

**EVILCORP**

IF IT WORKS DONT TOUCH IT

# REPORT

BY EVILCORP

Scritto da: Andrea Di Benedetto

Graphic Designer: Lorenzo Franchi

Direttore Tecnico: Samuele Aversa

Approvato da: Mario Reitano

Giugno 2024

# INDICE S9

## L0 .....

Chi siamo .....  
Missione e Visione Aziendale .....  
Team Group .....  
Regole di Ingaggio.....  
I Nostri Prezzi.....

## L1 .....

Introduzione .....  
Obiettivo .....  
Configurazione VM .....  
V.A. con Firewall Disattivato .....  
V.A. con Firewall Attivato .....  
Conclusioni .....



# Chi siamo

**Nome Azienda:** EvilCorp

**Settore:** Amministrazione

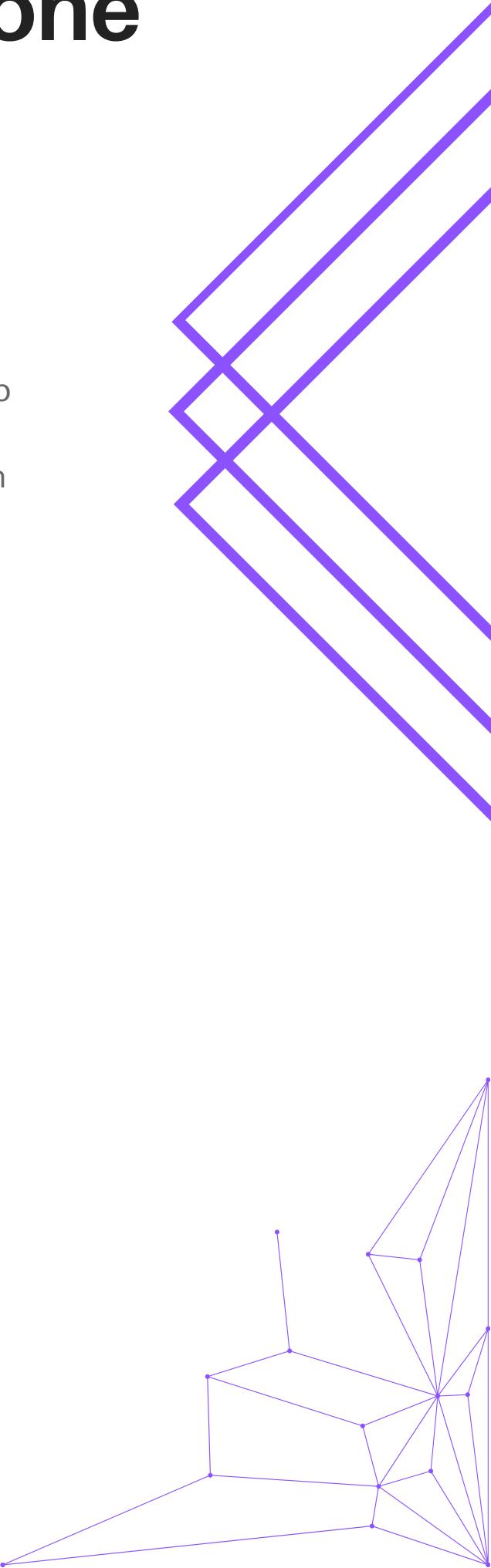
## Descrizione dell'Azienda

EvilCorp è un'azienda immaginaria che si occupa di amministrazione. EvilCorp fornisce servizi di amministrazione per altre aziende, gestendo dati sensibili e informazioni riservate. La sicurezza delle loro reti e dei loro dati è cruciale per mantenere la fiducia dei loro clienti e rispettare le normative.



# Missione e visione aziendale

Come parte del nostro impegno per garantire la sicurezza informatica, EvilCorp ha incaricato un team di pentester di eseguire un Vulnerability Assessment e un Penetration Testing della rete aziendale. Questo report descrive il processo e le regole di ingaggio, nonché una bozza dei costi operativi.



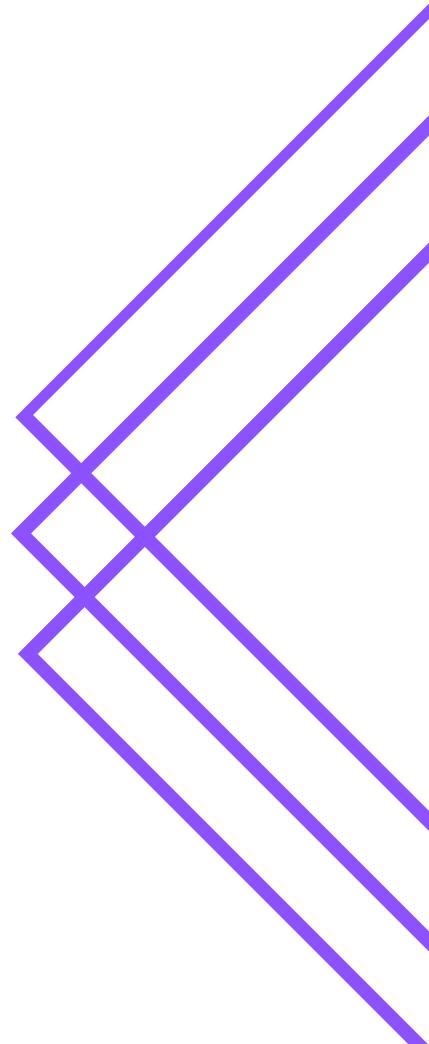
# Regole di ingaggio

Le regole di ingaggio definiscono i limiti e le aspettative del nostro lavoro di pentesting. Di seguito sono riportate le regole stabilite per questo incarico:

- 1. Autorizzazione:** EvilCorp ha fornito l'autorizzazione scritta per eseguire la scansione e i test di penetrazione sulla loro rete.
- 2. Scopo del Test:** Le scansioni verranno effettuate solo sugli indirizzi IP forniti dall'azienda.
- 3. Preventivo:** Viene stilato un preventivo del lavoro completo.
- 4. Perimetro d'azione:** Si determina l'area della rete aziendale su cui effettuare i test.
- 5. Ore di Lavoro:** Il team lavorerà dalle 9:00 alle 17:00, dal lunedì al venerdì.
- 6. Impatto sul Sistema:** I test saranno condotti in modo da minimizzare qualsiasi impatto sui sistemi di produzione.
- 7. Riservatezza:** Tutte le informazioni raccolte durante il test saranno mantenute riservate e utilizzate solo ai fini del test.
- 8. Strumenti:** Si presentano gli strumenti utilizzati dai pentester per effettuare l'analisi di rete.

# Team Group

Siamo un piccolo team di quattro professionisti, ognuno con una solida esperienza nel campo della cybersecurity. La nostra combinazione di competenze specifiche ci permette di affrontare efficacemente le sfide del settore, assicurando soluzioni innovative e sicure per proteggere al meglio i nostri sistemi e dati.



## REFERENCE LINKEDIN

Cliccando sui nostri nomi sarete reindirizzati sulle nostre pagine linkedin



[Andrea  
Di Benedetto](#)



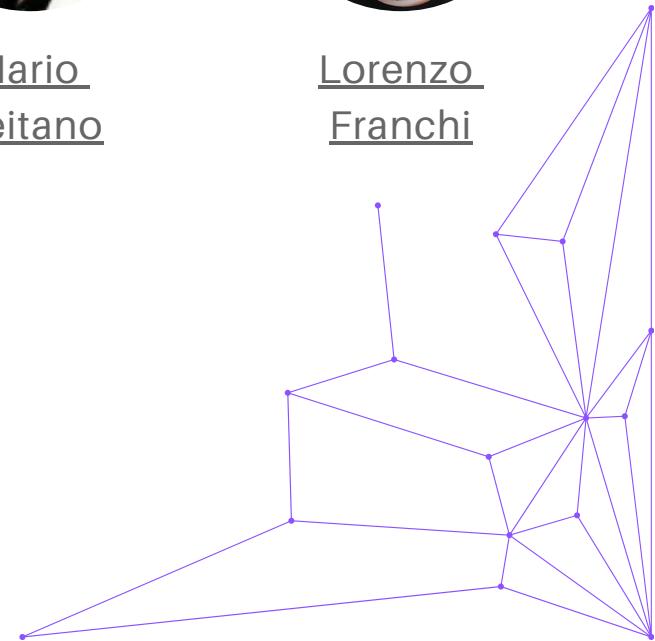
[Samuele  
Aversa](#)



[Mario  
Reitano](#)



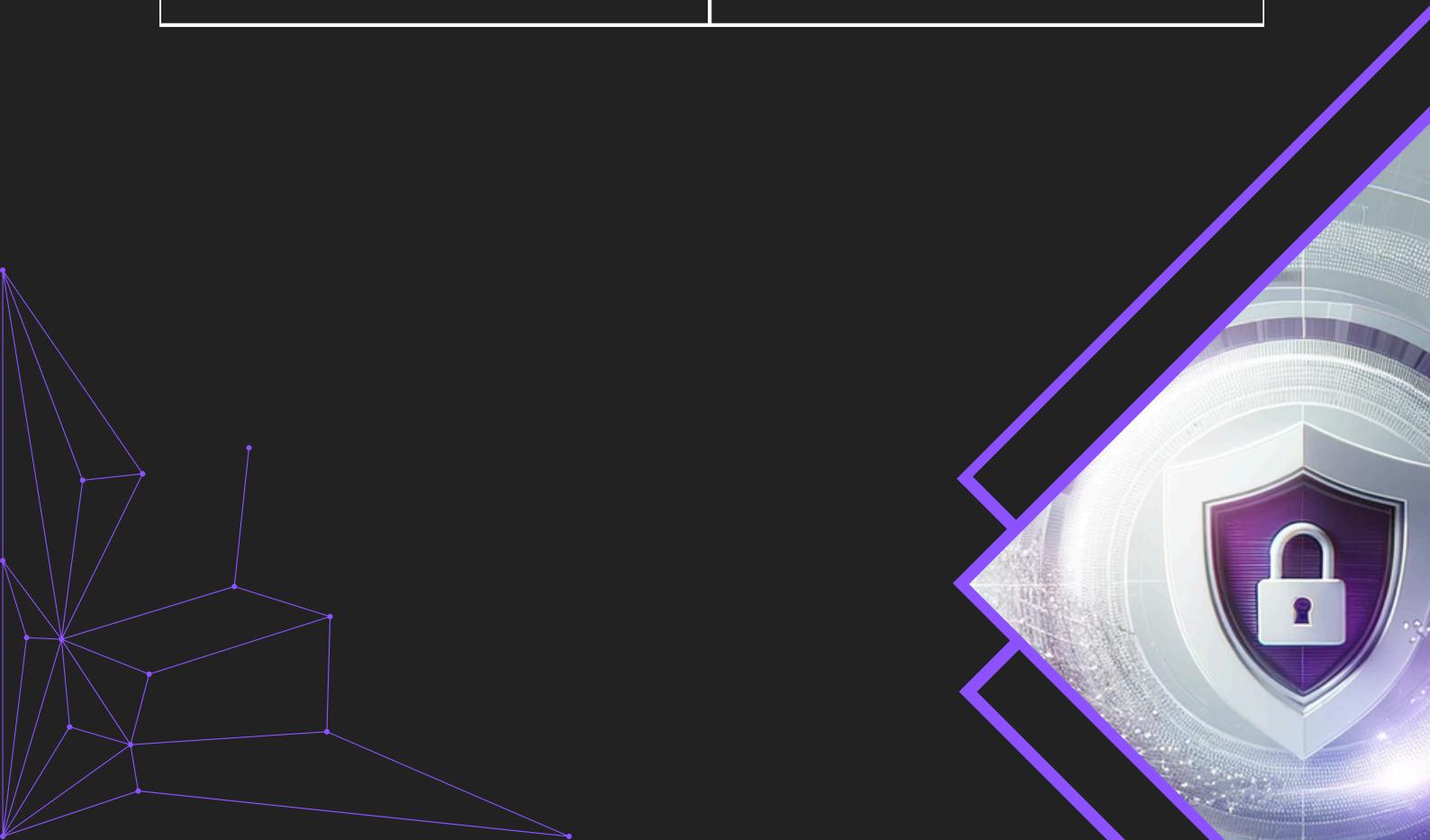
[Lorenzo  
Franchi](#)



# I Nostri Prezzi

Budget stimato per il progetto

<b>Analisi Vulnerabilità</b>	32.000 €
work	work
in	in
progress	progress

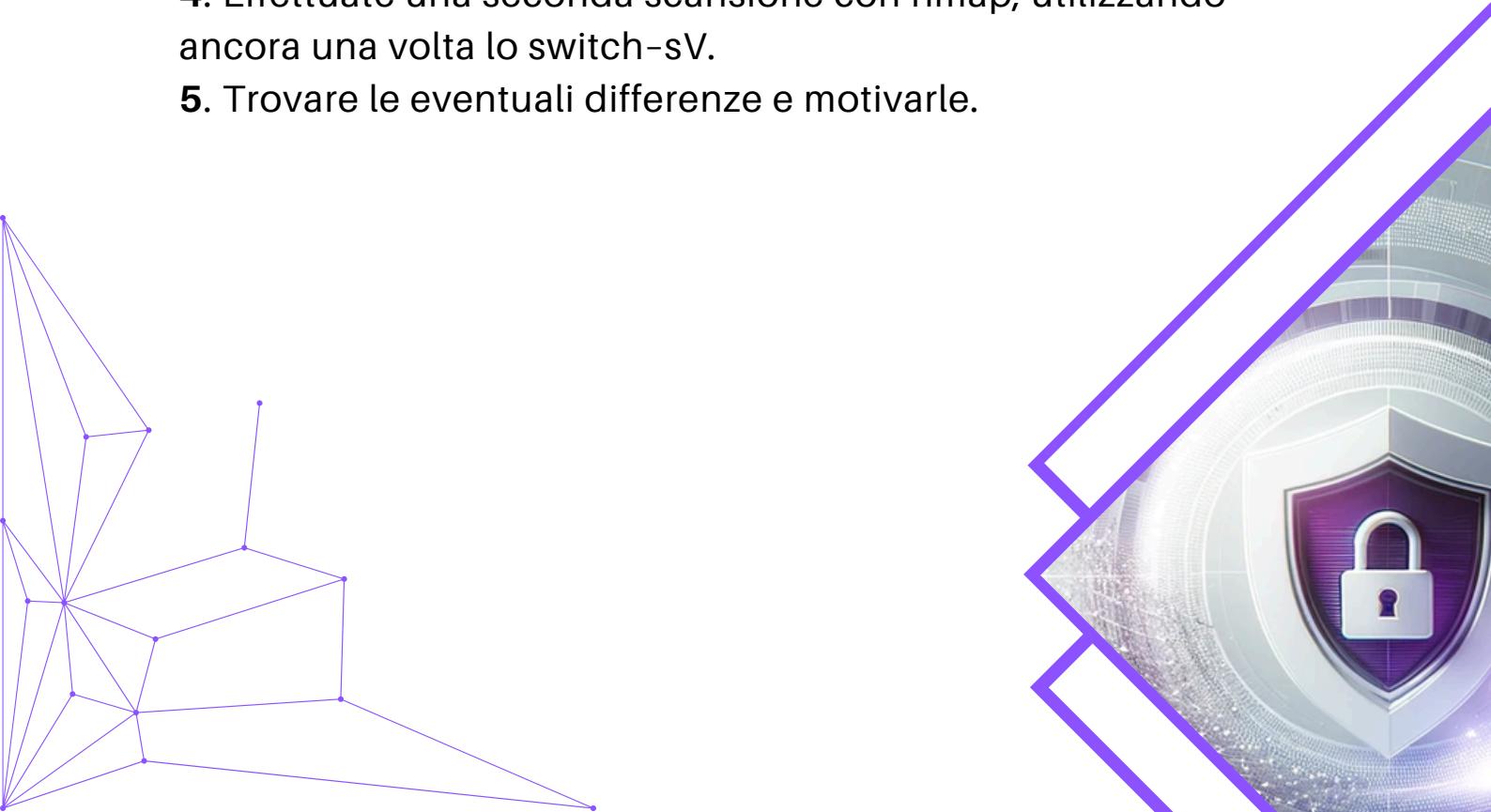


# L1

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:

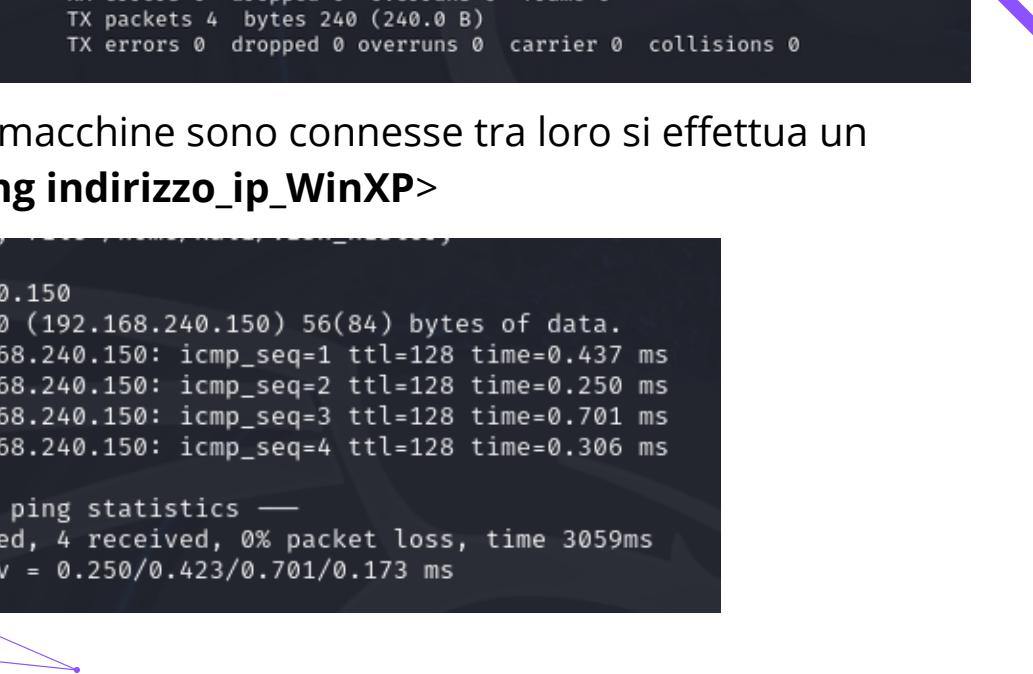
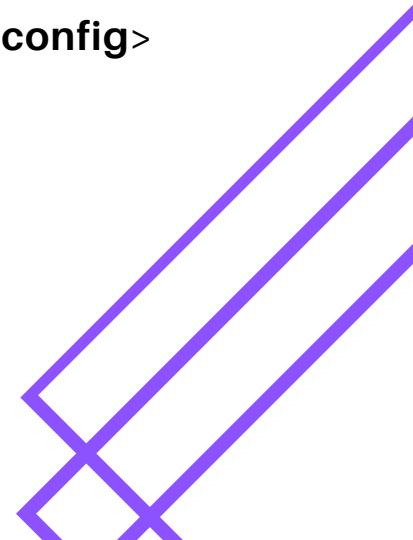
- 1.** Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
- 2.** Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch-sV, per la service detection e -o nomefilereport per salvare in un file l'output)
- 3.** Abilitare il Firewall sulla macchina Windows XP
- 4.** Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV.
- 5.** Trovare le eventuali differenze e motivarle.

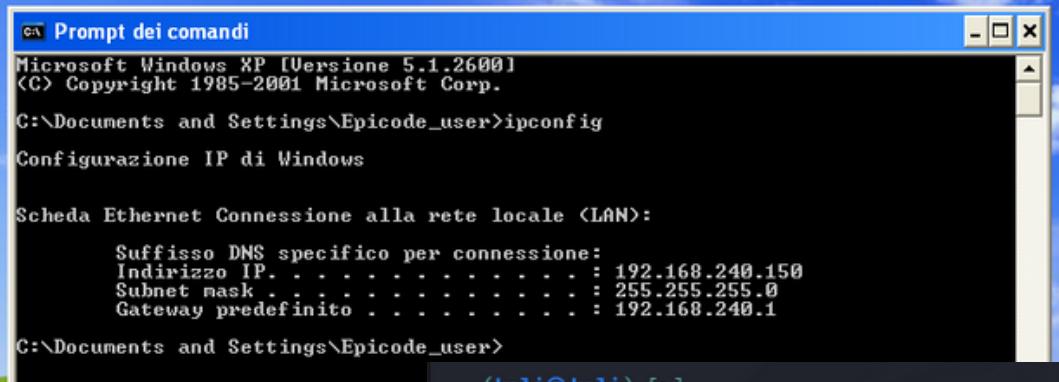


# Configurazione VM

Inizialmente si impostano gli indirizzi IP della macchina Kali e Windows XP rispettivamente a 192.168.240.100 e 192.168.240.150, così come richiesto dalla traccia. Per fare ciò si è andato a modificare il file interfaces al PATH /etc/network/ con il comando **<sudo nano /etc/network/interfaces>**.

Dopo aver fatto un reboot delle macchine, il comando **<ifconfig>** su Kali e il comando **<ipconfig>** su Windows XP dimostra l'effettivo cambio di indirizzi IP.





```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

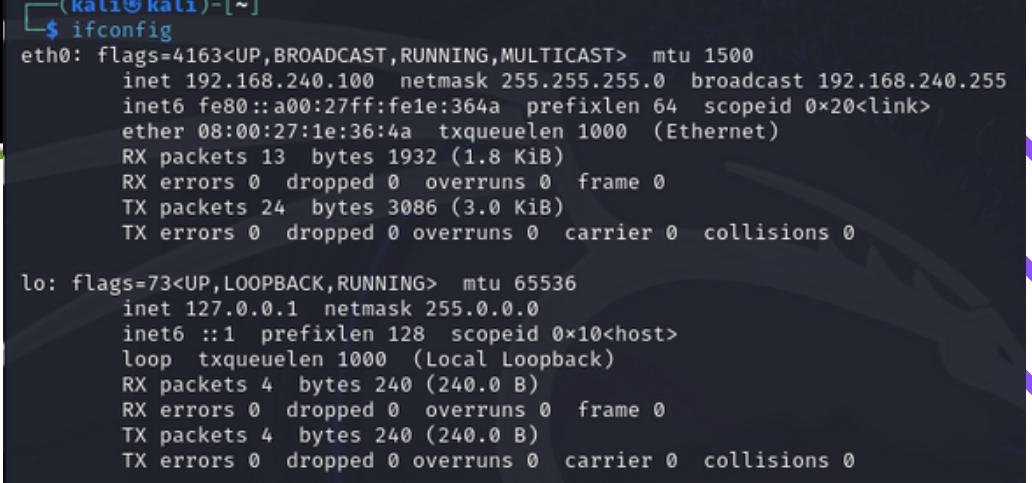
C:\Documents and Settings\Epicode_user>ipconfig

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

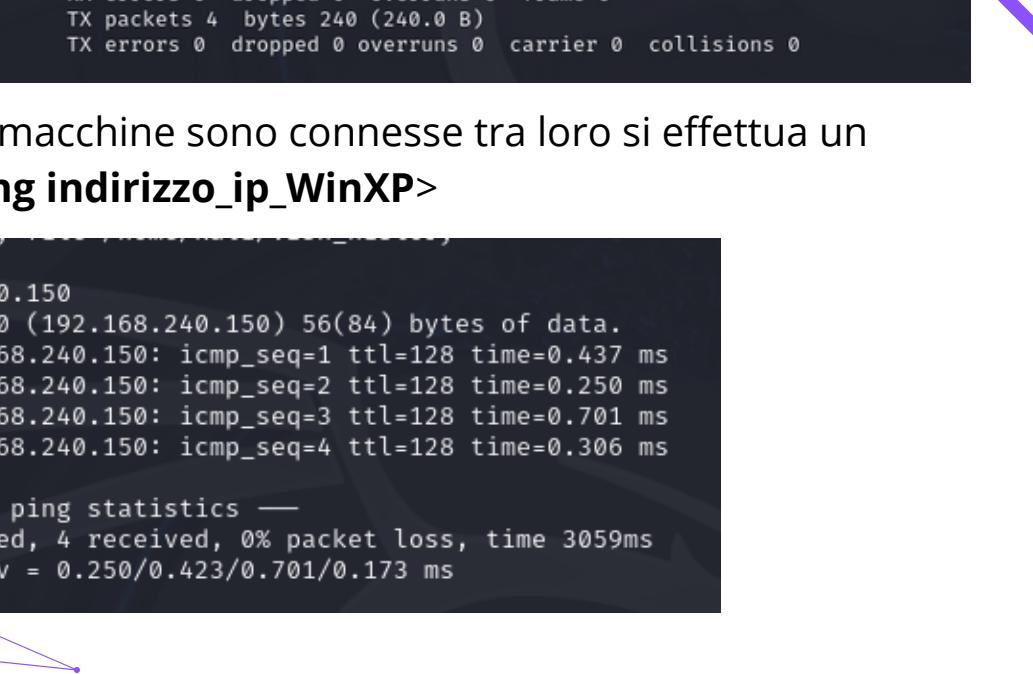
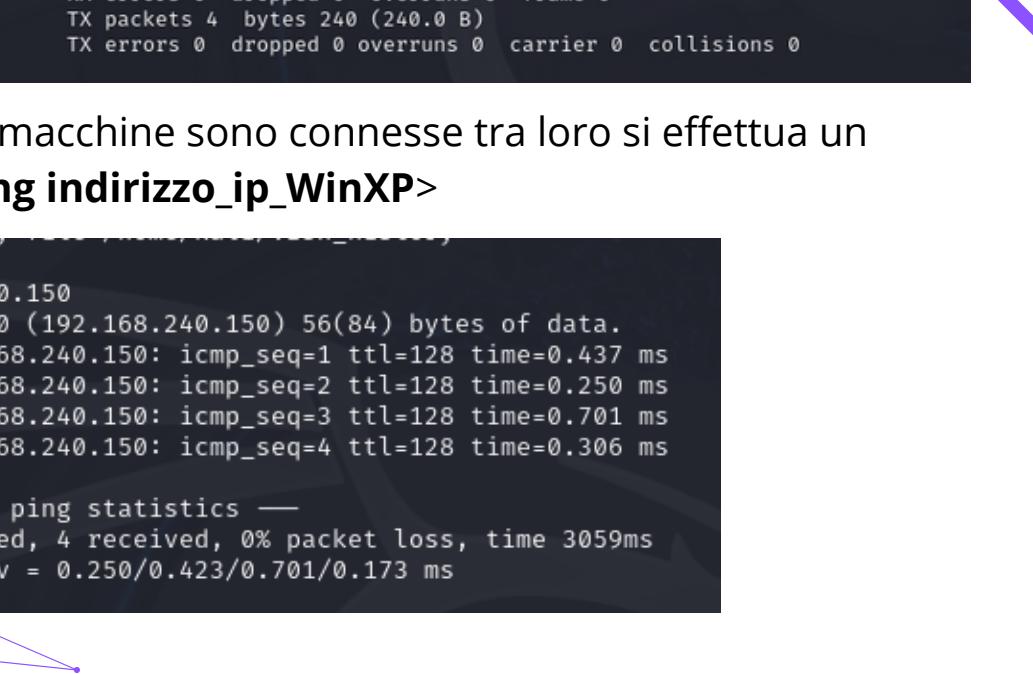
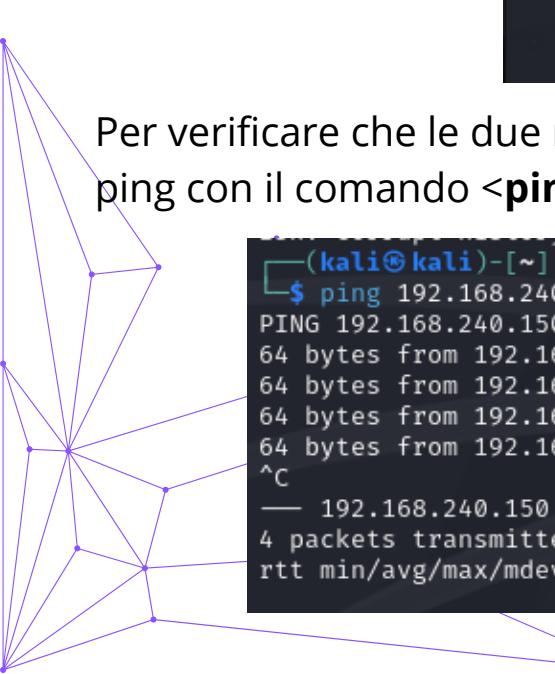
C:\Documents and Settings\Epicode_user>
```

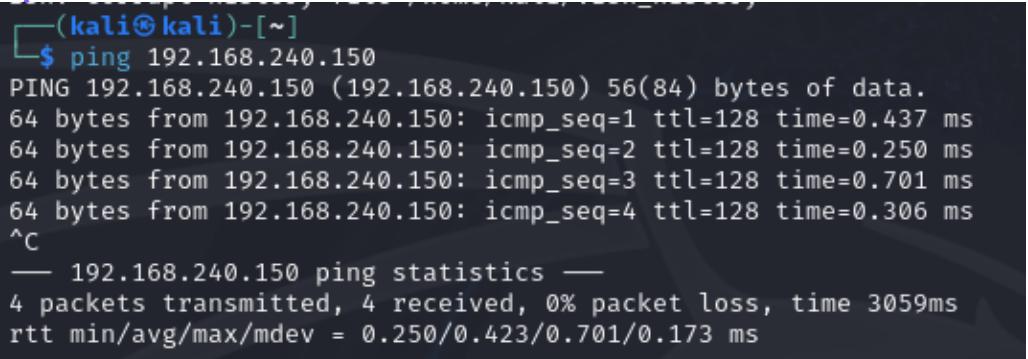


```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
        inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
            RX packets 13 bytes 1932 (1.8 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 24 bytes 3086 (3.0 KiB)
            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
```

Per verificare che le due macchine sono connesse tra loro si effettua un ping con il comando **<ping indirizzo\_ip\_WinXP>**



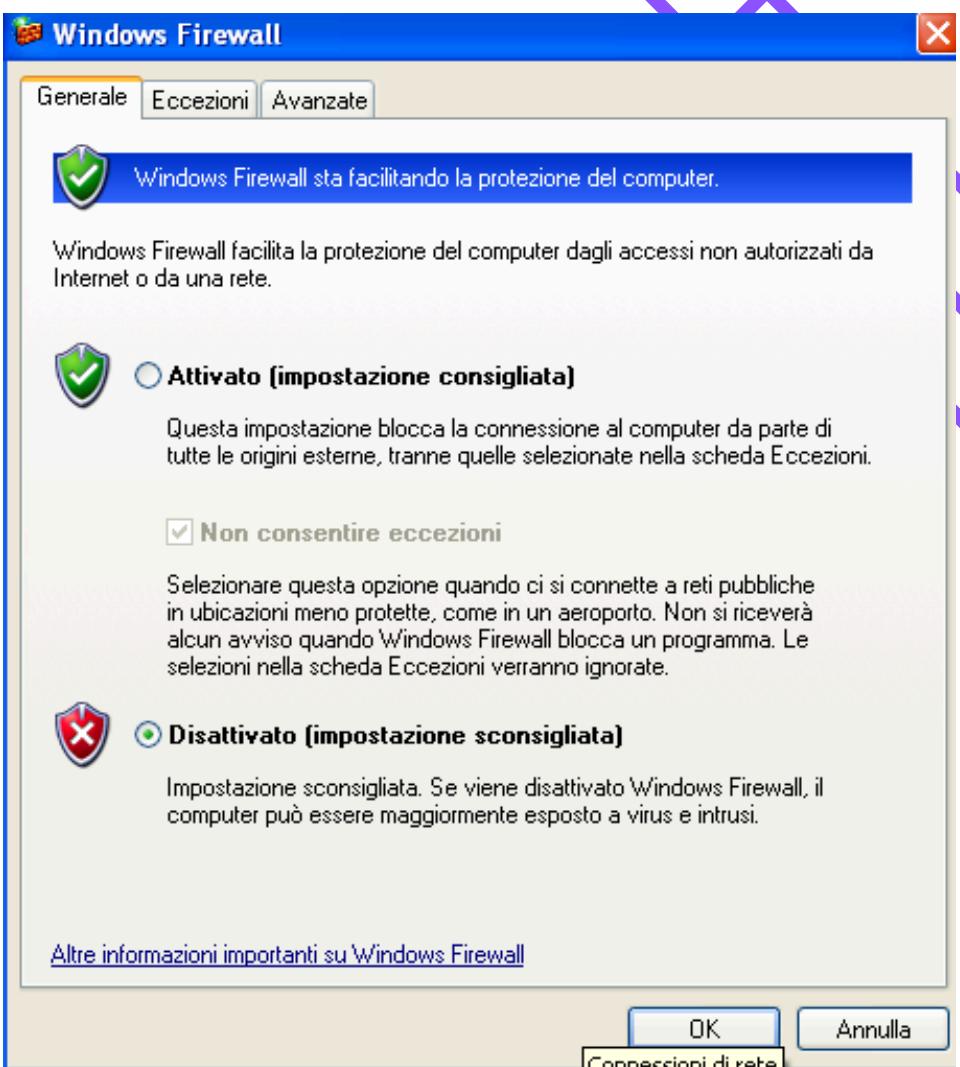


```
(kali㉿kali)-[~]
$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.437 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.250 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.701 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.306 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.250/0.423/0.701/0.173 ms
```

# V.A. con Firewall Disattivato

In questa fase viene disattivato il firewall di Windows XP per verificare la sua efficacia in caso di possibili attacchi provenienti dall'estero.

Il firewall di Windows XP è una funzionalità di sicurezza integrata nel sistema operativo progettata per monitorare e controllare il traffico di rete in entrata e in uscita. Funziona bloccando le connessioni non autorizzate e permettendo solo quelle che sono esplicitamente consentite dall'utente o dai programmi installati, contribuendo a proteggere il computer da accessi non autorizzati e attacchi esterni.



# V.A. con Firewall Disattivato

In questa fase viene disattivato il firewall di Windows XP per verificare l'efficacia in caso di possibili attacchi provenienti dall'esterno.

Questo permette di fare una scansione della rete dalla nostra macchina Kali utilizzando lo strumento nmap: con il comando `<nmap -sV indirizzo_ip_WinXP -o report_WinXP>` infatti si è potuta fare una scansione di tutte le porte e servizi attivi sulla macchina target WinXP.

`-sV` questa opzione permette di rilevare i servizi in esecuzione su ciascun host e di determinare le versioni specifiche di questi servizi.

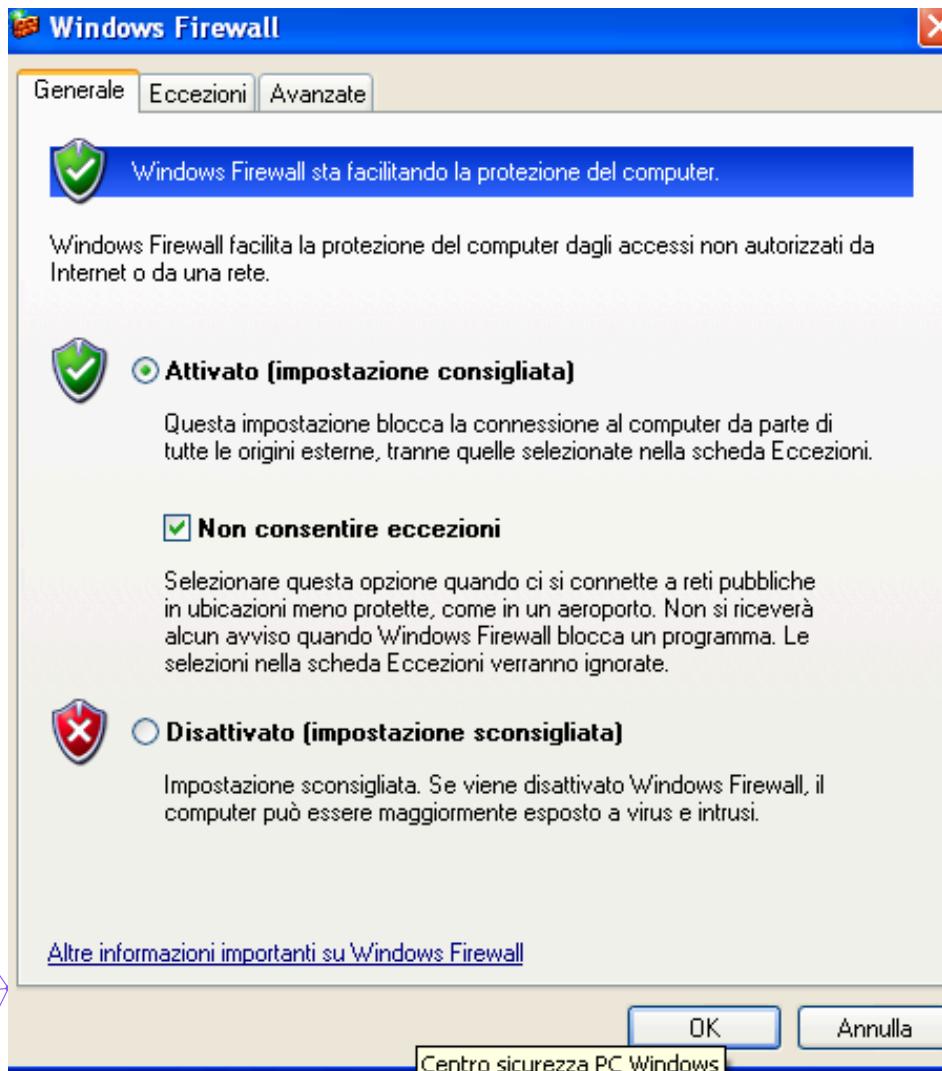
```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o report_winXP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:55 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        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 20.39 seconds
```

```
~/report_winXP - Mousepad
File Edit Search View Document Help
File Edit View Insert Document Help
1 # Nmap 7.94SVN scan initiated Mon Jun  3 10:55:45 2024 as: nmap -sV -o report_winXP
192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00027s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/
12 submit/ .
13 # Nmap done at Mon Jun  3 10:56:06 2024 -- 1 IP address (1 host up) scanned in 20.39 seconds
```

# V.A. con Firewall Attivo

Successivamente, per verificare l'efficacia del firewall si è rifatta una scansione della rete aziendale con quest'ultimo attivo. A livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.



# V.A. con Firewall Attivo

Quando si utilizza Nmap per scansionare un sistema Windows con il firewall attivo, i risultati mostrano in genere meno dettagli sulle porte a causa del blocco operato dal firewall. Durante queste scansioni, è comune trovare:

1. Porte chiuse o filtrate: La maggior parte delle porte viene bloccata dal firewall, risultando inaccessibili o mostrate come chiuse da Nmap.
2. Ritardi nella scansione: Il firewall può causare ritardi o ignorare completamente i pacchetti di scansione, influenzando la velocità e l'efficacia di Nmap.
3. Errori e avvisi: Nmap potrebbe segnalare errori indicando che le porte sono filtrate, suggerendo che il firewall sta impedendo l'accesso.
4. Informazioni limitate sui servizi: Le informazioni raccolte dalle porte aperte sono spesso ridotte, limitando la visibilità dei servizi in esecuzione.
5. False Positivi: Il firewall può causare falsi positivi, facendo apparire alcune porte come chiuse o filtrate anche quando non lo sono.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o report_winXP_firewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 11:05 CEST
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 3.11 seconds
```



# Conclusioni

In conclusione, la scansione Nmap eseguita su un sistema Windows ha rivelato differenze significative nei risultati a seconda dello stato del firewall. Con il firewall disattivato, la scansione ha identificato un numero maggiore di porte aperte e servizi attivi, suggerendo una superficie di attacco più ampia e potenziali vulnerabilità accessibili.

Al contrario, con il firewall attivato, la scansione ha mostrato un numero significativamente ridotto di porte aperte, indicando una protezione più robusta contro accessi non autorizzati. La presenza del firewall ha dimostrato la sua efficacia nel filtrare il traffico di rete e nel proteggere il sistema da potenziali attacchi.

Questi risultati sottolineano l'importanza di mantenere attivo il firewall come componente essenziale della sicurezza di rete. Il confronto tra le due scansioni evidenzia chiaramente il ruolo critico del firewall nella protezione delle risorse del sistema e nel mantenimento dell'integrità e della riservatezza dei dati.