W11D1 - Pratica (2)

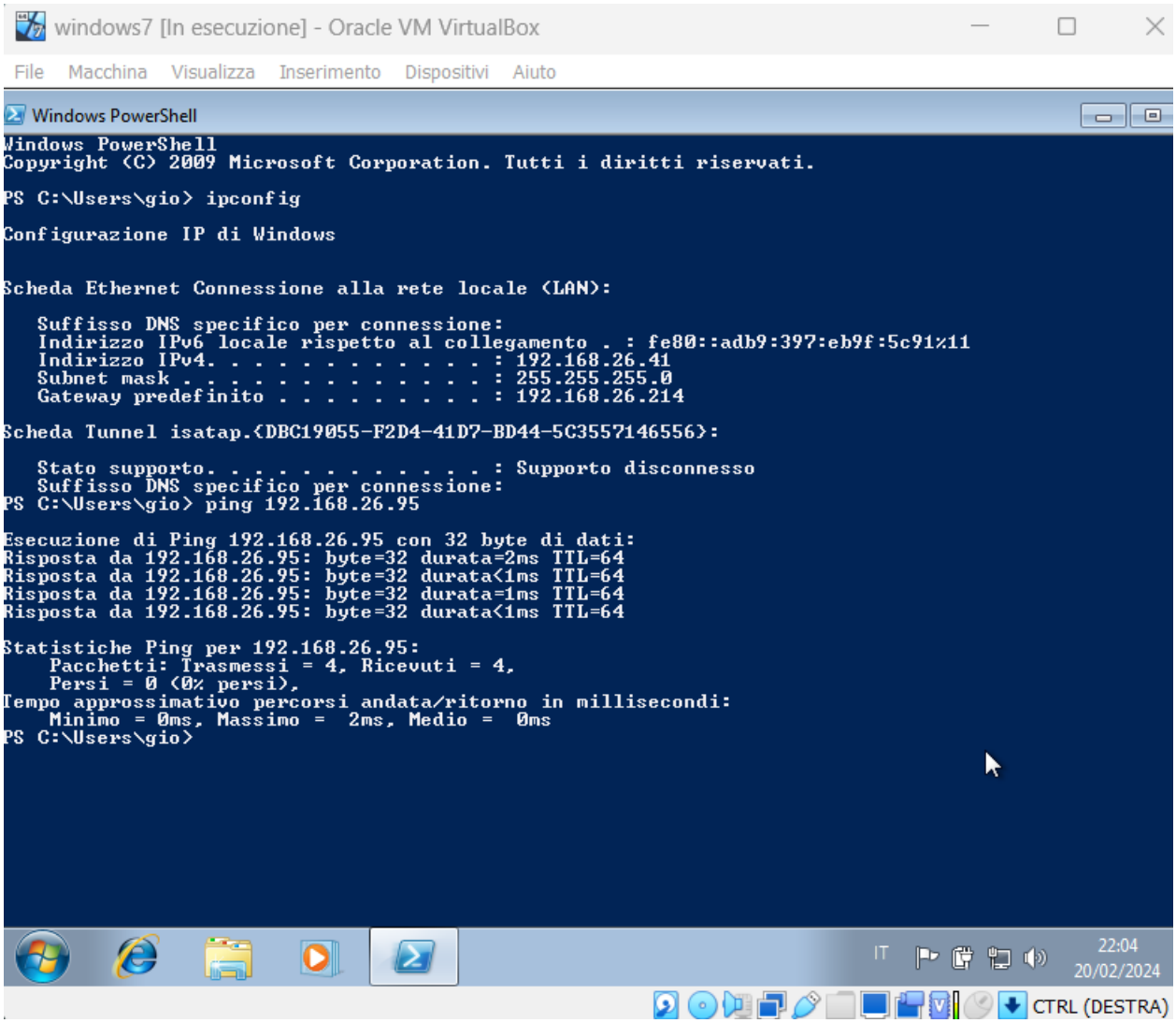
EPICODE

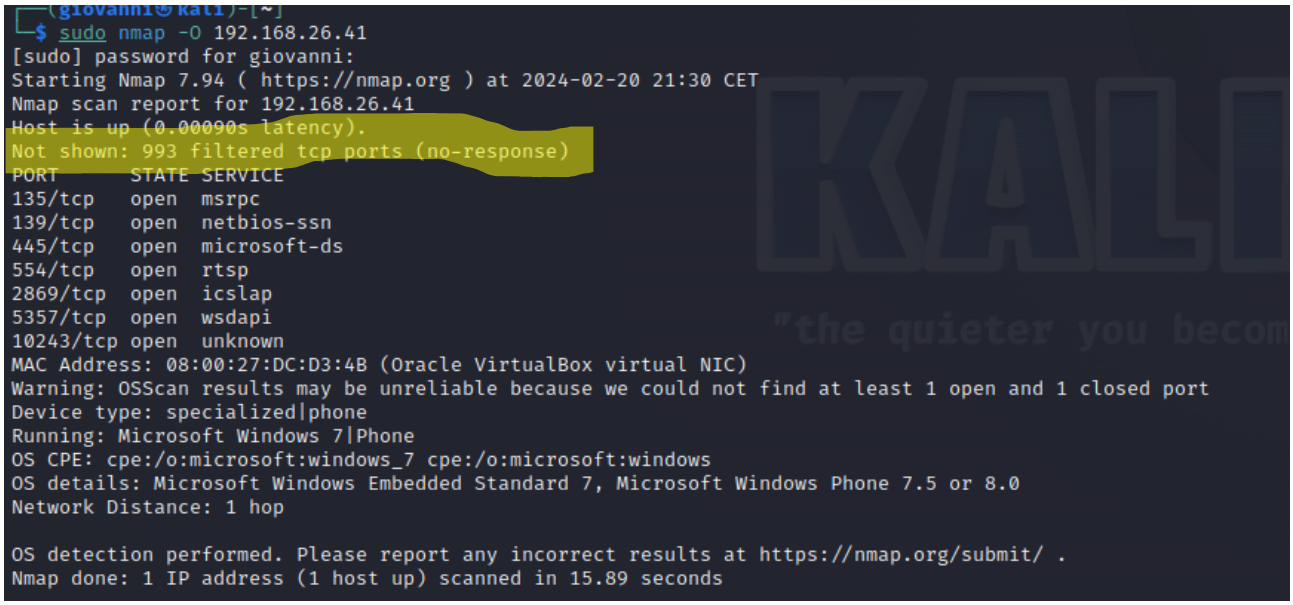
Esercizio
Scansione dei servizi

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Windows 7**:

- OS fingerprint
- Syn Scan
- Version detection




┌──(giovanni㉿kali)-[~]
└─$ sudo nmap -O 192.168.26.41
[sudo] password for giovanni:
Starting Nmap 7.94 (https://nmap.org) at 2024-02-20 21:30 CET
Nmap scan report for 192.168.26.41
Host is up (0.00090s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT   STATE SERVICE
135/tcp   open msrpc
139/tcp   open netbios-ssn
445/tcp   open microsoft-ds
554/tcp   open rtsp
2869/tcp open icslap
5357/tcp open wsdapi
10243/tcp open unknown
MAC Address: 08:00:27:DC:D3:4B (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.89 seconds