



S9 / L1

# SECURITY OPERATION

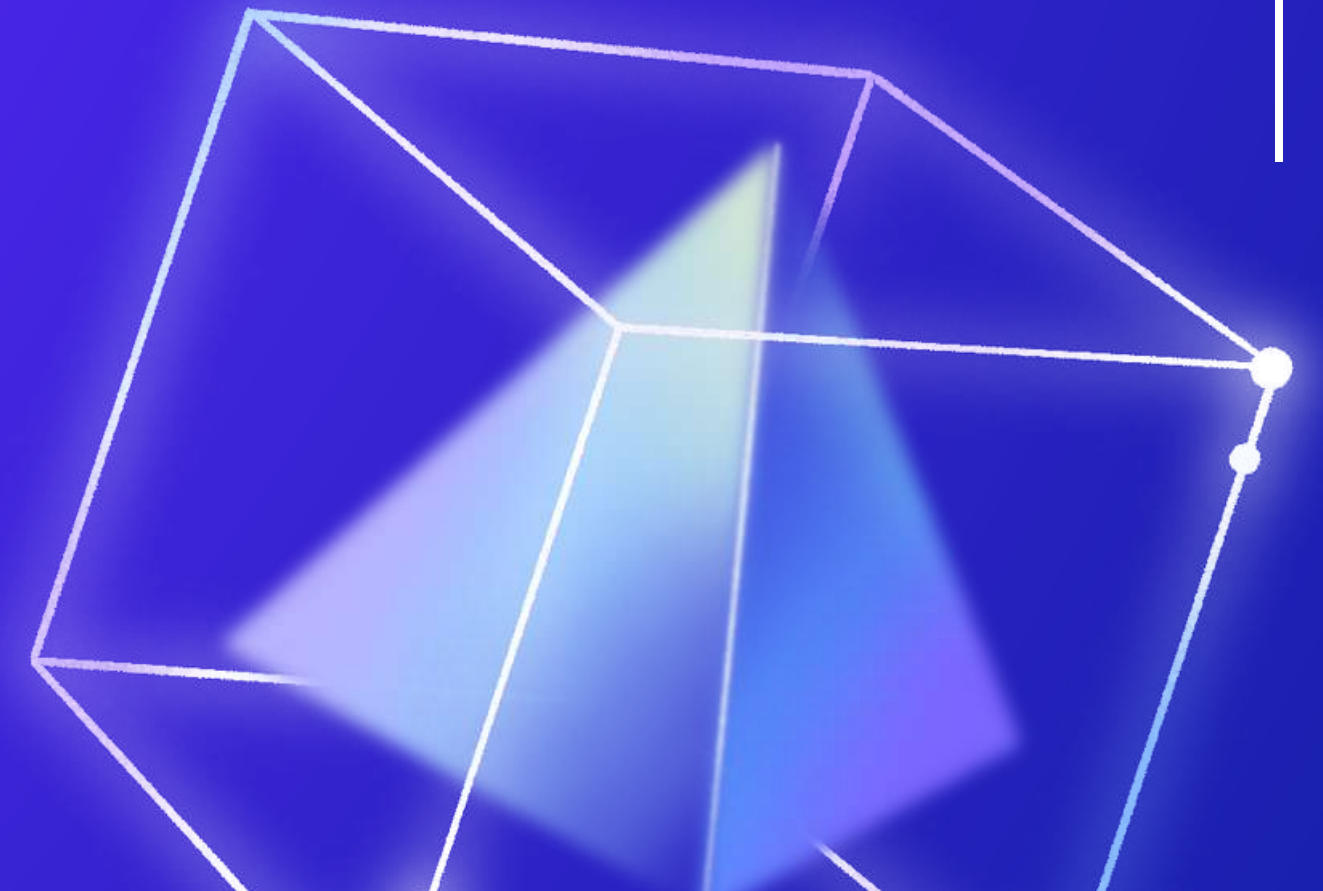
Riccardo Agostino Monti





# INDICE

• Scopo del test	01
• Requisiti	02
• Prima scansione	03
• Seconda scansione	04
• Considerazioni finali	05





# SCOPO DEL TEST





# SCOPO DEL TEST

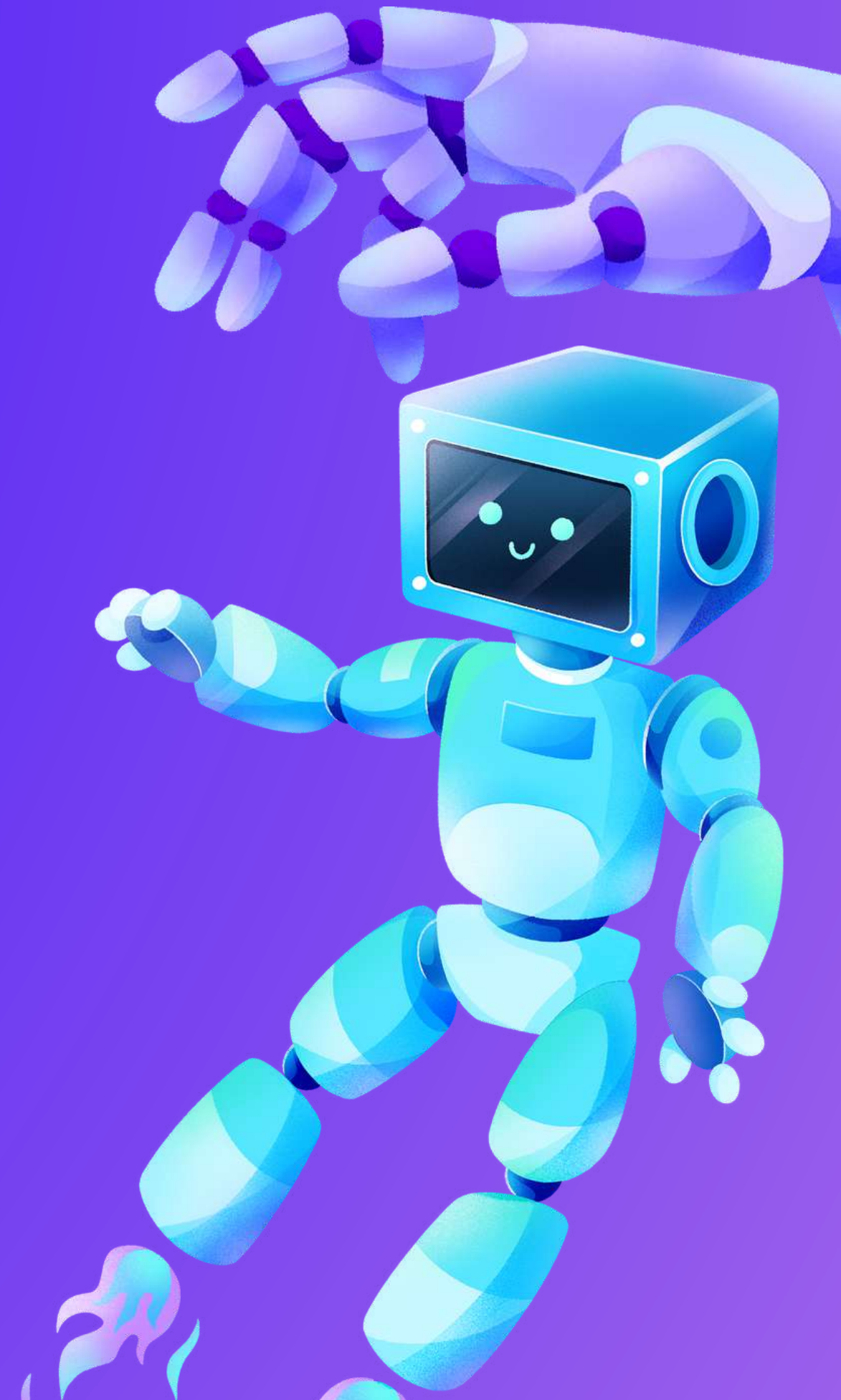
L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. E quindi, quanto l'uso di un firewall possa essere importante per ridurre la possibilità di attacco utilizzandolo come azione preventiva. Per farlo utilizzeremo nMap per capire le differenze. Eseguiamo quindi 2 scan, la prima col firewall di Win XP disattivato, la seconda con il Firewall Attivo

---

## Requisiti:

Configurare l'indirizzo di Windows XP come di seguito: 192.168.240.150

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





# REQUISITI





A photograph showing a person's hand reaching out towards a robotic arm. The robotic arm has a complex, articulated structure with multiple joints and segments, some of which are illuminated with red light. The background is dark and out of focus.

# CONFIGURAZIONE DI RETE

Per l'esecuzione del test di oggi ci viene richiesto di cambiare gli indirizzi ip delle nostre macchine del laboratorio.

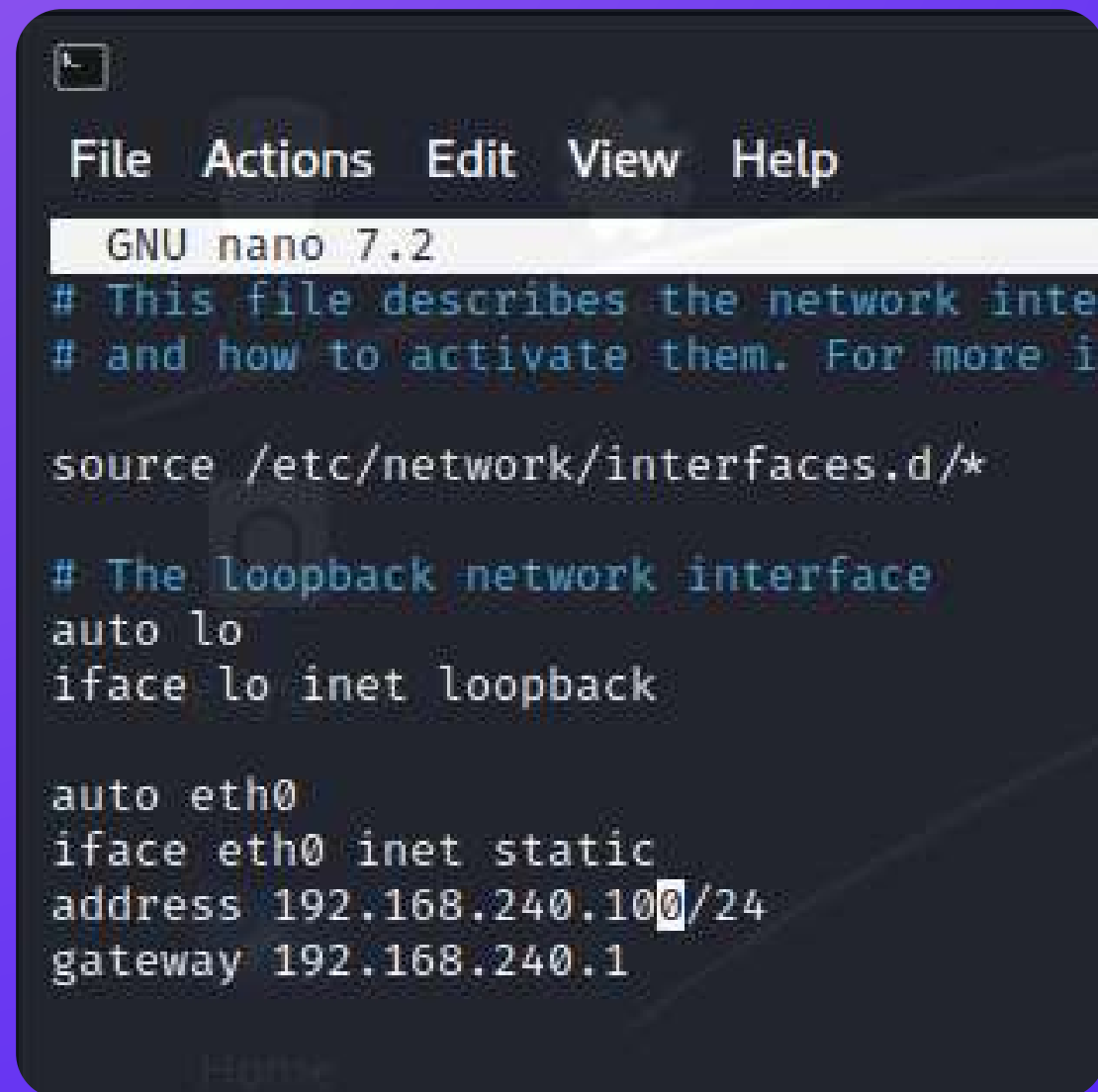


# SETUP KALI LINUX

Per la configurazione di kali linux basta lanciare sul terminale il comando:

```
<< sudo nano /etc/network/interfaces >>
```

E modificare il file come in immagine. Salviamo le modifiche con la combinazione CTRL+O (Ci verrà richiesto di confermare, premiamo Y) e successivamente chiudiamo il file con la combinazione CTRL+X a questo punto, riavviamo la macchina per ultimare la configurazione



```
File Actions Edit View Help
GNU nano 7.2
# This file describes the network interface
# and how to activate them. For more infor
source /etc/network/interfaces.d/*

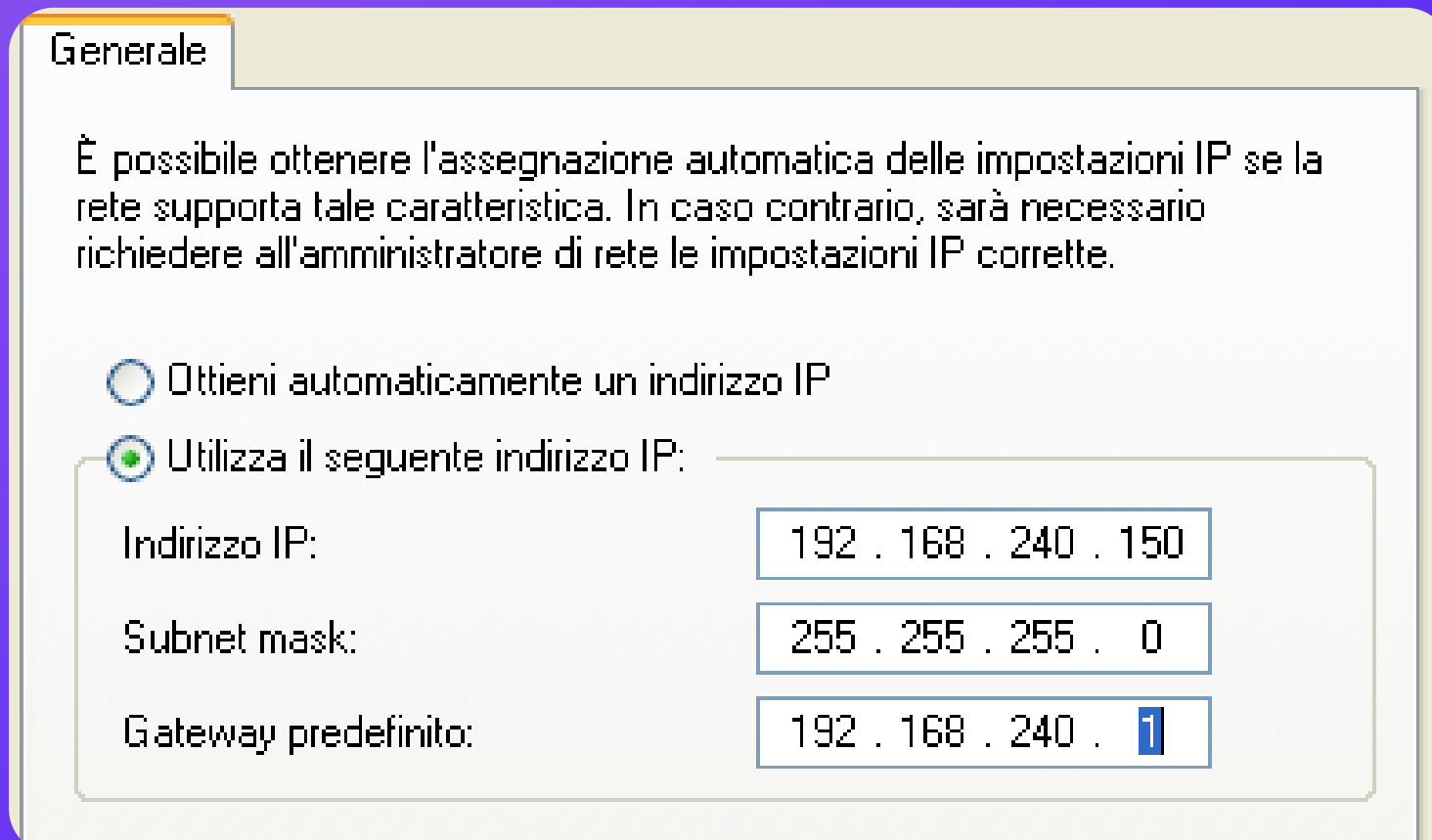
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.10/24
gateway 192.168.240.1
```





# SETUP WINDOWS XP



Generale

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP:	192 . 168 . 240 . 150
Subnet mask:	255 . 255 . 255 . 0
Gateway predefinito:	192 . 168 . 240 . 1

Per la configurazione di Windows XP seguire i seguenti passi:

1. Clicca su Start --> Pannello di controllo
2. Clicca su Connessione di Rete. Se non presente, clicca su "Passa alla Visualizzazione Classica a sinistra"
3. Selezione "Connessione alla rete locale (Lan)", premi il tasto destro del mouse, quindi clicca su Proprietà
4. Seleziona "Protocollo Internet (TCP/IP) e clicca su Proprietà.
5. Modifica la configurazione come in immagine e conferma.





```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

# CONTROLLO CONNETTIVITÀ

A questo punto eseguiamo un ping da una delle due macchine verso l'altra. Se il ping restituisce i pacchetti significa che le due macchine comunicano. Come si vede in immagine tutto è stato configurato correttamente





# PRIMA SCANSIONE





# PRIMO SCAN

Dopo che ci siamo assicurati che tutto sia configurato correttamente lanciamo il comando:

```
<< nmap -sV 192.168.240.150 >>
```

Per lanciare la scansione.

La prima scansione ha rivelato che sono presenti servizi attivi sulle porte 135 , 139, 445, tutte porte che utilizzano il protocollo TCP e utilizzano servizi di Microsoft.

```
(kali@kali) - [~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29  
Nmap scan report for 192.168.240.150  
Host is up (0.0038s 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_xp  
  
Service detection performed. Please report any incorrect results  
to https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 20.17 s
```





# SECONDA SCANSIONE





# CONSIDERAZIONI FINALI

01

La seconda scansione non è andata a buon fine, da questo possiamo intuire che il Firewall di Win XP abbia qualche tipo di regola che blocca questo tipo di scansione da un Host non autorizzato. In questo modo un attaccante non avrà modo di percepire porte e servizi aperti da sfruttare per attaccare il bersaglio. Con l'attivazione del Firewall abbiamo quindi eseguito un'azione preventiva che ha bloccato la nostra scansione. E quindi buona pratica attivare sempre un firewall per proteggersi.