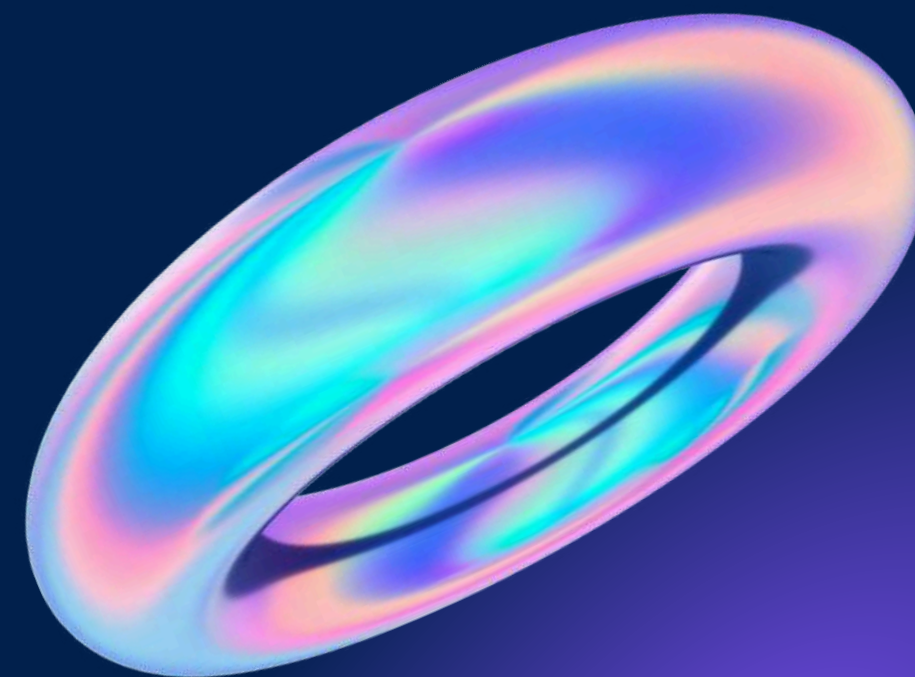




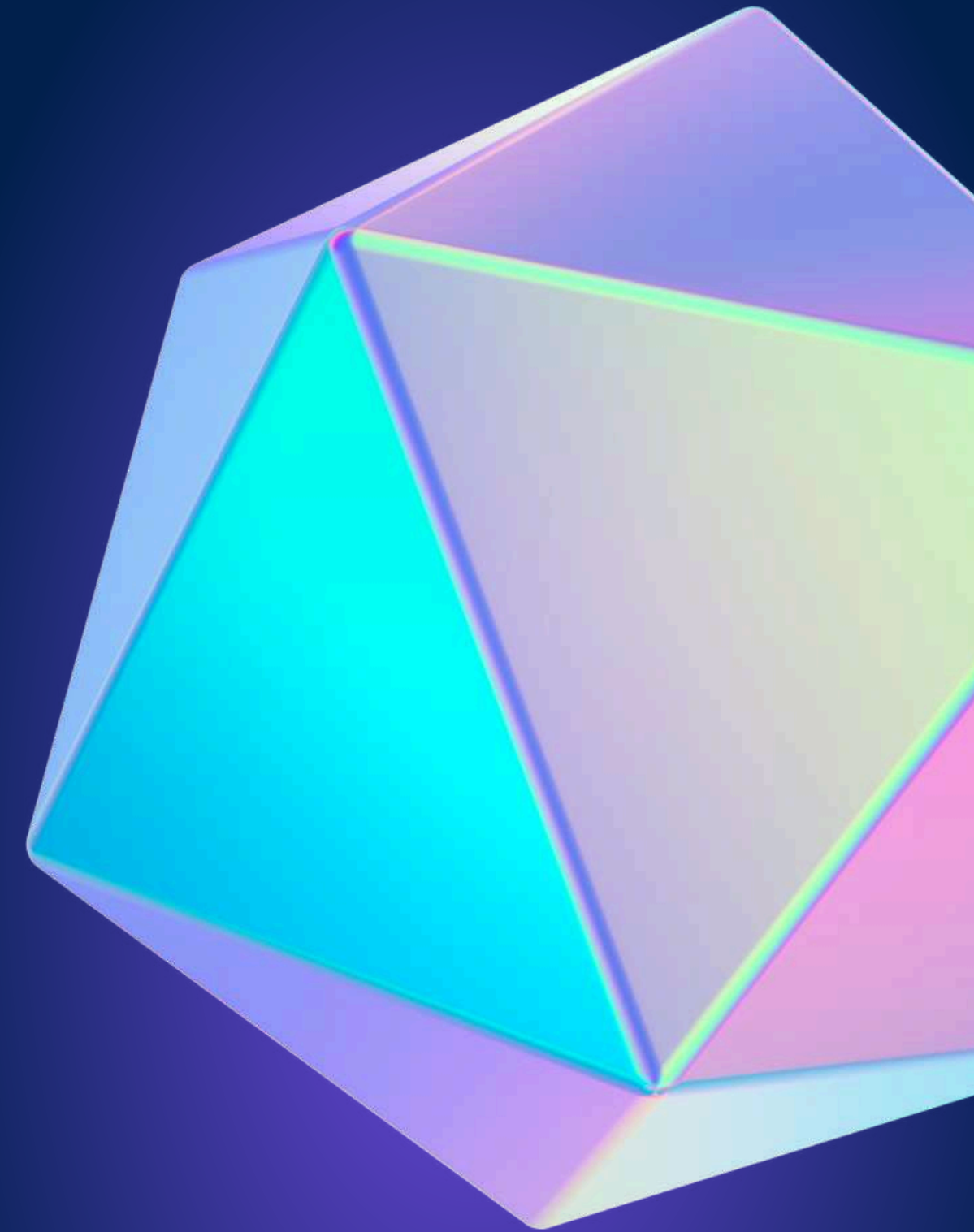
SQL1

Antonio Perna

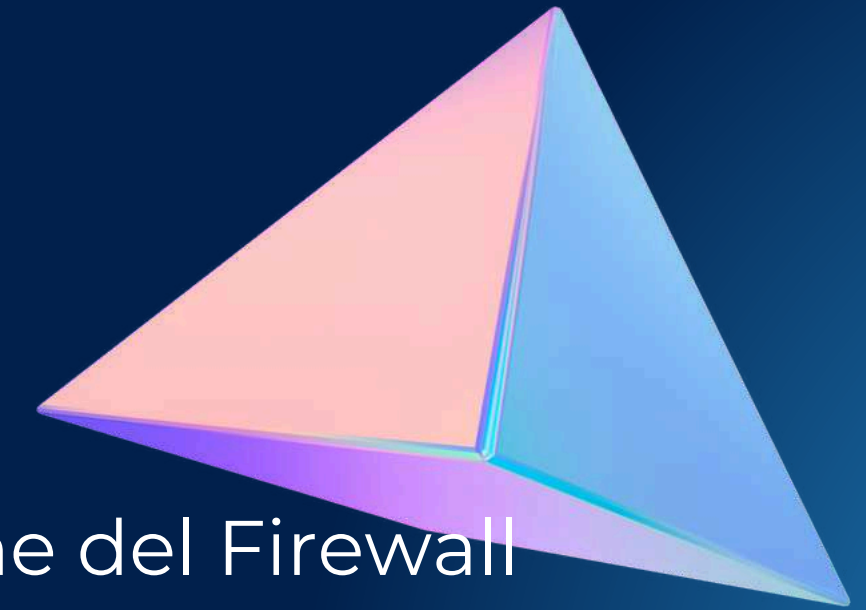




Security Operation: azioni preventive



Cosa fare



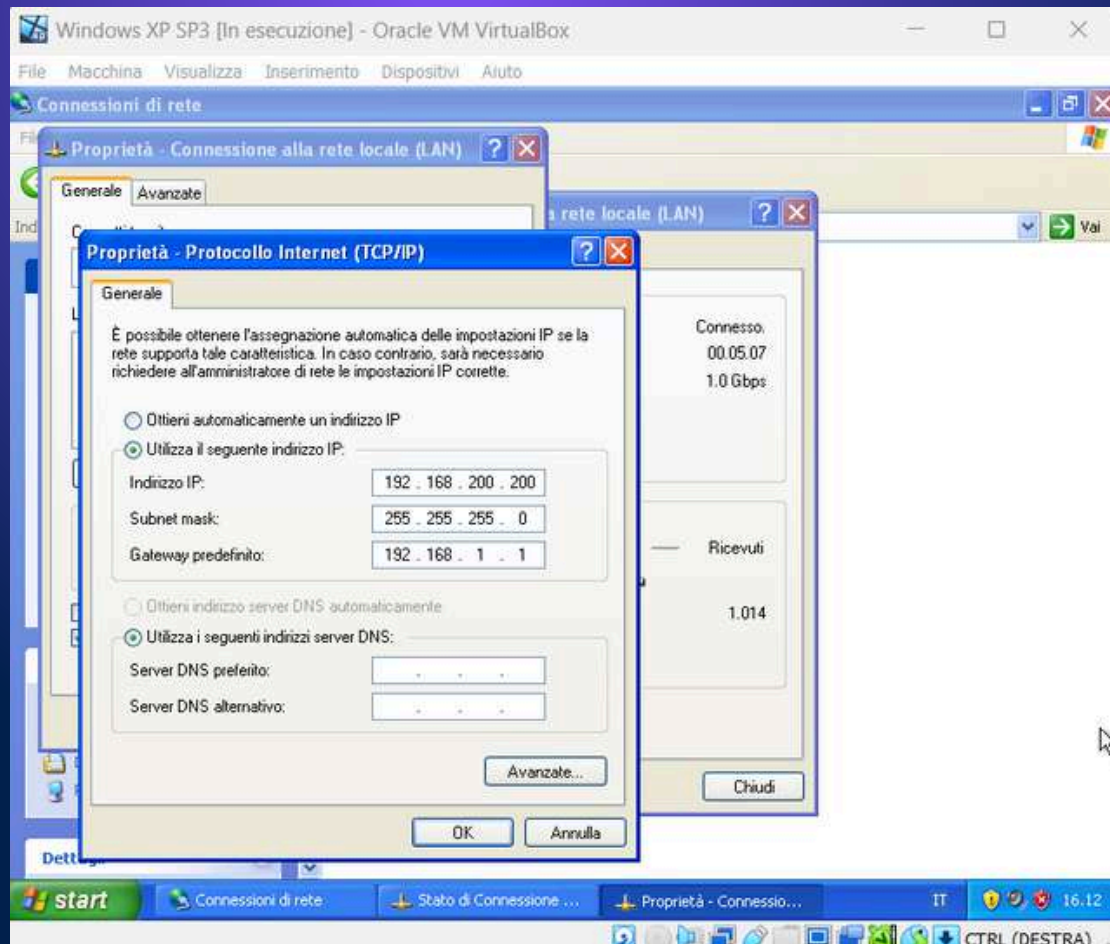
L'è servizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch -sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV.
5. Trovare le eventuali differenze e motivarle.



Prova con firewall disattivo

A screenshot of a Kali Linux virtual machine window titled "kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal window shows the execution of the command `nmap -sV 192.168.200.200`. The output indicates that the host is up and lists several open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The scan was completed in 19.82 seconds.

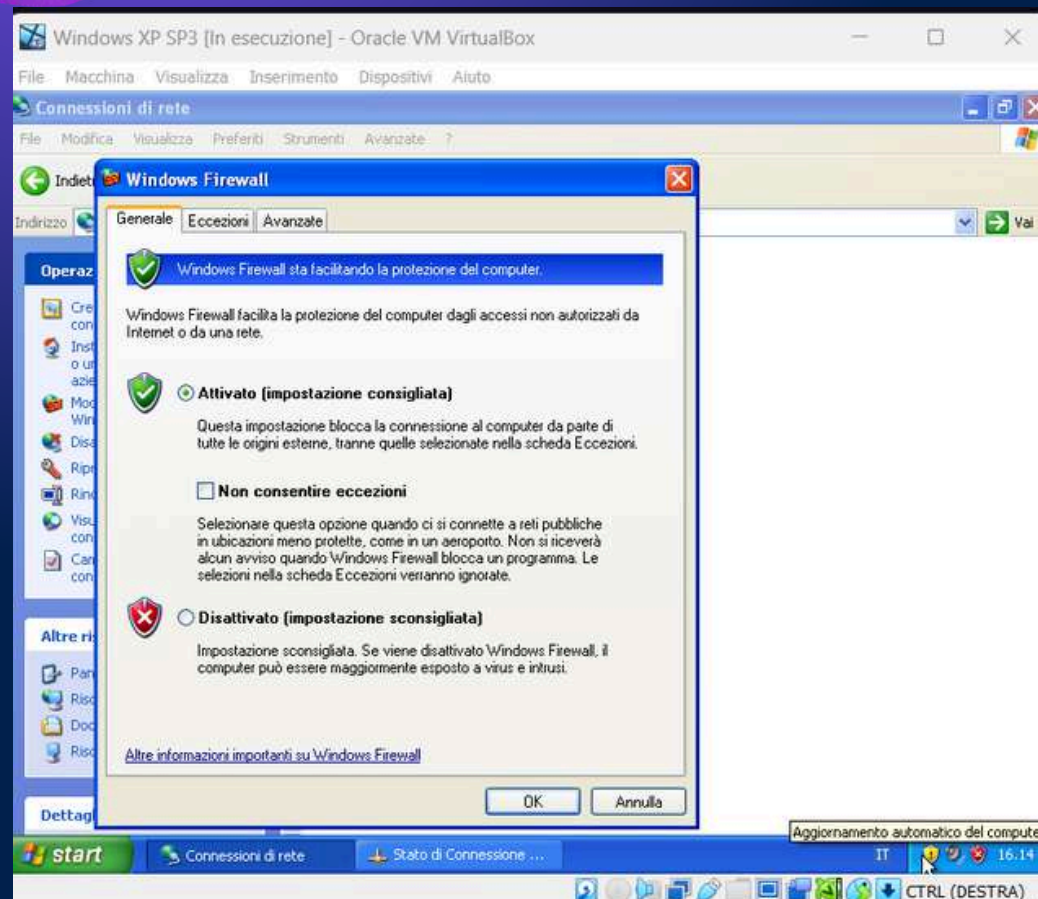
```
(kali@kali)-[~]
$ nmap -sV 192.168.200.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:12 EDT
Nmap scan report for 192.168.200.200
Host is up (0.0036s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft 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 19.82 seconds

(kali@kali)-[~]
$
```

Dopo aver configurato l'indirizzo ip della macchina, andiamo a fare una scansione con il comando `nmap -sV` che ci riporterà tutte le porte aperte che ci sono.

Prova con firewall attivo



```
(kali@kali)-[~]  
$ nmap -sV 192.168.200.200  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:15 EDT  
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 3.24 seconds
```

Proviamo a fare lo stesso comando di prima e vediamo che la scansione non va a buon fine e ci consiglia di provare con -Pn

Prova con firewall attivo

```
(kali@kali)-[~]  
$ nmap -sV 192.168.200.200 -Pn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:16 EDT  
Nmap scan report for 192.168.200.200  
Host is up.  
All 1000 scanned ports on 192.168.200.200 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 216.37 seconds
```

A questo punto, proviamo a fare una nuova scansione con lo switch -Pn e quindi col comando `nmap-sV ip -Pn` e vediamo che va a filtrare le porte ma non possiamo sapere se sono aperte o chiuse, ovviamente, col firewall attivo, andiamo a limitare la comunicazione alla macchina.