

ES Lezione 1 Settimana 9

Nell'esercizio di oggi abbiamo effettuato due scansioni della nostra macchina virtuale Windows XP, tramite Kali.

Nella prima prova abbiamo provato ad effettuare questa scansione dei servizi aperti lasciando il firewall di W XP attivo, come possiamo notare la macchina non è riuscita ad effettuare la scansione perchè il firewall lo ha impedito.

Nel secondo tentativo, con il firewall spento, siamo riusciti a portare a termine la scansione e salvare la stessa in un file. Possiamo notare i servizi attivi con relative porte e sistema operativo.

```
kali@kali: ~  
File Actions Edit View Help  
Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 10:18 EST  
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 3.16 seconds  
  
(kali@kali)-[~]  
$ nmap -sV -o reportWXP 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 10:20 EST  
Nmap scan report for 192.168.240.150  
Host is up (0.00051s latency).  
Not shown: 998 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  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 20.40 seconds  
  
(kali@kali)-[~]  
$ ls  
blu      Documents  gameshell  Music      Public      Videos  
blucartella Downloads  gameshell-save.sh percorsoCuccia reportWXP  
Desktop  flag.txt   gameshell.sh Pictures     Templates  
  
(kali@kali)-[~]
```