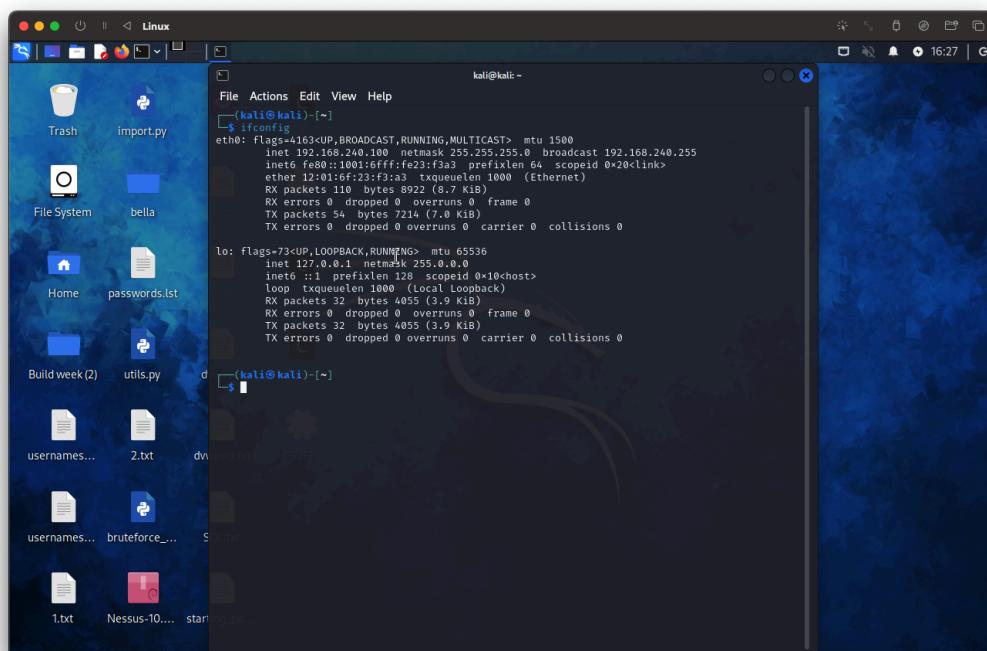
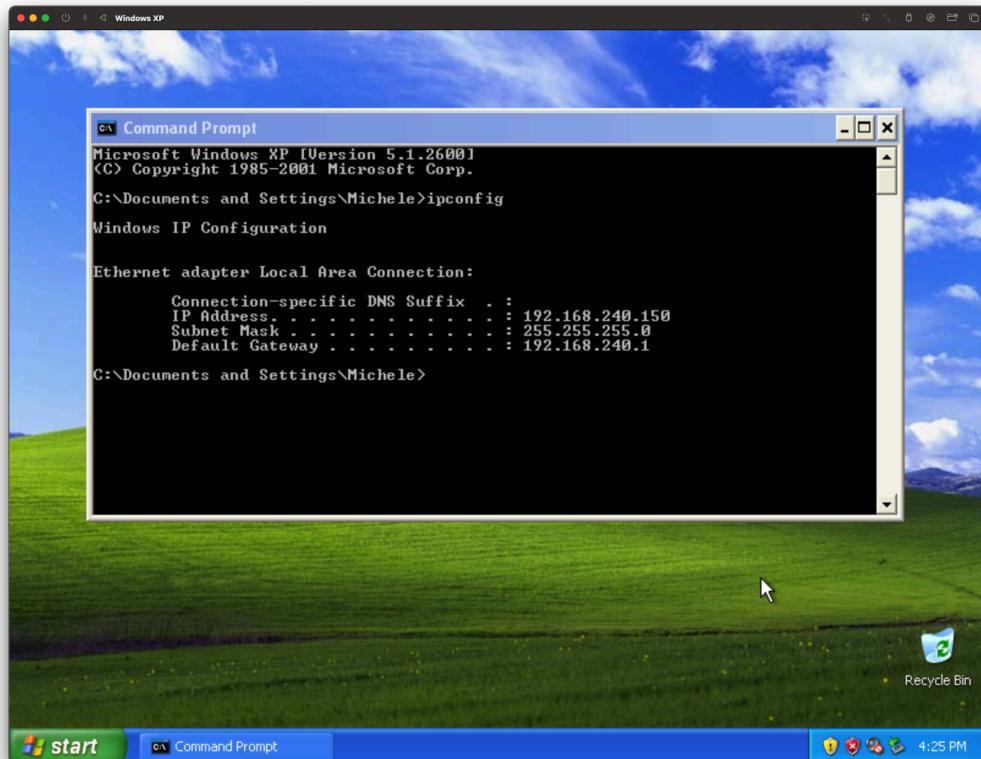


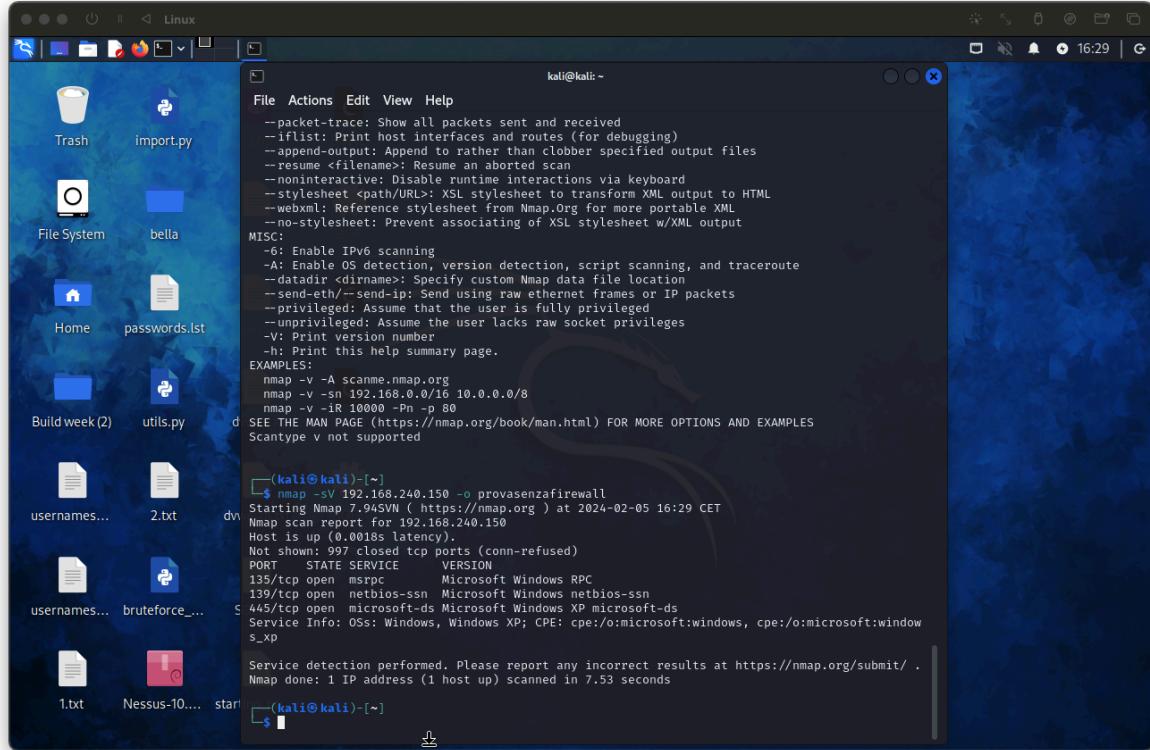
Analisi di Windows XP

Utilizzerò due macchine virtuali, una con kali linux e l'altra con windows XP, con i seguenti ip:



L'analisi effettuata oggi mostra come il firewall di windows xp riesca a mitigare le vulnerabilità del sistema stesso .

Nella seguente immagine viene evidenziato come eseguendo un nmap con il firewall disattivato vengano riscontrate alcune porte aperte quindi potenzialmente vulnerabili:

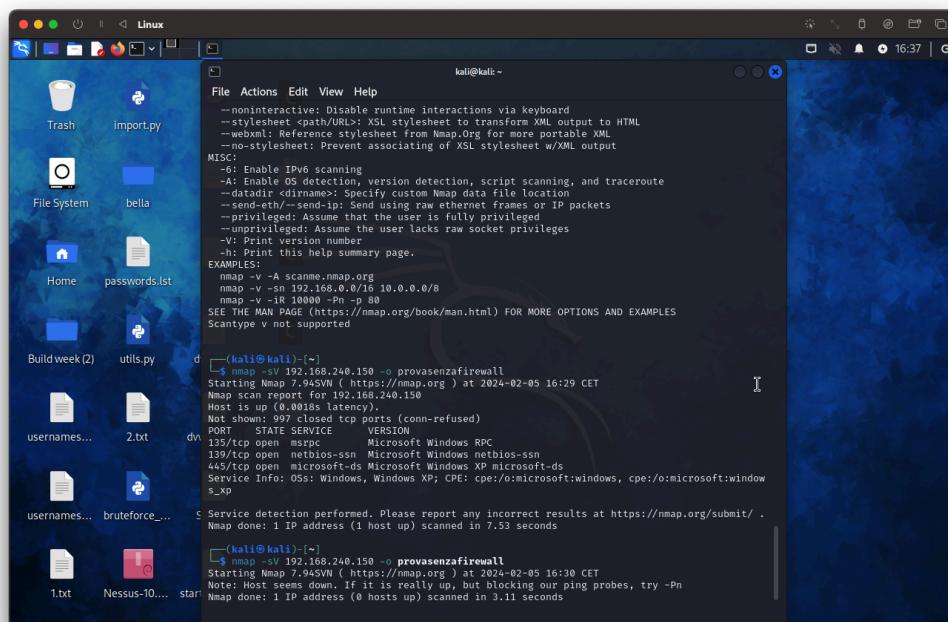


```
kali@kali: ~
File Actions Edit View Help
-packet-trace: Show all packets sent and received
-iffilter: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scannee.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported

(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 --provasenzafirewall
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-02-05 16:29 CET
Nmap scan report for 192.168.240.150
Host is up (0.0018s 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_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds
(kali㉿kali)-[~]
$
```

Successivamente, eseguendo invece una scansione con il firewall attivo, non riscontro queste vulnerabilità, anzi addirittura il firewall non permette il ping.



```
kali@kali: ~
File Actions Edit View Help
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scannee.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported

(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 --provasenzafirewall
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-02-05 16:29 CET
Nmap scan report for 192.168.240.150
Host is up (0.0018s 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_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o provasenzafirewall
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-02-05 16:30 CET
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 3.11 seconds
(kali㉿kali)-[~]
```

Come è possibile notare, il firewall protegge la macchina dagli attacchi alle porte prima evidenziate.

Effettuando una scansione senza ping, è possibile però verificare almeno che il target sia acceso, anche se non è possibile trovare alcuna vulnerabilità.

The screenshot shows a Kali Linux desktop environment with several terminal windows open. The desktop background is a blue floral pattern. The taskbar at the top shows icons for a terminal, file manager, browser, and other utilities. The desktop has a dark theme with light-colored icons.

The terminal windows contain the following Nmap command and its output:

```
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -Sn 192.168.0.0/16 10.0.0.0/8
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scanstype v not supported

[(kali㉿kali)-~]
$ nmap -sv 192.168.240.150 -o provasenzafirewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 16:29 CET
Nmap scan report for 192.168.240.150
Host is up (0.001s 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_s_xp

d Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds

[(kali㉿kali)-~]
$ nmap -sv 192.168.240.150 -o provasenzafirewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 16:30 CET
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 3.11 seconds

[(kali㉿kali)-~]
$ nmap -sv -Pn 192.168.240.150 -o provasenzafirewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 16:31 CET
Nmap scan report for 192.168.240.150
Host is up.
S All 1000 scanned ports on 192.168.240.150 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 202.04 seconds

[(kali㉿kali)-~]
$
```