

Valutiamo l'impatto dell'attivazione del firewall su una macchina Windows XP durante la scansione dei servizi esterni tramite Nmap.

Abbiamo iniziato verificando che il firewall sulla macchina fosse disattivato. Successivamente, abbiamo eseguito una prima scansione con Nmap, utilizzando lo switch -sV per identificare i servizi e l'opzione -o per salvare l'output in un file. In questa fase senza il firewall attivato, la scansione ha rilevato aperte varie porte e ha identificato i servizi associati a esse, fornendo un quadro dettagliato dello stato dei servizi sulla macchina.

Dopo questa fase, abbiamo attivato il firewall sulla macchina.

Successivamente, abbiamo eseguito una seconda scansione con Nmap, mantenendo lo switch -sV. In questa scansione con il firewall attivato, ci sono state differenze significative rispetto alla prima scansione. Il firewall ha bloccato il ping inviato da Kali così impedendo la scansione.

Infine, abbiamo eseguito una terza scansione aggiungendo -Pn per disattivare l'invio di ping riscontrando nuovamente delle discrepanze che potrebbero indicare il blocco di servizi o porte da parte del firewall, sottolineando così l'efficacia di questa misura di sicurezza nella protezione del sistema da potenziali minacce esterne.

```
(kali@kali)-[~]
$ nmap -sV -o nofirewallscan 192.168.240.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 10:13 EST
Nmap scan report for 192.168.240.160
Host is up (0.00068s 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 20.65 seconds

(kali@kali)-[~]
$ nmap -sV -o firewallscan 192.168.240.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 10:15 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 3.09 seconds

(kali@kali)-[~]
$ nmap -sV -Pn -o firewallscan2 192.168.240.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 10:15 EST
Nmap scan report for 192.168.240.160
Host is up.
All 1000 scanned ports on 192.168.240.160 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 219.19 seconds
```

