ESERCIZIO W18D1
PRATICA 1

Obiettivo: Valutare l'impatto dell'attivazione del firewall sulla capacità di **nmap** di rilevare i servizi e le porte aperte su una macchina Windows XP.

Durante l'esercizio, sono stati eseguiti i seguenti passaggi:

Configurazione delle Macchine:

Utilizzo di una macchina Windows XP (IP: 192.168.240.150) e una macchina Kali Linux (IP: 192.168.240.100).

```
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:fe21:b1d0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 1105  bytes 73999 (72.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1154  bytes 86828 (84.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

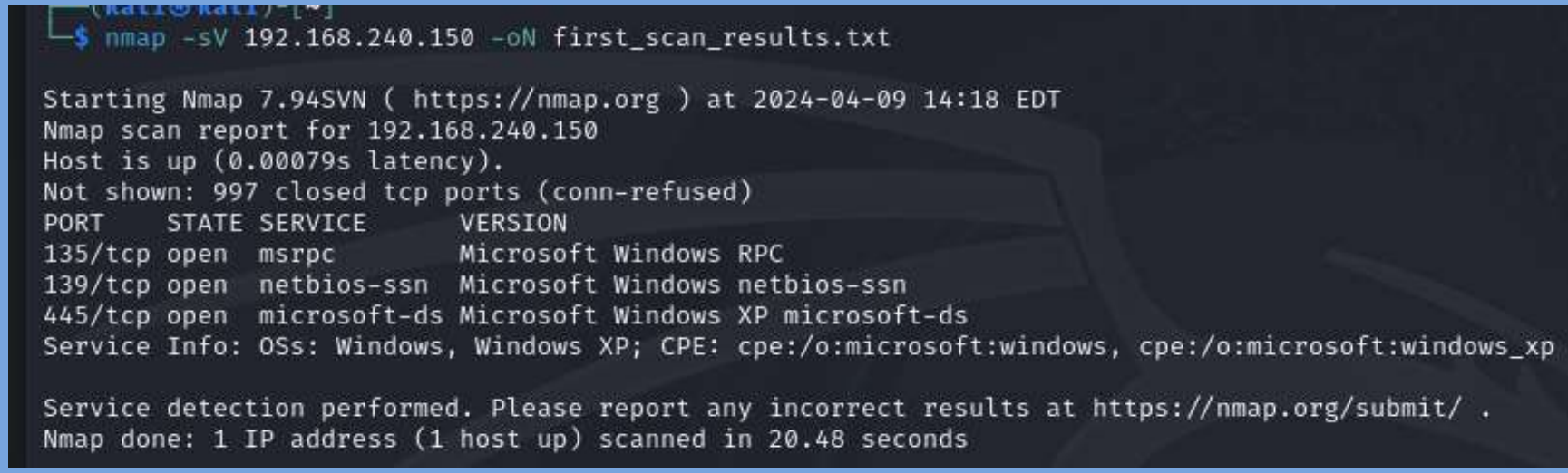
```
Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . . : 192.168.240.150
        Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . . : 192.168.1.1
```

Prima Scansione (nmap senza Firewall):

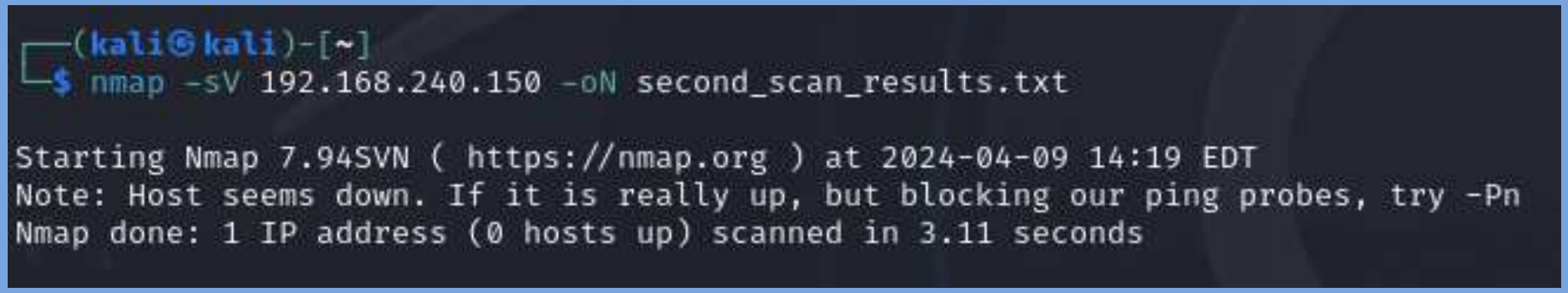
•Eseguita una scansione **nmap** dalla macchina Kali Linux verso la macchina Windows XP.

•Risultati:

- •Porte aperte rilevate: **135/tcp** (msrpc), **139/tcp** (netbios-ssn), **445/tcp** (microsoft-ds).



1. **Attivazione del Firewall su Windows XP:**
   - Il Firewall di Windows XP è stato attivato sulla macchina target (192.168.240.150).
2. **Seconda Scansione (nmap con Firewall attivo):**
   - Tentativo di eseguire una seconda scansione **nmap** dalla macchina Kali Linux verso la macchina Windows XP con il Firewall attivo.
   - **Risultati**:
     - **nmap** non è riuscito a determinare lo stato dell'host e ha riportato che l'host sembra essere "down" o non raggiungibile.



Analisi dei Risultati:

L'attivazione del firewall sulla macchina Windows XP ha influenzato significativamente la capacità di **nmap** di condurre una scansione efficace e rilevare i servizi e le porte aperte sulla macchina target.

Durante la prima scansione (**nmap** senza firewall), sono state rilevate diverse porte aperte e i relativi servizi, confermando la visibilità dei servizi di rete sulla macchina.

Tuttavia, durante la seconda scansione (**nmap** con firewall attivo), **nmap** non è riuscito a comunicare con l'host target e ha segnalato che l'host sembra essere "down".

Questo suggerisce che il firewall ha bloccato o filtrato il traffico di rete in ingresso, inclusi i tentativi di scansione da parte di **nmap**, rendendo l'host non accessibile per la scansione.

Conclusioni:

L'esperimento dimostra l'importanza del firewall come misura di sicurezza per limitare l'esposizione dei servizi di rete e impedire l'accesso non autorizzato.

L'attivazione del firewall ha dimostrato di influenzare negativamente la capacità di **nmap** di rilevare i servizi e le porte aperte sulla macchina Windows XP, evidenziando l'efficacia delle misure di difesa informatica nella protezione delle risorse di rete.