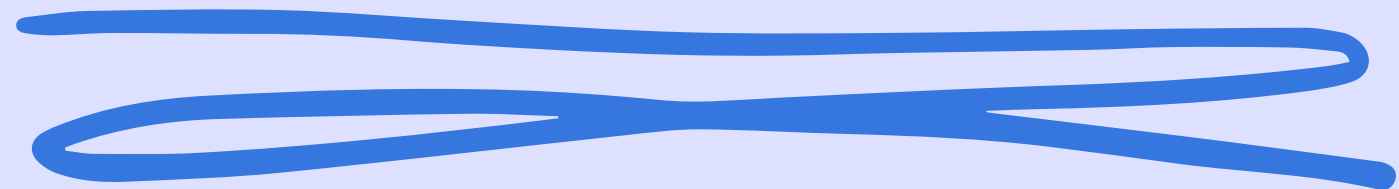


S9 L1

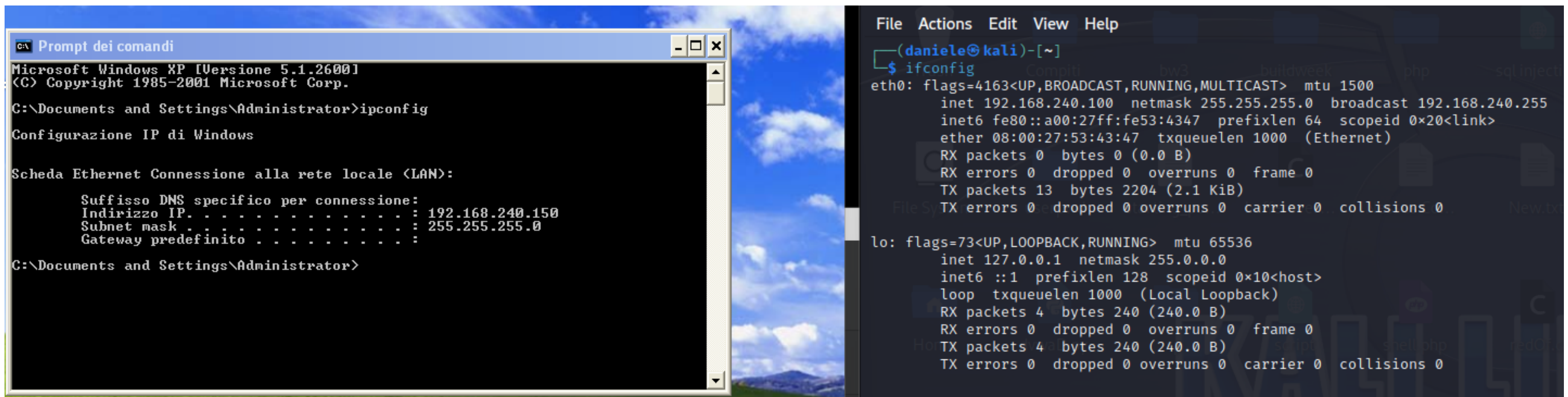


SOC Intro

Daniele Zizzi

In questo esercizio andremo a scansionare il sistema XP, con e senza firewall, mettendo in evidenza le differenze nella scansione e i rischi scaturiti dalla mancanza o disattivazione di esso.

Di seguito, la configurazione di rete delle due macchine, XP e kali.



The image displays two side-by-side terminal windows. The left window is a Windows XP command prompt titled 'C:\ Prompt dei comandi'. It shows the output of the 'ipconfig' command, displaying the IP configuration for the 'Scheda Ethernet Connessione alla rete locale (LAN)'. The IP address is 192.168.240.150, the subnet mask is 255.255.255.0, and the default gateway is not set. The right window is a Kali Linux terminal with a dark background. It shows the output of the 'ifconfig' command, displaying the configuration for the 'eth0' interface (192.168.240.100) and the 'lo' interface (127.0.0.1).

```
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):

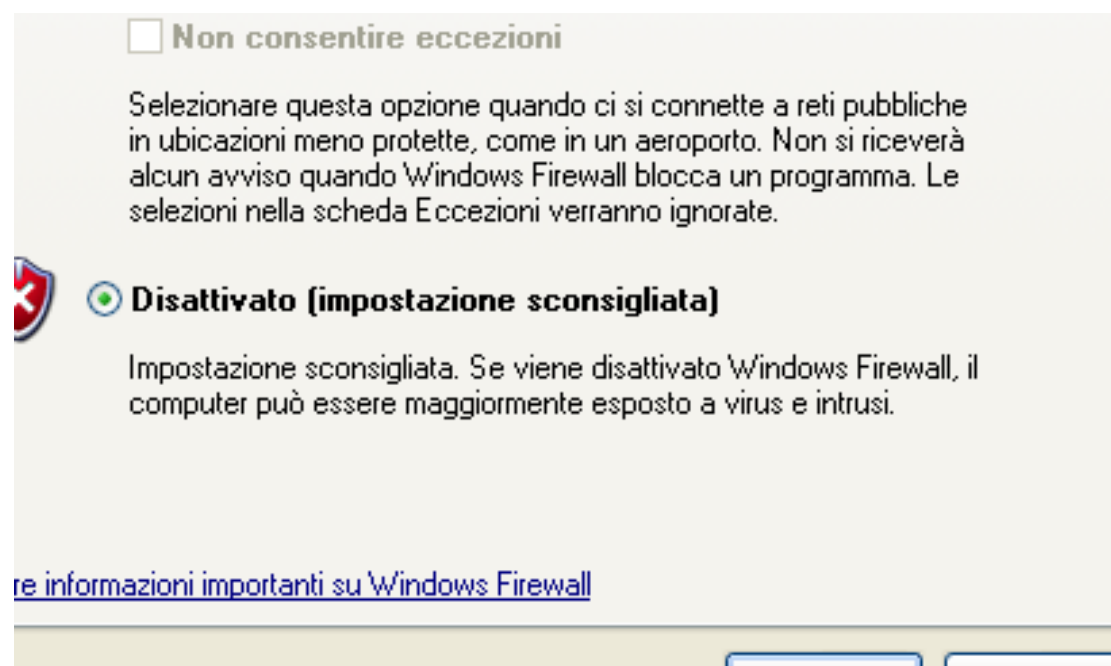
    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

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

```
File Actions Edit View Help
(daniele@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:fe53:4347 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:53:43:47 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 2204 (2.1 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
```




Dopo una scansione dei servizi attivi su windows, con firewall disattivato, riceviamo una lista di essi, numero di porta e lo stato. Non riusciamo ad ottenere la versione dei servizi, nonostante la mancanza del firewall.



```
(daniele@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 14:19 CET
Nmap scan report for 192.168.240.150
Host is up (0.00015s 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 20.26 seconds
```

Con il firewall attivo, poichè windows blocca pacchetti icmp, nmap non riesce a scansionare il sistema. Pertanto utilizziamo lo switch “-Pn”, per far operare nmap senza l'utilizzo del ping. Come risultato, comunque, non otteniamo nulla, poichè il firewall non permette ad nmap, di ottenere informazioni sulle porte e servizi erogati, poichè blocca tali richieste.

 Attivato (impostazione consigliata) Questa impostazione blocca la connessione al computer da parte di tutte le origini esterne, tranne quelle selezionate nella scheda Eccezioni.	<pre>(daniele@kali)-[~] \$ nmap -sV 192.168.240.150 Starting Nmap 7.94 (https://nmap.org) at 2023-11-20 14:23 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 3.06 seconds</pre>
 Windows Firewall sta facilitando la protezione del computer. Windows Firewall facilita la protezione del computer dagli accessi non autorizzati da Internet o da una rete.  Attivato (impostazione consigliata) Questa impostazione blocca la connessione al computer da parte di tutte le origini esterne, tranne quelle selezionate nella scheda Eccezioni.	<pre>(daniele@kali)-[~] \$ nmap -sV -Pn 192.168.240.150 Starting Nmap 7.94 (https://nmap.org) at 2023-11-20 14:23 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 214.46 seconds</pre>

È buona norma configurare correttamente e tenere sempre attivo il firewall, in modo che un attaccante, non riesca a visualizzare i servizi attivi e quindi sfruttarne le vulnerabilità presenti. Se il firewall non è configurato correttamente o completamente disattivato, l'attaccante può visualizzare le versioni dei servizi e sfruttarne le vulnerabilità, quindi effettuare exploit ed ottenere un accesso non autorizzato ad una macchina target, che potrebbe essere un semplice pc di un'azienda o un server che eroga servizi importanti oppure un nas con file che non devono essere divulgati per nessun motivo.