



## EPICODE CS0124

### REPORT S9L1

La traccia ci chiede di eseguire una scansione dei servizi attivi sulla macchina windows xp tramite kali linux

Per prima cosa cambiamo gli indirizzi ip della macchina come da consegna, successivamente eseguiamo una scansione prima con il firewall windows attivo, quindi possiamo notare che la richiesta viene ignorata e veniamo avvertiti da windows di un possibile conflitto con un altro indirizzo ip.

La seconda volta riproviamo con il firewall down e vediamo come vengono esposti i servizi attivi di windows xp con le rispettive porte e tipi di connessioni.

The image shows a Kali Linux terminal window on the left and a Windows XP network configuration window on the right. The terminal displays the output of the `ifconfig` command for the `eth0` interface, showing an IP address of `192.168.13.20` and a netmask of `255.255.255.0`. It also shows the output of the `nmmap -sV 192.168.13.20` command, which reports that the host is up and lists several open ports: `135/tcp` (msrpc), `139/tcp` (netbios-ssn), and `445/tcp` (microsoft-ds). The Windows XP window on the right shows the 'Proprietà - Protocollo Internet (TCP/IP)' dialog box, with the 'Generale' tab selected. The 'Indirizzo IP' section is set to 'Utilizza il seguente indirizzo IP' with the IP address `192.168.13.20` and a subnet mask of `255.255.255.0`. The 'Gateway predefinito' is set to `192.168.13.1`. The 'Server DNS' section is set to 'Utilizza i seguenti indirizzi server DNS' with the preferred DNS server `8.8.8.8`.

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.13.20 netmask 255.255.255.0 broadcast 192.168.13.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 16 bytes 1493 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2424 (2.3 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 0<10<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

kali@kali:~$ nmmap -sV 192.168.13.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:42 CET
Notes: 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 3.13 seconds

kali@kali:~$ nmmap -sV 192.168.13.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:43 CET
Nmap scan report for 192.168.13.20
Host is up (0.00011s 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 20.30 seconds
```