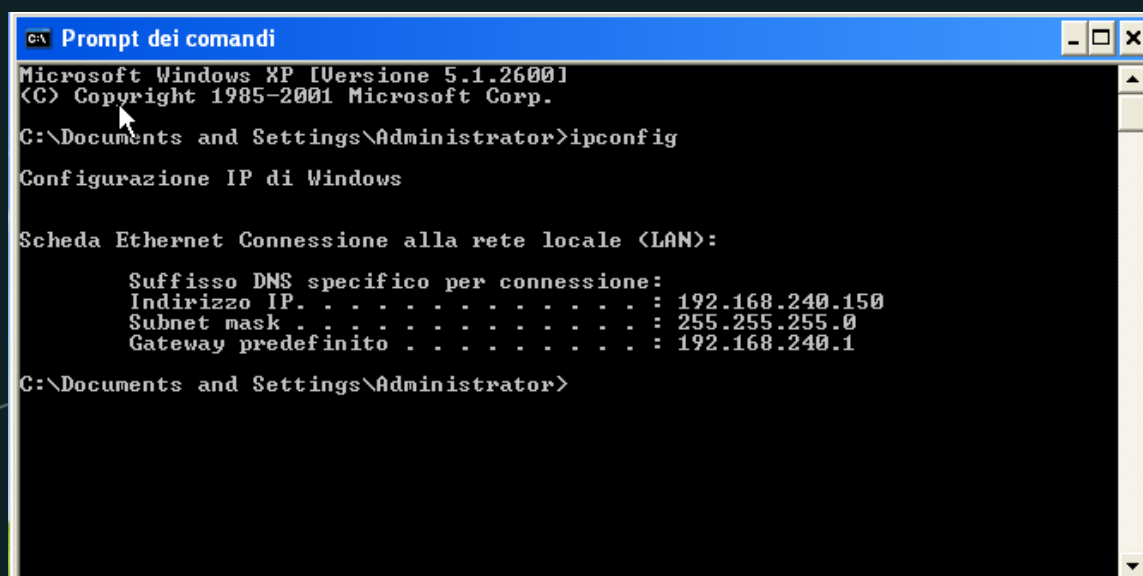
Successivamente ci spostiamo di
directory in directory tramite il path
`etc/network` e modifichiamo il file
`interfaces`.

Una volta modificato l'indirizzo,
eseguiamo il reboot della macchina e
verifichiamo che tutto sia stato
modificato e salvato tramite il
comando `ifconfig`.

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255  
    inet6 fe80::a00:27ff:fe74:1679 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:74:16:79 txqueuelen 1000 (Ethernet)  
    RX packets 66266 bytes 4008919 (3.8 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 71950 bytes 5333237 (5.0 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Configurazione WinXP

Per modificare il suo IP invece, premiamo il tasto start in basso a sinistra, dopodichè > Risorse del Computer > Risorse di rete > Visualizza connessioni di rete > Premiamo una volta sulla rete LAN > Cambia impostazioni connessione > Protocollo internet TCP/IP > Proprieta e modifichiamo l'indirizzo IP. Una volta faccio ciò riavviamo la macchina e verifichiamo che tutto sia stato modificato e salvato tramite il comando ipconfig.



```

c:\ Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.240.1

C:\Documents and Settings\Administrator>
```

Creazione Rete con NAT

Successivamente da VirtualBox creiamo una rete con NAT, (Premere la voce Strumenti > Rete con NAT > Crea) e impostiamo il prefisso IPv4 in questo modo:

192.168.240.0/24

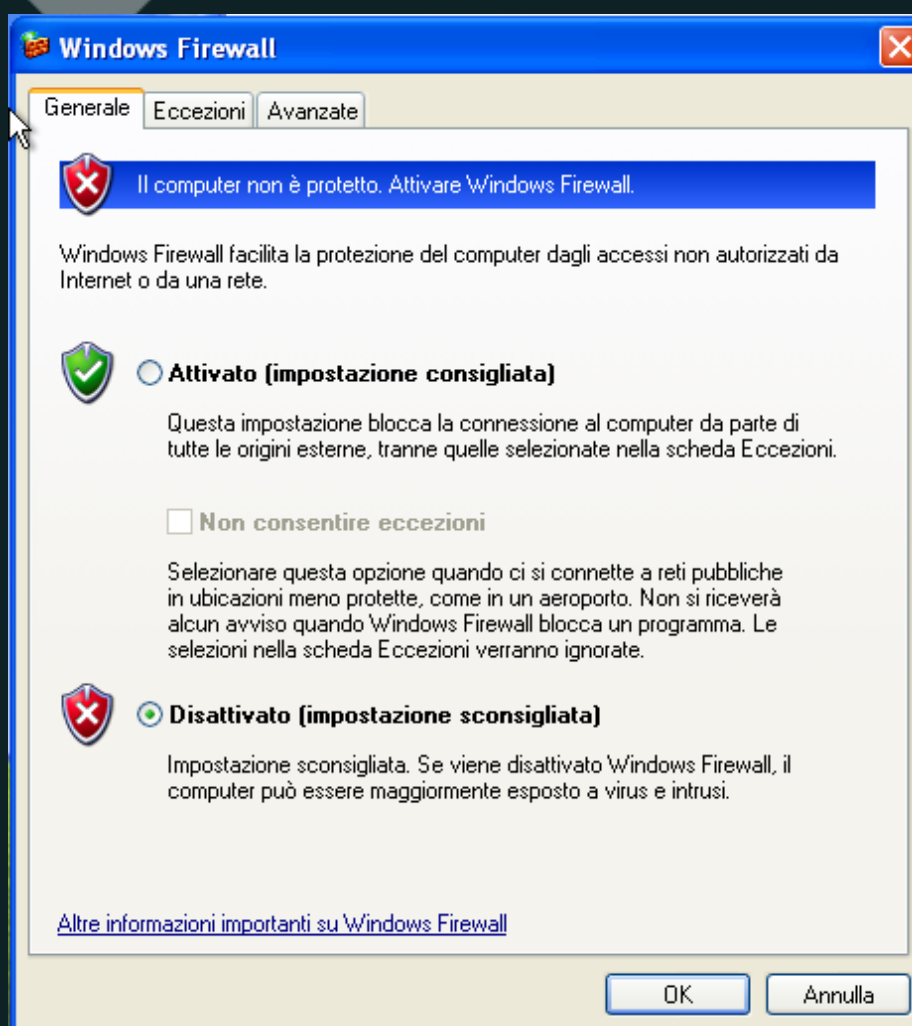
Fatto ciò colleghiamo le macchine a questa rete e proviamo il ping fra le macchine, se va a buon fine allora abbiamo eseguito tutti i passaggi in maniera corretta.

```
(kali㉿kali)-[~]  
$ ping 192.168.240.150  
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.  
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.788 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.600 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.00 ms  
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.894 ms  
^C  
— 192.168.240.150 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3028ms  
rtt min/avg/max/mdev = 0.600/0.821/1.003/0.148 ms
```



```
Prompt dei comandi  
Microsoft Windows XP [Versione 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\Documents and Settings\Administrator>ping 192.168.240.100  
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:  
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64  
Statistiche Ping per 192.168.240.100:  
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),  
Tempo approssimativo percorsi andata/ritorno in millisecondi:  
Minimo = 0ms, Massimo = 1ms, Medio = 0ms  
C:\Documents and Settings\Administrator>
```

**Una volta fatto ciò andiamo a verificare che il firewall di Windows XP sia disattivato, seguendo questi passaggi:
Start > Risorse del Computer > Risorse di rete > Visualizza connessioni di rete > Modifica impostazioni Windows Firewall:**



Prima Scansione:

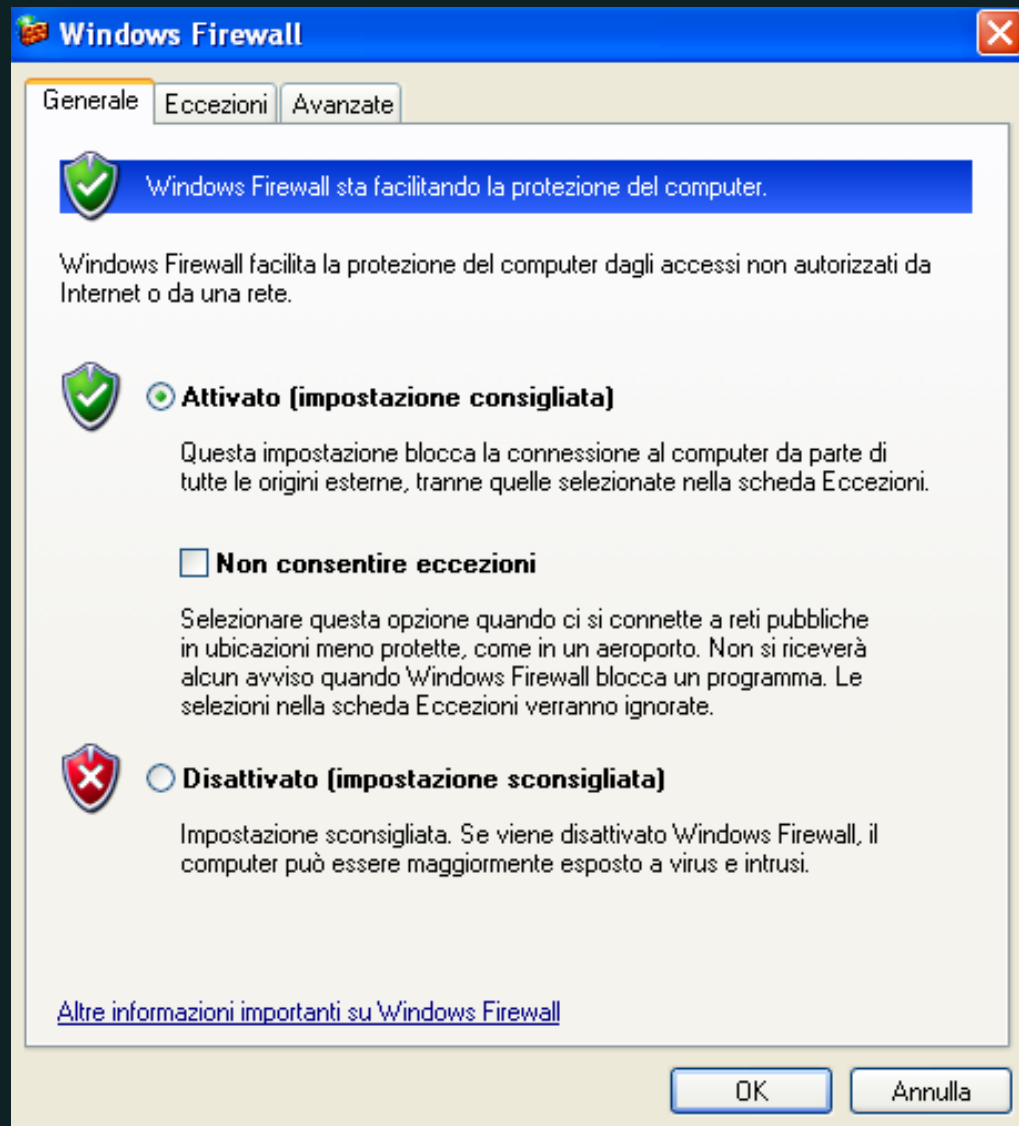
Come vediamo il Firewall è disattivato,
quindi procediamo con la prima scansione
Nmap da Kali a WindowsXP, questo è il
risultato:

```
$ nmap 192.168.240.150 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:03 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00037s 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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.55 seconds
```

Come vediamo, la scansione ci comunica che la
macchina Windows XP ha 3 porte aperte;
In questo modo un attaccante avrebbe già
parecchie informazioni per provare a sfruttare
qualche vulnerabilità della macchina.

Adesso, attiviamo il firewall nella macchina Windows XP:



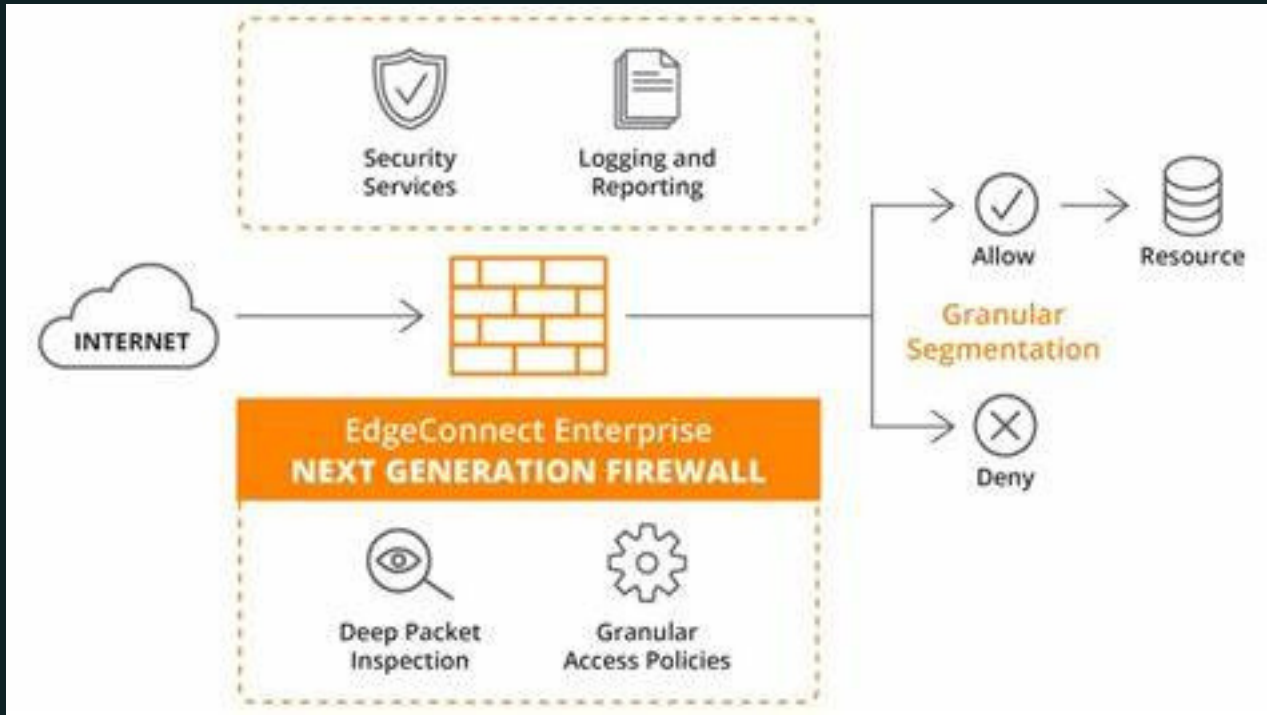
Una volta attivato, proviamo a effettuare una nuova scansione con Nmap, per vedere quanto effettivamente sia fondamentale un firewall a protezione delle nostre macchine:

```
(kali㉿kali)-[~]  
$ nmap 192.168.240.150 -sV -Pn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:06 EDT  
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 9.00% done; ETC: 07:09 (0:03:12 remaining)  
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 32.50% done; ETC: 07:09 (0:02:17 remaining)  
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 63.00% done; ETC: 07:09 (0:01:15 remaining)  
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 77.50% done; ETC: 07:09 (0:00:46 remaining)  
Stats: 0:03:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 95.50% done; ETC: 07:09 (0:00:09 remaining)  
Nmap scan report for 192.168.240.150  
Host is up.  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 201.61 seconds
```

Come possiamo vedere, il tool riporta “All 1000 scanned ports are in ignored states”, come se le 1000 porte scansionate fossero chiuse, anche se sappiamo che non è così!

Il firewall ha bloccato un tentativo di Information Gathering Attivo!

Ma quindi, cos'è e cosa fa un Firewall (NGFW)?



I firewall definiscono i confini della rete. Tutto il traffico che passa attraverso un NGFW viene ispezionato da quel firewall. Questa ispezione consente al firewall di applicare regole di politica di sicurezza che consentono o bloccano il traffico.

Un NGFW si basa sulle capacità di un firewall tradizionale, incorporando funzionalità aggiuntive.

Per esempio, un NGFW opera a livello di applicazione dello stack TCP/IP per applicare intrusion Prevention System (IPS), antimalware, sandboxing e altre protezioni. Queste funzioni consentono a un NGFW di identificare e bloccare le minacce avanzate prima che rappresentino un rischio per i sistemi aziendali.

Grazie



Report by:

Giuseppe Pignatello