Report di Attività

Traccia: Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato. L'esercizio 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.

Attività Svolte:

1. Ho configurato gli indirizzi IP richiesti dalla traccia sia su Kali Linux che su Windows XP.
2. Successivamente, ho eseguito un ping dalla macchina Windows XP verso Kali Linux per verificare la connettività, ottenendo un esito positivo.
3. Ho disattivato il Firewall di Windows XP.
4. Utilizzando Kali Linux, ho eseguito una scansione con nmap sulla macchina target, utilizzando gli switch –sV per la rilevazione dei servizi e -o per salvare l'output in un file.
5. Dalla scansione, ho rilevato che solo tre porte erano aperte: la 135, la 139 e la 445.
6. Successivamente, ho attivato il Firewall sulla macchina Windows XP.
7. Ho eseguito una seconda scansione con nmap dalla macchina Kali Linux, utilizzando ancora una volta lo switch –sV.
8. Dalla seconda scansione, ho notato che le porte aperte erano la 139 e la 445, mentre la porta 135 non era più accessibile.
9. Inoltre, è stata rilevata una nuova porta aperta, la 2869.

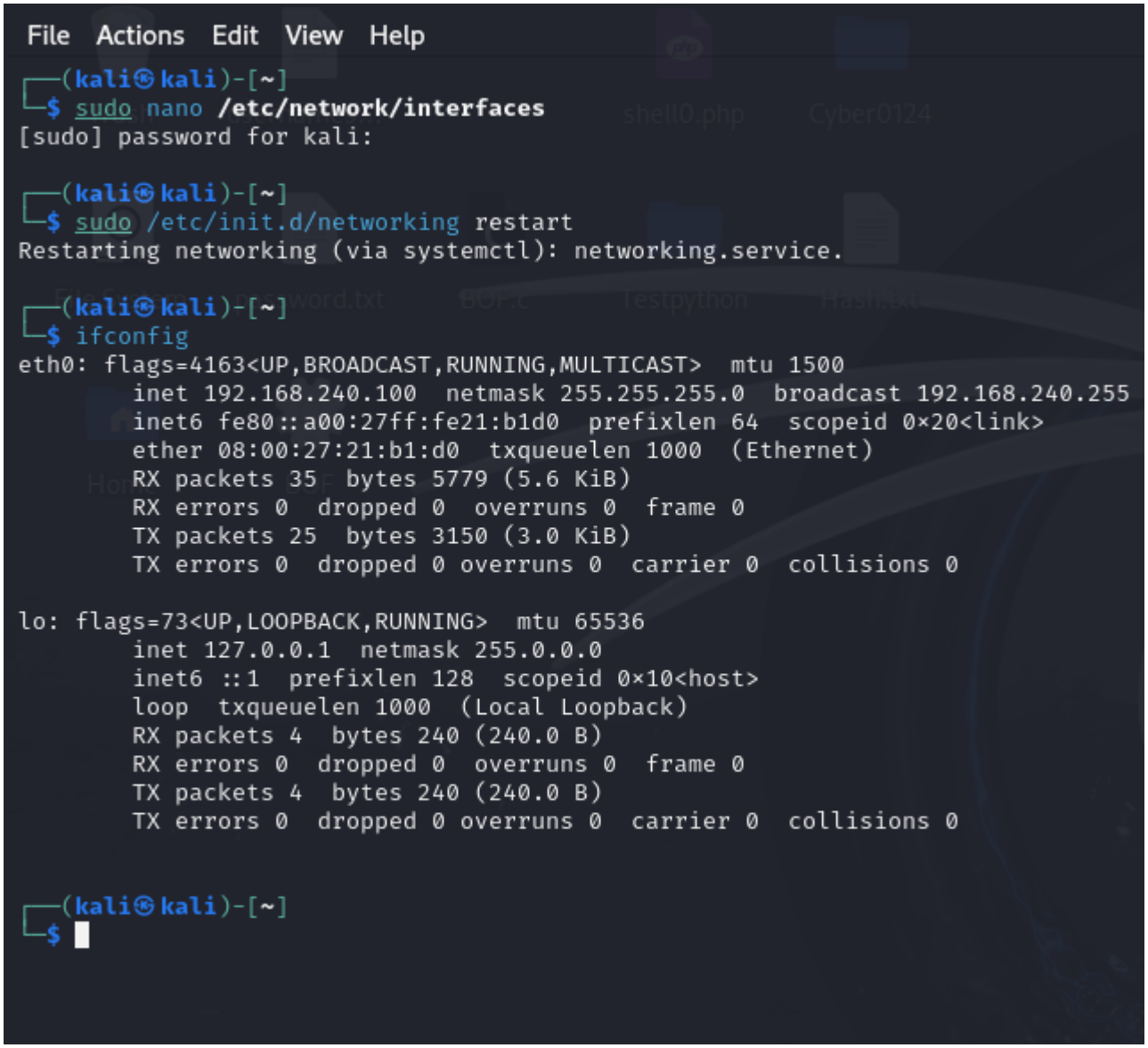
Conclusioni e Motivazioni:

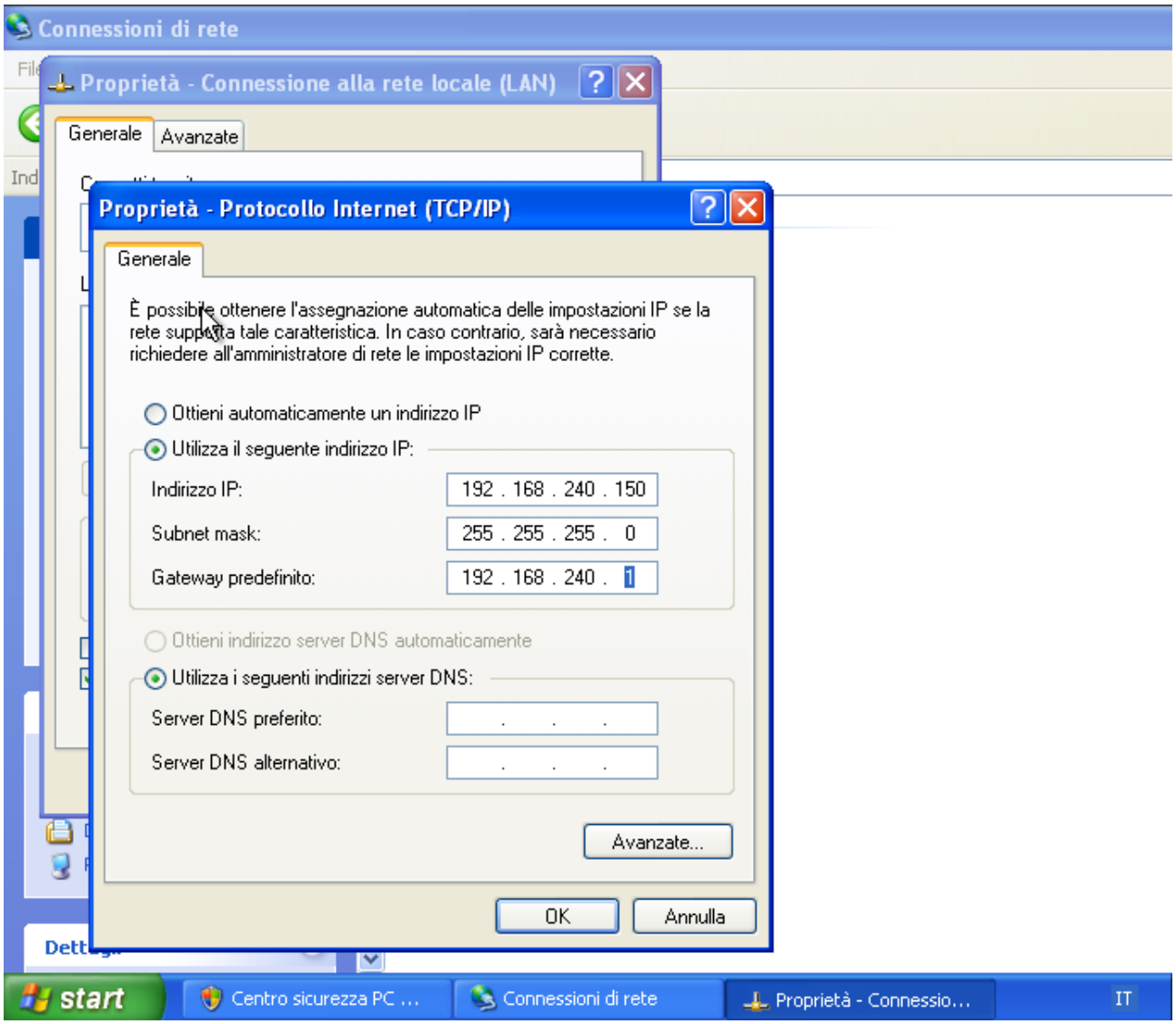
L'attivazione del Firewall sulla macchina Windows XP ha avuto un impatto significativo sulla scansione dei servizi dall'esterno. Le differenze nelle porte aperte possono essere motivate come segue:

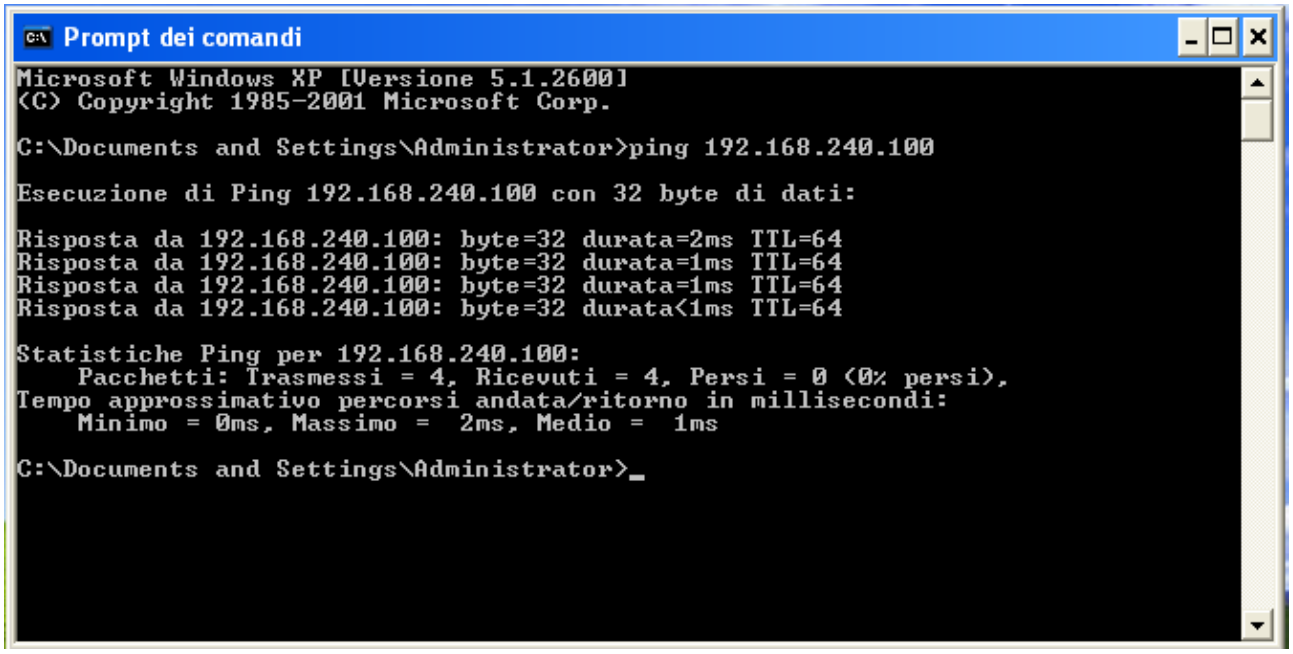
1. **Porta 135 scomparsa:** La porta 135 è comunemente associata al servizio RPC (Remote Procedure Call) utilizzato per la comunicazione tra processi su sistemi Windows. La sua scomparsa dopo l'attivazione del Firewall indica che il Firewall ha bloccato l'accesso a questo servizio, rendendolo non disponibile per la scansione.
2. **Nuova porta 2869 aperta:** La porta 2869 è associata al servizio UPnP (Universal Plug and Play), utilizzato per la scoperta e la gestione dei dispositivi di rete. La sua comparsa dopo l'attivazione del Firewall potrebbe indicare che il Firewall ha permesso l'accesso a questo

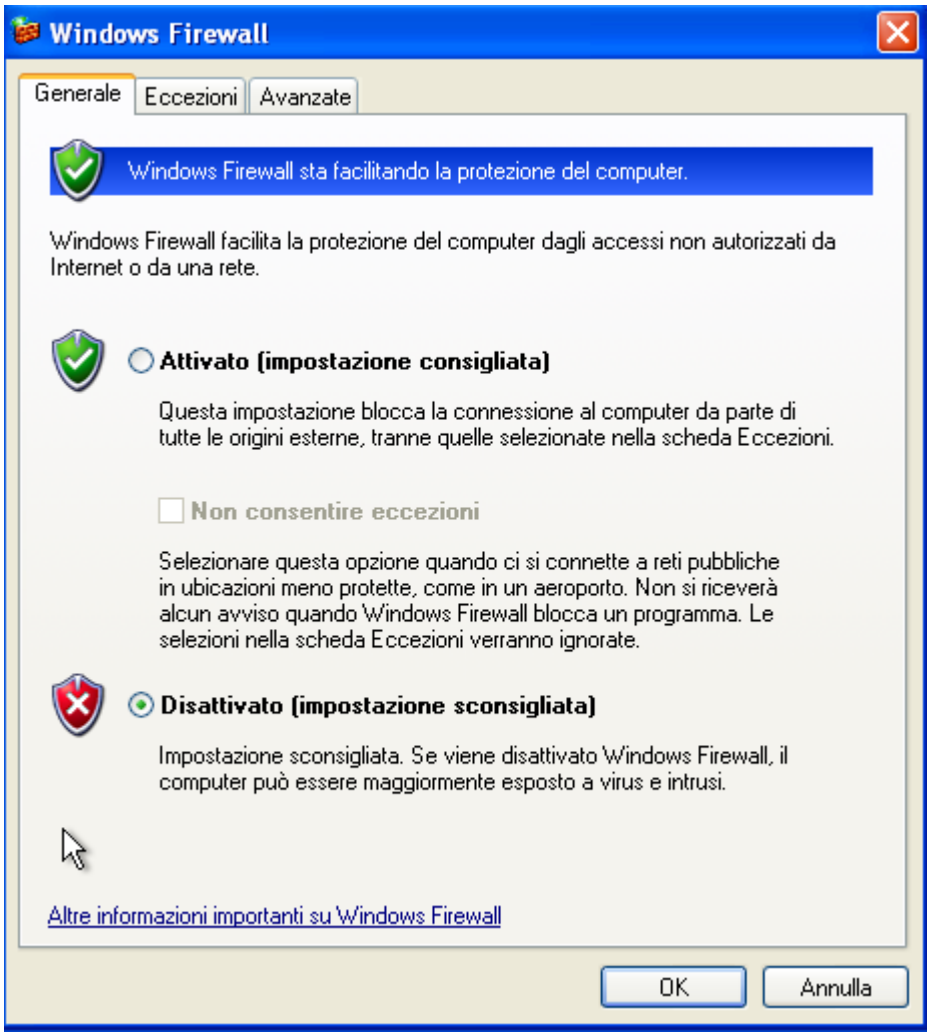
servizio. Tuttavia, è importante notare che UPnP è noto per alcune vulnerabilità di sicurezza, quindi la sua apertura potrebbe esporre la macchina a rischi aggiuntivi.

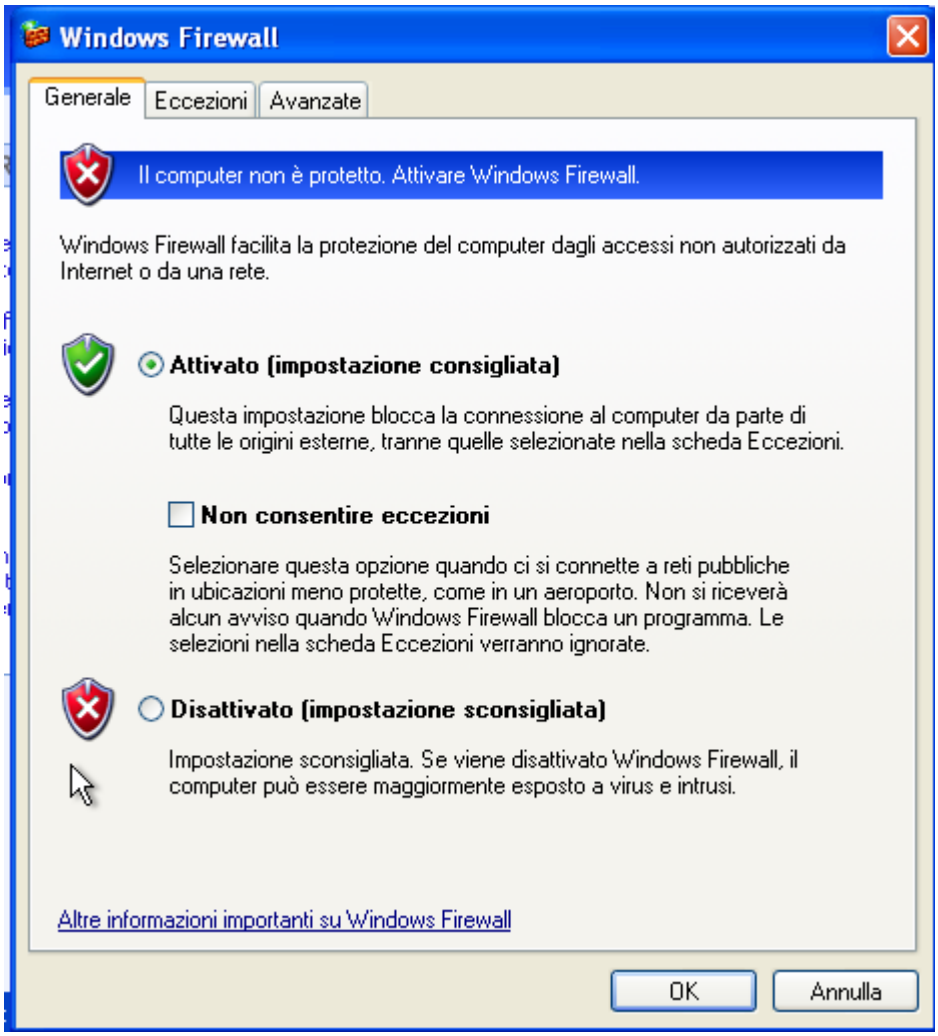
Inoltre, la menzione della differenza tra le versioni a 32 bit e a 64 bit del sistema operativo è teorica e non può essere confermata senza ulteriori prove. Tuttavia, è plausibile che una versione a 64 bit potrebbe implementare misure di sicurezza più avanzate rispetto a una versione a 32 bit.




Connessioni di rete
Proprietà - Connessione alla rete locale (LAN)
Generale
Avanzate
Proprietà - Protocollo Internet (TCP/IP)
Generale
È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.
Ottieni automaticamente un indirizzo IP
Utilizza il seguente indirizzo IP:
Indirizzo IP: 192 . 168 . 240 . 150
Subnet mask: 255 . 255 . 255 . 0
Gateway predefinito: 192 . 168 . 240 . 1
Ottieni indirizzo server DNS automaticamente
Utilizza i seguenti indirizzi server DNS:
Server DNS preferito:
Server DNS alternativo:
Avanzate...
OK
Annulla
start
Centro sicurezza PC ...
Connessioni di rete
Proprietà - Connessio...
IT


Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.240.100
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:
Risposta da 192.168.240.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.240.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 2ms, Medio = 1ms
C:\Documents and Settings\Administrator>_


Windows Firewall
Generale
Eccezioni
Avanzate
Windows Firewall sta facilitando la protezione del computer.
Windows Firewall facilita la protezione del computer dagli accessi non autorizzati da Internet o da una rete.
Attivato (impostazione consigliata)
Questa impostazione blocca la connessione al computer da parte di tutte le origini esterne, tranne quelle selezionate nella scheda Eccezioni.
Non consentire eccezioni
Selezionare questa opzione quando ci si connette a reti pubbliche in ubicazioni meno protette, come in un aeroporto. Non si riceverà alcun avviso quando Windows Firewall blocca un programma. Le selezioni nella scheda Eccezioni verranno ignorate.
Disattivato (impostazione sconsigliata)
Impostazione sconsigliata. Se viene disattivato Windows Firewall, il computer può essere maggiormente esposto a virus e intrusi.
Altre informazioni importanti su Windows Firewall
OK
Annulla




```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -o nofirewallwindows  -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:55 CET
Nmap scan report for 192.168.240.150
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:A6:31:F5 (Oracle VirtualBox virtual NIC)
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 20.53 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -o firewallwindows  -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:03 CET
Nmap scan report for 192.168.240.150
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE      VERSION
139/tcp  open   netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp closed icslap
MAC Address: 08:00:27:A6:31:F5 (Oracle VirtualBox virtual NIC)
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 24.13 seconds
```