WARDIERE INC.

S9L1

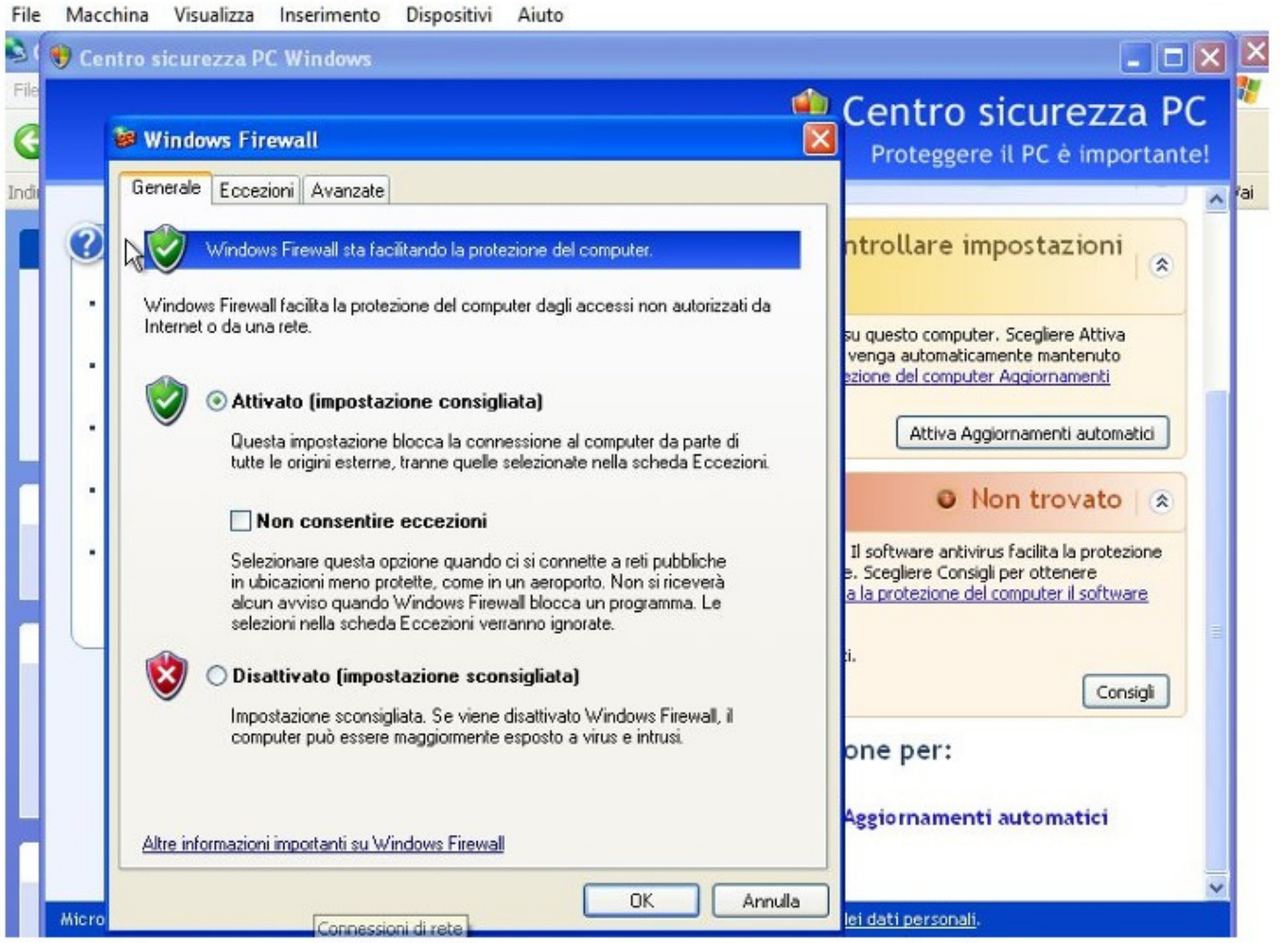
2022
Company

Accertiamoci che il Firewall di Windows sia disattivato e lanciamo la scansione verso il nostro target con lo switch –sV. La scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP 135,139,445.

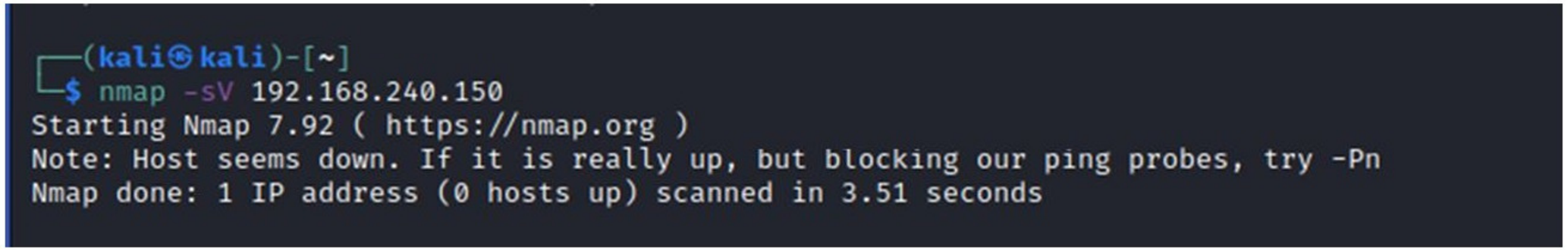
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 192.168.240.150
Host is up (0.68s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  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 20.89 seconds
```

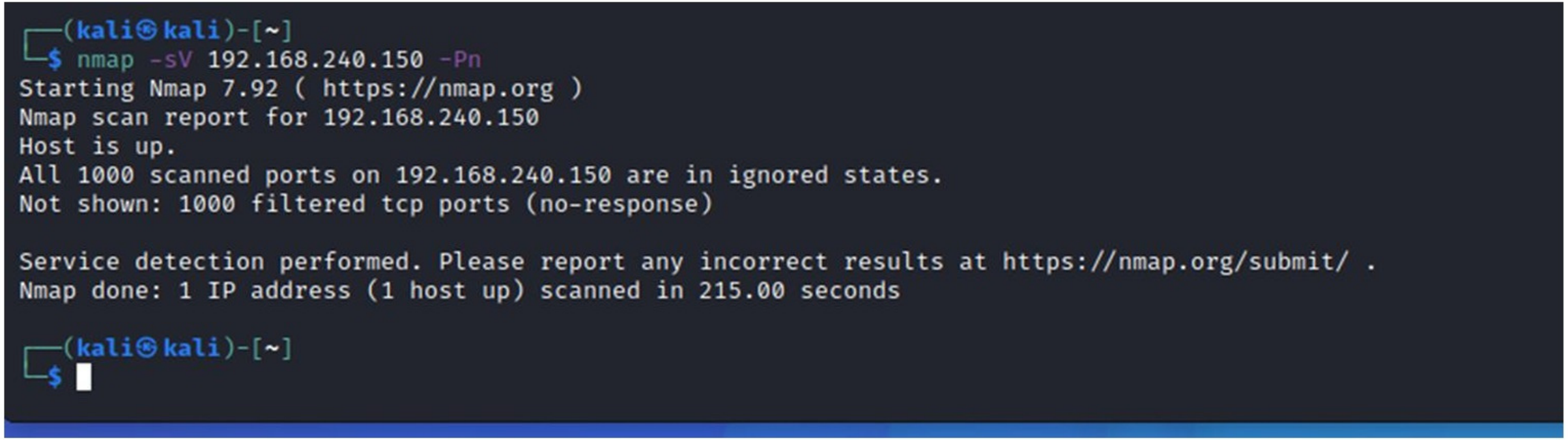
Attiviamo il Firewall di Windows XP e procediamo nuovamente alla scansione.



Il risultato della scansione ci riporta che la macchina o non è accesa, oppure se è accesa sta bloccando l'host discovery di nmap. Ci consiglia quindi di provare con il parametro –Pn. La situazione è piuttosto chiara, il Firewall sta bloccando il traffico in entrata con protocollo ICMP (il ping). Proviamo a sfruttare lo switch –Pn per evitare il ping e passare direttamente alla scansione dei servizi



Utilizzando lo switch –Pn, la scansione salterà il ping e passerà alla service discovery. A questo giro tutte le porte sembrano filtrate, ovvero non hanno risposto alle richieste dello scanner. È palese che il Firewall sta bloccando l'accesso alle porte. Ricordate che una porta risulta filtrata quando lo scanner non riceve nessun segnale – in generale non si può dire con certezza se una porta filtrata sia aperta o chiusa (nella fattispecie sappiamo che sulle porte 135,139,445 sono in ascolto servizi).



Conclusione:

L’abilitazione del Firewall di Windows XP sta di fatto bloccando la scansione dall’esterno verso i servizi attivi sulla macchina Windows XP. Sappiamo che i servizi sono vulnerabili in quanto li abbiamo sfruttati nella Unit 2 durante i nostri test con Metasploit – di conseguenza possiamo dire che il Firewall sta preventivamente riducendo rischi di attacchi dall’esterno, rendendo inaccessibili dall’esterno i servizi sulle porte 135,139,445 TCP.