

S9 L1

Report esercizio “Security Operation: azioni preventive”

Giulia Salani

INDICE

TRACCIA	2
REPORT	3
1. PREPARAZIONE AMBIENTE DI LAVORO	3
1.1 COMPOSIZIONE AMBIENTE	3
1.2 OBIETTIVO	3
1.3 ISTRUZIONI PASSO A PASSO	3
1.3.1 IMPOSTAZIONE IP KALI LINUX	4
1.3.2 IMPOSTAZIONE IP WINDOWS	5
1.3.3 VERIFICA DELLA COMUNICAZIONE FRA LE MACCHINE	8
2. SCANSIONE CON NMAP	9
2.1 DEFINIZIONE	9
2.2 OBIETTIVO	9
2.3 ISTRUZIONI PASSO A PASSO	9
2.3 SCANSIONE CON FIREWALL DISATTIVATO	9
2.3 SCANSIONE CON FIREWALL ATTIVO	12
3. ANALISI DELLE SCANSIONI EFFETTUATE CON NMAP	13
3.1 SCANSIONE VERSO WINDOWS XP CON FIREWALL DISATTIVATO	13
3.2 SCANSIONE VERSO WINDOWS XP CON FIREWALL ATTIVO	14
RIEPILOGO	15

TRACCIA

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`.

Che differenze notate?

E quale può essere la causa del risultato diverso?

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

REPORT

1. PREPARAZIONE AMBIENTE DI LAVORO

1.1 COMPOSIZIONE AMBIENTE

In questo progetto, le macchine coinvolte sono **Kali Linux** e **Windows XP**, rispettivamente **macchina attaccante** e **macchina target**.

1.2 OBIETTIVO

Poiché eseguiremo l'esercizio in modalità internal, affinché le macchine possano comunicare dovranno essere sulla stessa rete.

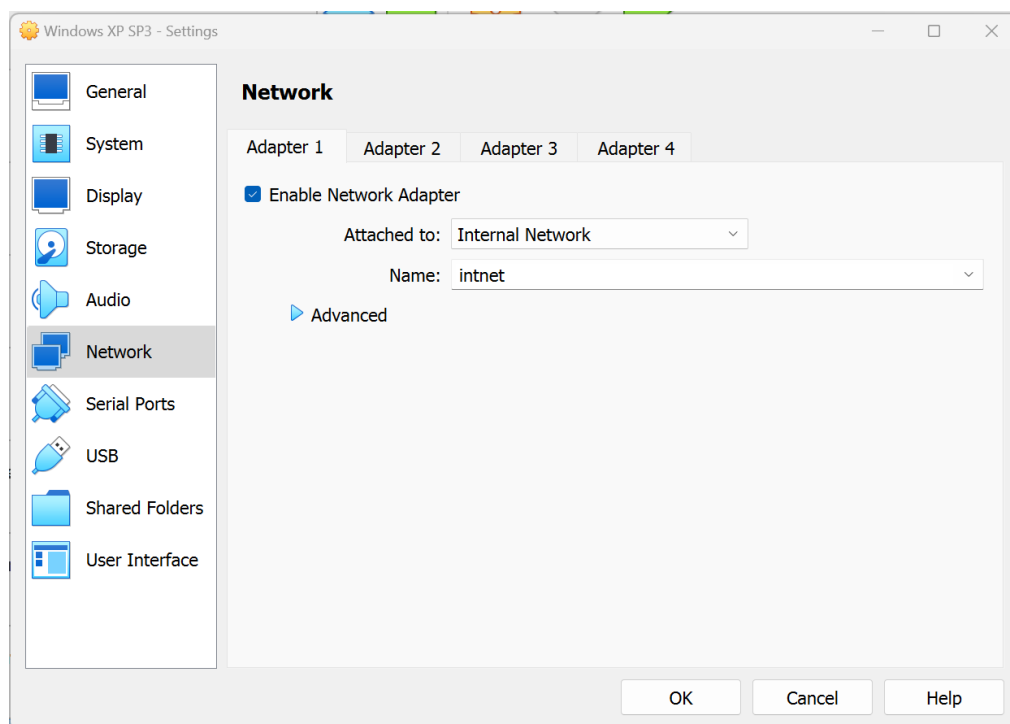
Seguendo quanto indicato in consegna, dobbiamo configurare sulle macchine i seguenti IP:

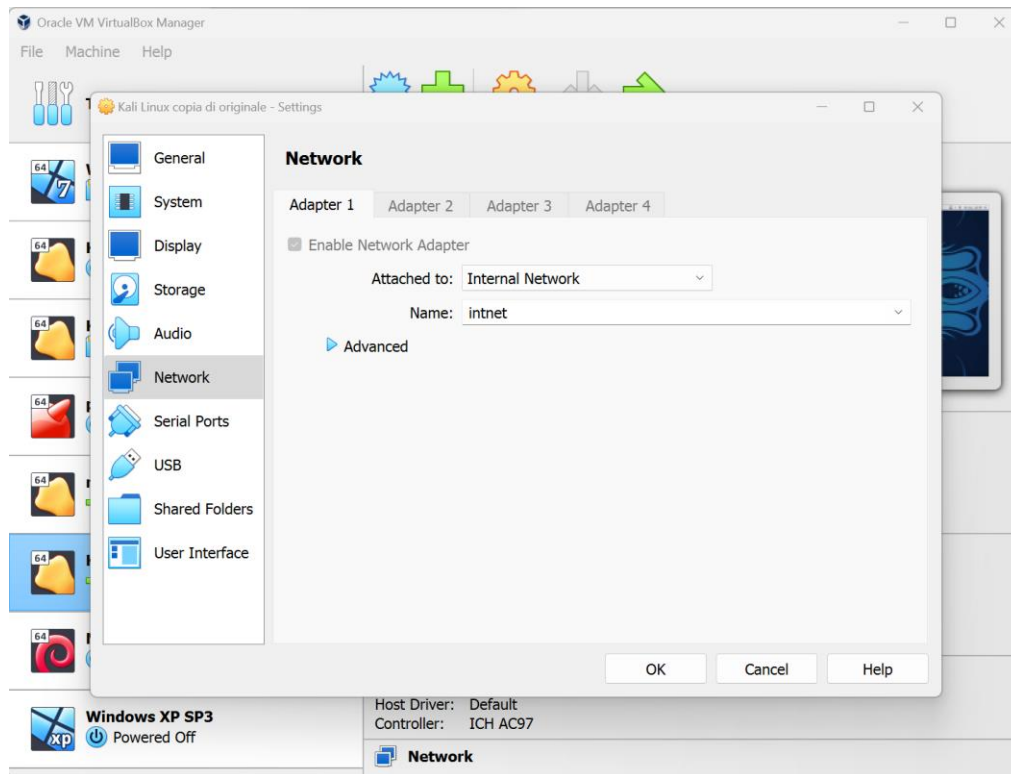
IP Kali → **192.168.240.100**

IP Windows XP → **192.168.240.150**

1.3 ISTRUZIONI PASSO A PASSO

Verifichiamo innanzitutto che le macchine siano configurate in modalità internal. Per farlo, apriamo Oracle VM Virtualbox Manager e controlliamo che la scheda NETWORK di entrambe le macchine sia impostata come segue:





Avuta questa conferma, avviamo le macchine.

1.3.1 IMPOSTAZIONE IP KALI LINUX

L'impostazione dell'IP avviene attraverso una modifica di **/etc/network/interfaces**, un **file di configurazione che definisce le impostazioni di rete** per le interfacce del sistema e che contiene informazioni come indirizzi IP, maschere di sottorete e gateway. Questo file viene utilizzato per configurare manualmente le connessioni di rete o specificare opzioni di configurazione. È possibile intervenire su questo file solo ottenuti i privilegi di root.

Lo apriamo con privilegi di root usando il seguente comando:

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nano /etc/network/interfaces
[sudo] password for kali: 
```

Seguendo il prompt del terminale, inseriamo la password ed entriamo nel file. Lo modifichiamo come nella figura seguente:

```

kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

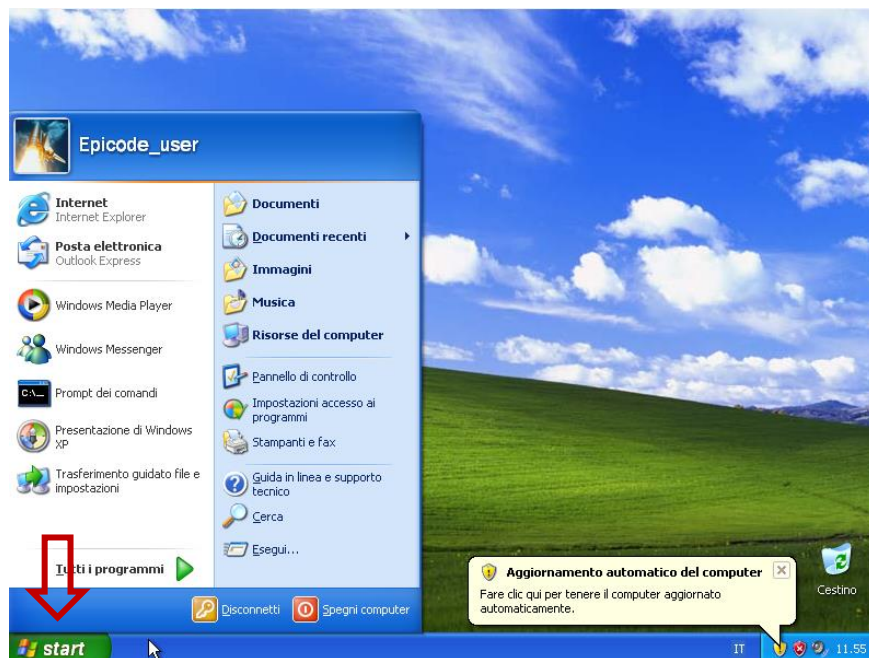
auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1

```

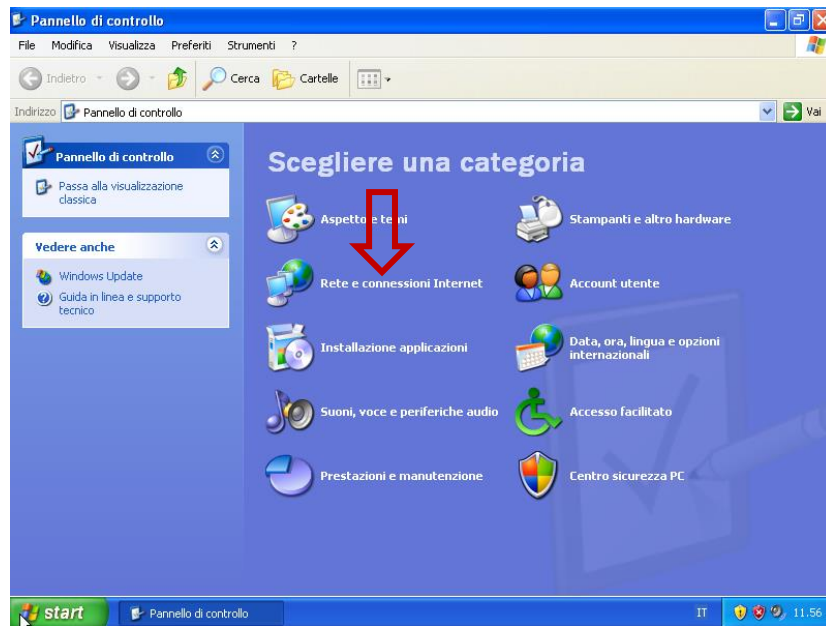
Per rendere effettiva la modifica, riavviamo la macchina.

1.3.2 IMPOSTAZIONE IP WINDOWS

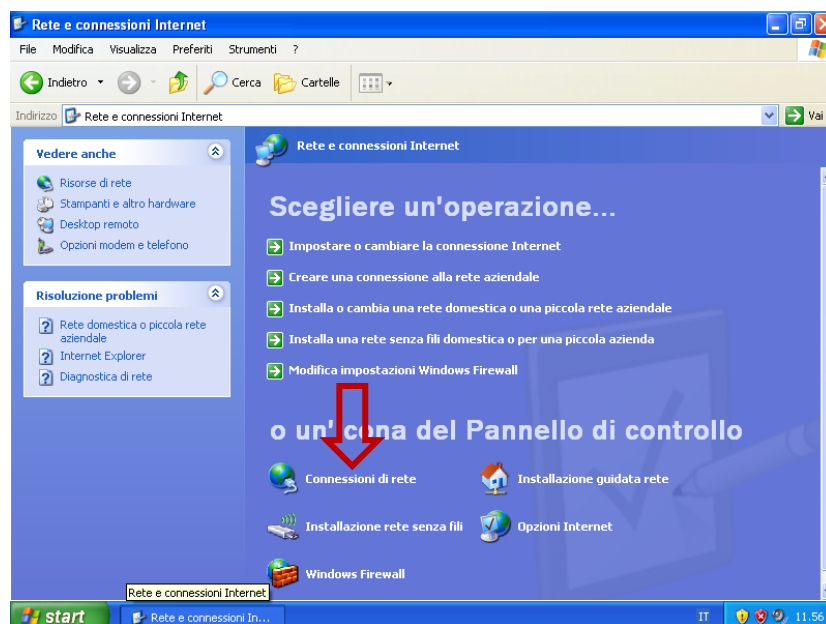
Clicchiamo su **Start**:



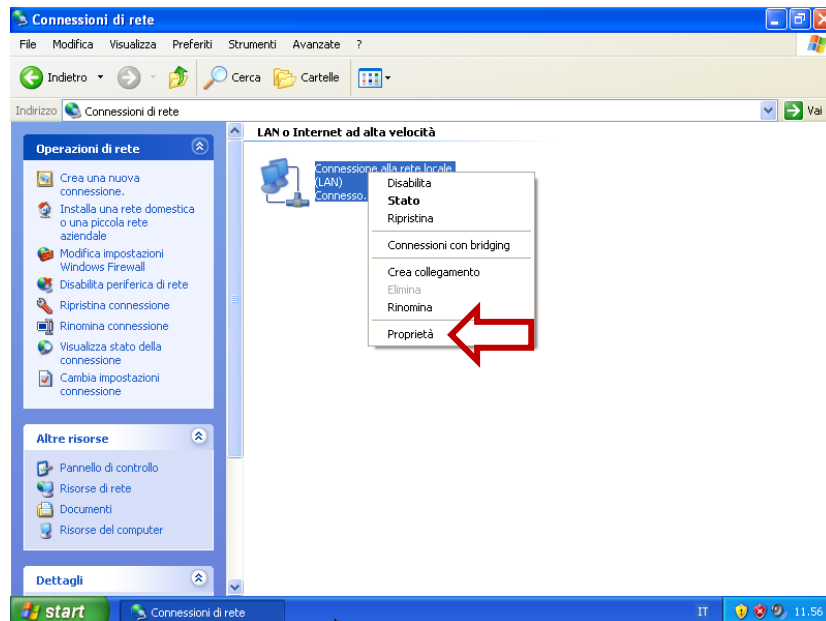
Scegliamo **Rete e connessioni di rete**:



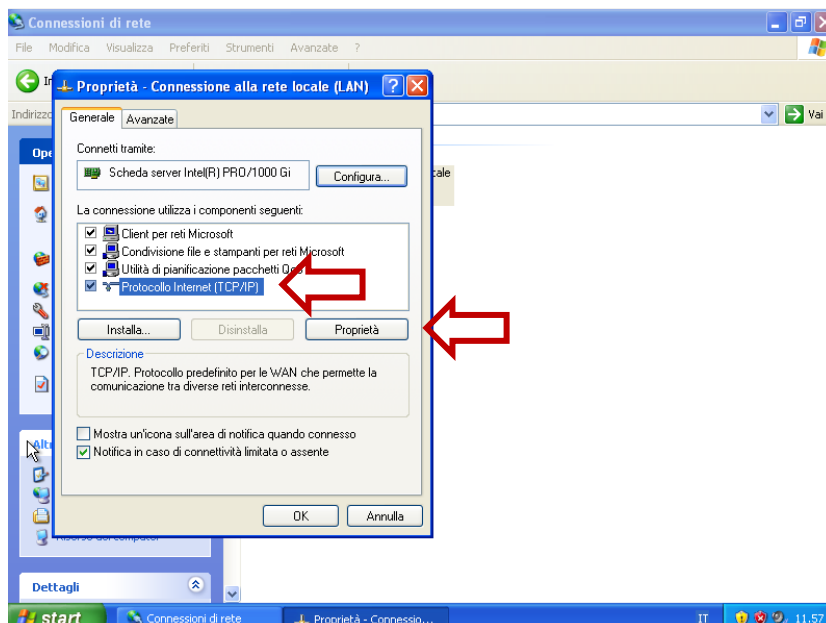
Scegliamo **Connessioni di rete**:



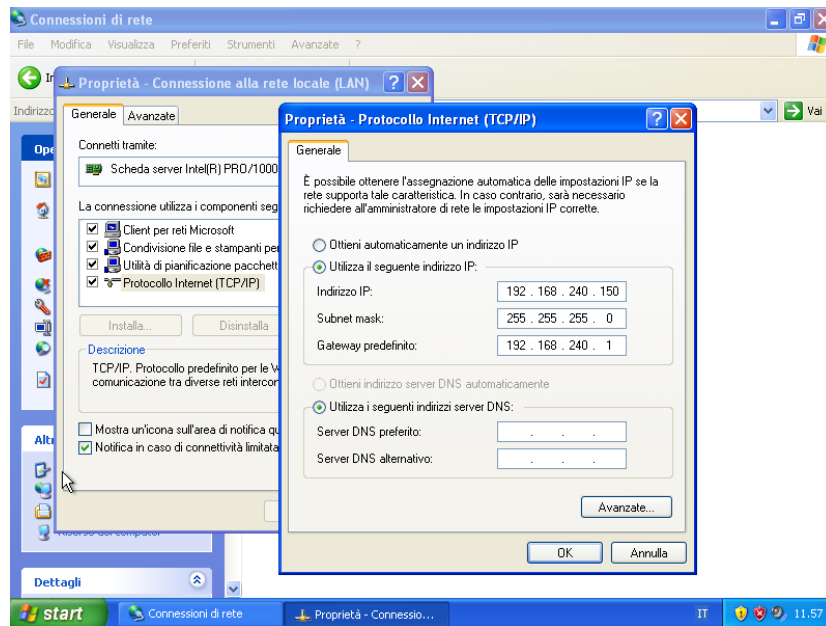
L'unica connessione è quella alla rete locale (infatti noi siamo in modalità internal). Tasto destro e clicchiamo su **Proprietà**:



Selezioniamo **Protocollo Internet (TCP/IP)** e clicchiamo sul pulsante **Proprietà**:



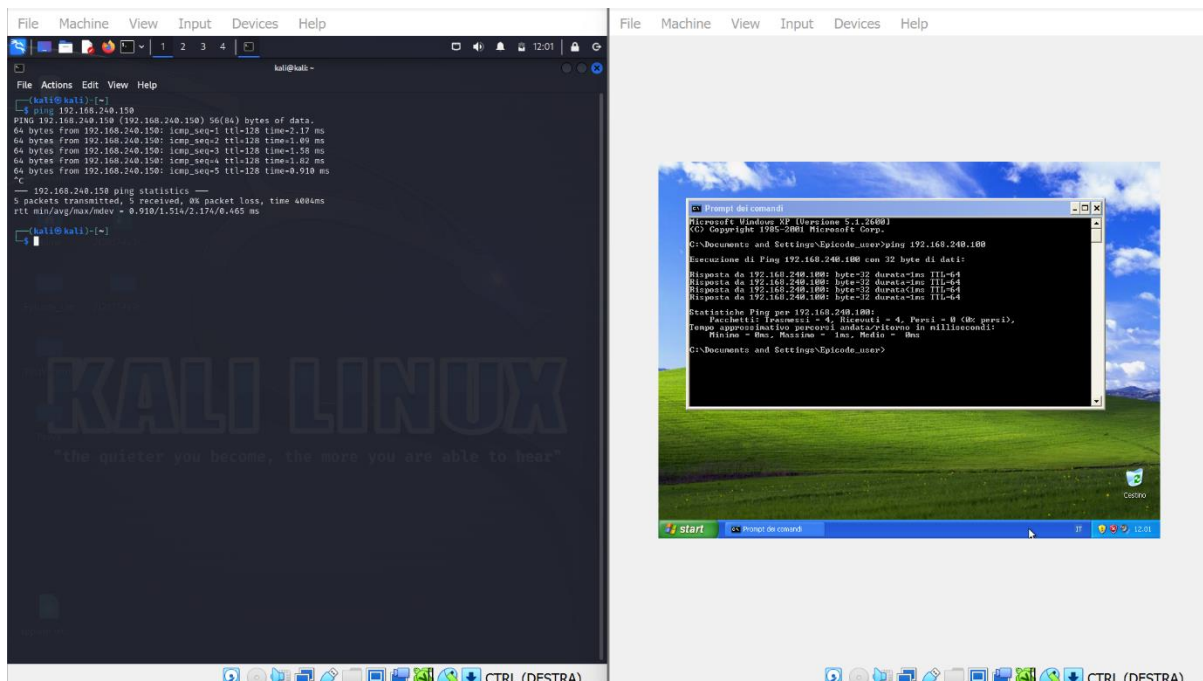
Qui potremo modificare Indirizzo IP e di conseguenza il Gateway come da screen:



Clicchiamo sul pulsante **OK**, chiudiamo tutto e riavviamo la macchina.

1.3.3 VERIFICA DELLA COMUNICAZIONE FRA LE MACCHINE

Ora dobbiamo verificare che le macchine comunichino fra loro. Per farlo, apriamo un terminale su entrambe ed eseguiamo il comando ping + IP della macchina avversaria:



Se, come in questo caso, le macchine riescono a scambiare almeno 4 pacchetti fra loro, significa che la verifica ha dato esito positivo e possiamo interrompere il ping con la combinazione CTRL + C (altrimenti proseguirebbe all'infinito).

2. SCANSIONE CON NMAP

2.1 DEFINIZIONE

Nmap è uno strumento di scansione di rete open source utilizzato per rilevare host e servizi in una rete, analizzandone la sicurezza. Di seguito i suoi quattro principali switch:

- -sT: Esegue una scansione TCP completa inviando pacchetti SYN al sistema target e aspettandosi risposte ACK.
- -sS: Esegue una scansione stealth, cercando di evitare il rilevamento intrusivo.
- -sV: Rileva le versioni dei servizi in esecuzione sulle porte aperte.
- -O: Esegue il fingerprinting dell'OS per identificare il sistema operativo target.

2.2 OBIETTIVO

La scansione con Nmap è un passo fondamentale in una fase di raccolta di informazioni e analisi preliminare durante un penetration test o una valutazione della sicurezza. L'obiettivo principale è ottenere informazioni dettagliate sulla rete target, identificare le porte aperte e i servizi in esecuzione su di esse. Queste informazioni sono cruciali per preparare e condurre un attacco mirato con Metasploit.

Nel nostro caso, eseguiremo la scansione in modalità -sV, ovvero chiederemo a Nmap di rilevare le versioni dei servizi in esecuzione sulle porte aperte.

2.3 ISTRUZIONI PASSO A PASSO

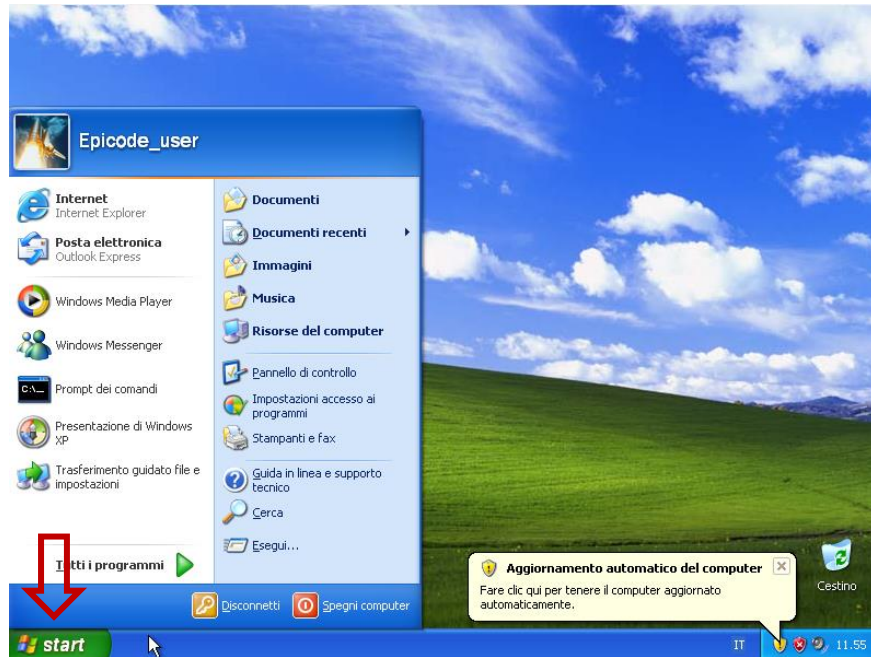
Da consegna, dovremo eseguire la scansione con Nmap in due situazioni diverse: la prima situazione vedrà il firewall della macchina Windows XP disattivato, mentre nella seconda il firewall dovrà essere attivo.

Vediamo i due casi nel dettaglio.

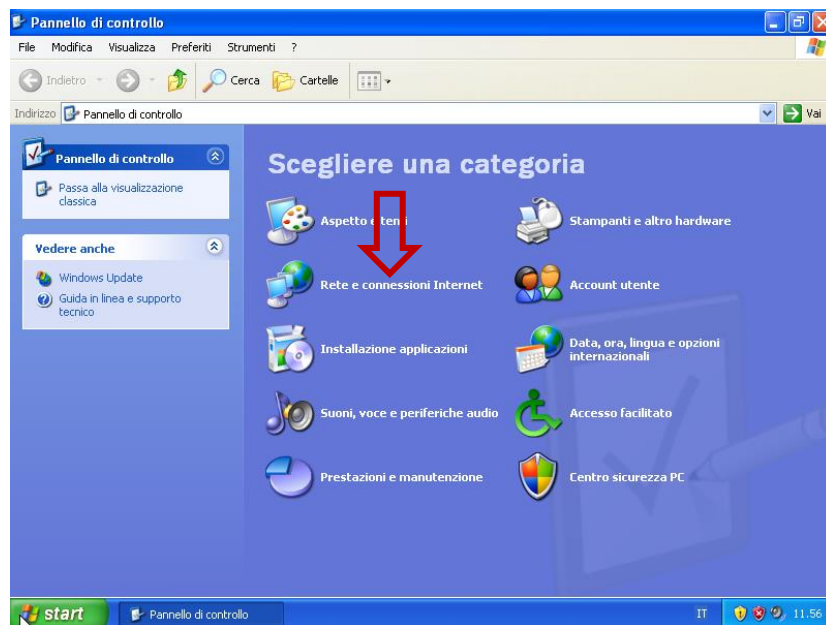
2.3 SCANSIONE CON FIREWALL DISATTIVATO

Nella macchina Windows XP, il firewall è disattivato. Ce lo comunica la consegna ma verifichiamolo velocemente seguendo i seguenti semplici passi.

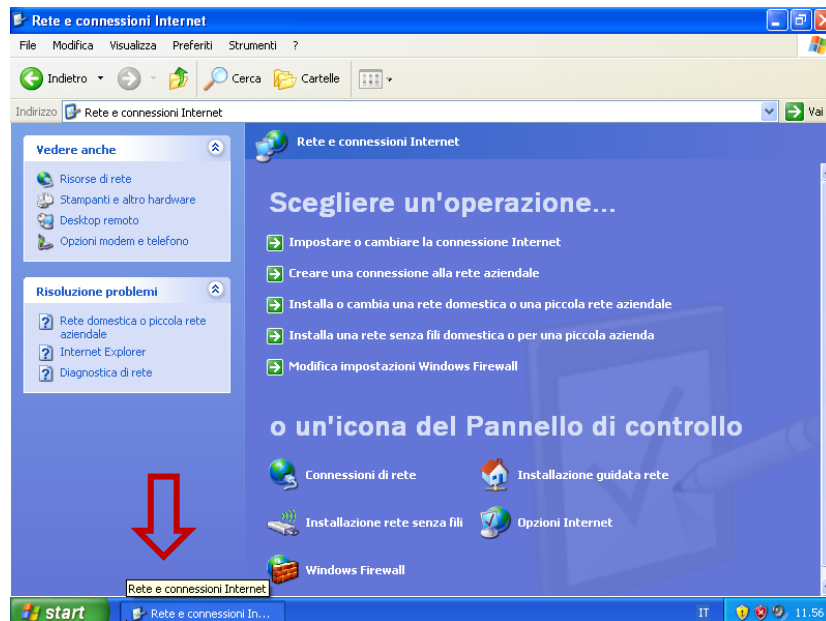
Su Windows XP, clicchiamo su **Start**:



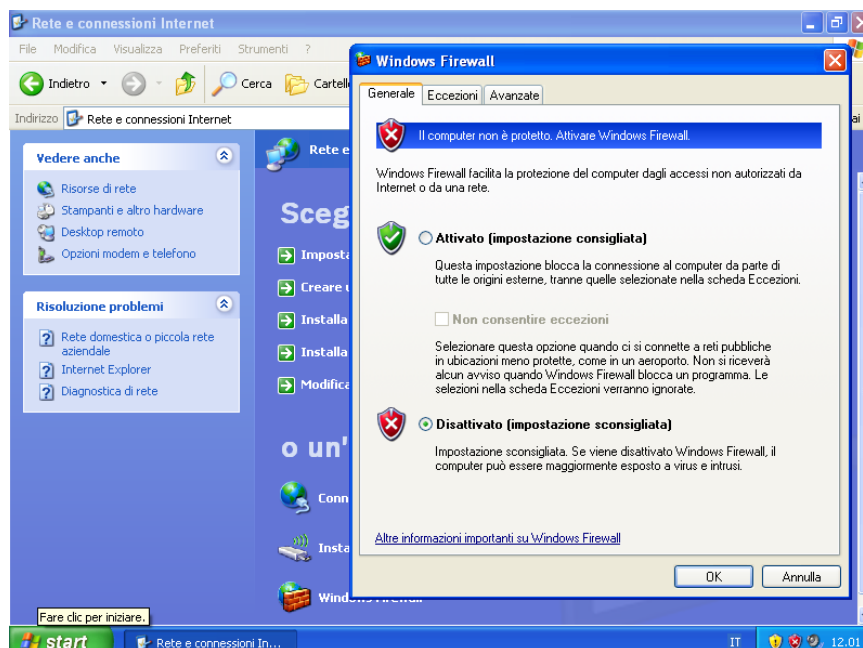
E clicchiamo di nuovo su **Rete e connessioni Internet**:



Contrariamente a quanto fatto durante la modifica dell'IP, questa volta selezioniamo **Windows Firewall**:



Qui possiamo verificare che il firewall è disattivato.



Spostiamoci sulla macchina Kali Linux e apriamo il terminale.

Lanciamo il comando `nmap -sV` seguito dall'IP di Windows XP:

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 12:02 CET
Nmap scan report for 192.168.240.150
Host is up (0.90s 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: OS: 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 20.66 seconds

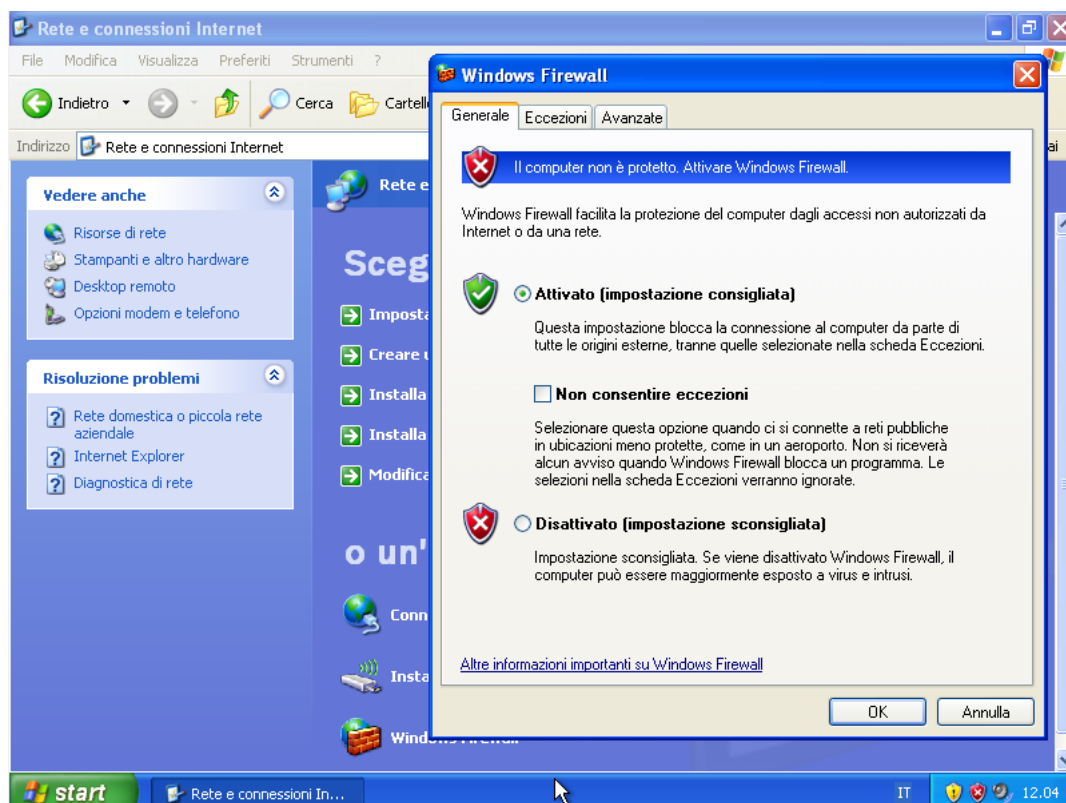
(kali@kali)~$

```

Nmap ha individuato una serie di informazioni. Vediamo nella prossima sezione come cambia l'output se il Firewall è disattivato.

2.3 SCANSIONE CON FIREWALL ATTIVO

Torniamo su Windows XP e attiviamo il Firewall:



Spostiamoci su Kali e lanciamo la scansione.

Dopo poco, Nmap ci comunica che "host seems down", quindi l'host o macchina target "sembra essere spento" e suggerisce di provare il switch `-Pn`.

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 12:05 CET
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 3.16 seconds
```

Tale switch viene utilizzato per eseguire la scansione di un host senza inviare i pacchetti di discovery di host ICMP. In altre parole, disabilita la rilevazione dell'host tramite ping. L'opzione -Pn è utile quando si desidera scansionare un host senza fare affidamento sulla risposta ai pacchetti di ping.

Alcuni host o reti, infatti, **possono essere configurati per ignorare o bloccare i pacchetti di ping**, quindi utilizzare -Pn può essere una scelta valida in tali situazioni per garantire che la scansione venga comunque eseguita.

Utilizziamo dunque il comando nmap -Pn -sV seguito dall'IP target e otteniamo il seguente output:

```
(kali@kali)-[~]
$ nmap -Pn -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 12:22 CET
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 214.48 seconds

(kali@kali)-[~]
$
```

3. ANALISI DELLE SCANSIONI EFFETTUATE CON NMAP

3.1 SCANSIONE VERSO WINDOWS XP CON FIREWALL DISATTIVATO

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 12:02 CET
Nmap scan report for 192.168.240.150
Host is up (0.90s 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 20.66 seconds

(kali@kali)-[~]
$
```

Quando il firewall non è attivo, Nmap prima di tutto ci comunica che "host is up" (quindi l'host è raggiungibile).

Ha inoltre rilevato 997 porte chiuse (la connessione è stata rifiutata), mentre vi sono 3 porte aperte con i seguenti servizi in ascolto:

Porta 135:

Il servizio **Microsoft Windows RPC (Remote Procedure Call)** è un componente fondamentale del sistema operativo Windows che **consente la comunicazione tra processi in modalità remota**. La

porta 135 è comunemente associata al servizio RPC. Questo servizio facilita la comunicazione tra programmi su computer diversi, consentendo loro di eseguire procedure l'uno sull'altro.

In Windows XP, il servizio **RPC è responsabile dell'esecuzione di chiamate di procedura remote tra processi su una rete**. È essenziale per il funzionamento di molte funzionalità di rete e di sistema. Tuttavia, la porta 135 è stata associata anche a vulnerabilità di sicurezza nel passato, come **il worm Blaster/MSBlast, che sfruttava una falla nel servizio RPC**.

Porta 139:

Il **servizio NetBIOS-SSN (NetBIOS Session Service)** è associato alla porta 139 ed è parte del protocollo NetBIOS (Network Basic Input/Output System). **Il protocollo NetBIOS è stato sviluppato per consentire la comunicazione tra dispositivi in una rete locale**.

La porta 139 è spesso utilizzata per la condivisione di file e stampanti tramite il protocollo NetBIOS su TCP/IP. Questa funzionalità consente a diversi computer di una rete di accedere alle risorse di file e stampa su un altro computer. Tuttavia, il servizio NetBIOS su TCP/IP, soprattutto quando utilizzato senza le debite precauzioni di sicurezza, può presentare rischi per la sicurezza del sistema.

In passato, questa configurazione è stata sfruttata da malware e minacce di sicurezza, come i worm che si diffondevano automaticamente attraverso le reti.

Porta 445:

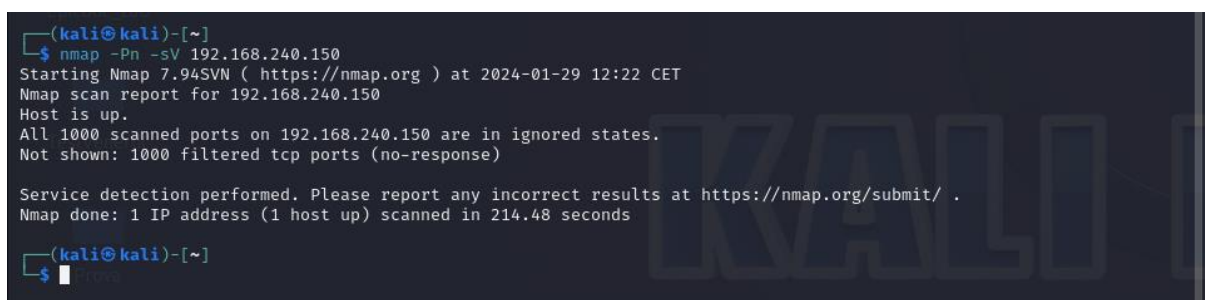
Il **servizio "XP Microsoft-DS"** associato alla porta 445 è comunemente noto come **Microsoft-DS (Microsoft Directory Service)** e **si riferisce al servizio di condivisione file e stampanti su reti Windows utilizzando il protocollo SMB (Server Message Block)** sulla versione 1.0.

La porta 445 è utilizzata per la comunicazione SMB su TCP/IP ed è una versione più moderna rispetto alla porta 139, associata al protocollo NetBIOS. Microsoft-DS è parte integrante del servizio di condivisione file e stampanti di Windows e consente ai computer di una rete di accedere e condividere risorse come file e stampanti.

Il protocollo SMB è stato soggetto a diverse vulnerabilità nel corso degli anni, ed è stato coinvolto in attacchi informatici, inclusi worm e malware.

Infine, Nmap riporta l'informazione sul sistema operativo: si tratta di Windows XP.

3.2 SCANSIONE VERSO WINDOWS XP CON FIREWALL ATTIVO



```
(kali@kali)-[~]
$ nmap -Pn -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 12:22 CET
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 214.48 seconds

(kali@kali)-[~]
$
```

Per ottenere un feedback da Nmap una volta attivato il firewall, è stato necessario utilizzare il switch -Pn. La scansione è comunque molto ridotta rispetto a quella analizzata nella sezione precedente.

Anche in questo caso Nmap ci comunica che l'host è raggiungibile, però ci comunica anche che tutte le 1000 porte del sistema sono in un stato "ignored", ovvero le porte sono filtrate e non hanno risposto. Questo significa che il tentativo di connessione di Nmap non è stato né accettato, né rifiutato.

Si tratta di un comportamento tipico di un sistema dotato di firewall.

Si nota inoltre che non è stato rilevato il sistema operativo della macchina target.

RIEPILOGO

Il progetto S9 L1 è stato svolto in tre fasi.

Come prima cosa, abbiamo preparato l'ambiente, che prevedeva una macchina attaccante Kali Linux e una macchina target Windows XP. La preparazione è consistita nel configurare entrambe le macchine su internal, impostare i loro IP come da consegna e verificare che le due macchine riuscissero a comunicare.

Dopodiché abbiamo eseguito una scansione su Windows XP con Nmap in due situazioni diverse: nella prima, il firewall di Windows era disattivato e nella seconda invece era attivo.

A questo punto abbiamo analizzato i due differenti output e concluso che il firewall ha impedito a Nmap di interrogare le 3 porte che sappiamo essere aperte e con servizi in ascolto. I tentativi di connessione di Nmap non sono stati né accettati, né rifiutati: reazione tipica di un sistema dotato di firewall.

Inoltre, quando il Firewall era attivo non è stato possibile individuare la versione del sistema operativo della macchina target, a differenza della situazione in cui il firewall era disattivato.