Traccia W17D1:

EPICODE

Esercizio
Hacking Windows XP

Sulla base di quanto visto nell'esercizio pratico di ieri, formulare delle ipotesi di remediation.

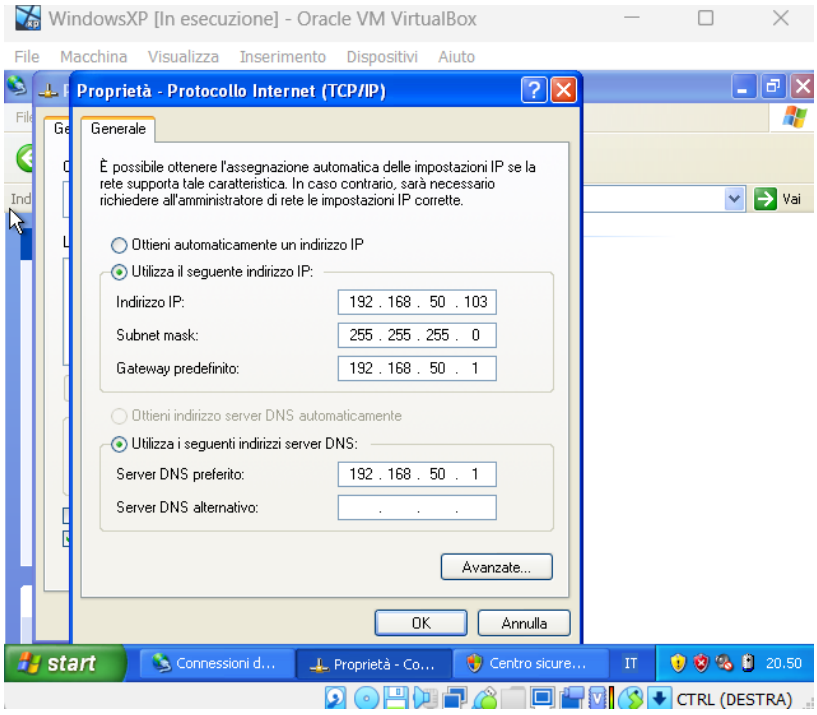
Ad esempio:

1. L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se si, con quale effort?
2. L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?
3. Una volta dentro l'attaccante, può accedere a webcam e/o tastiera, possiamo risolvere queste problematiche?

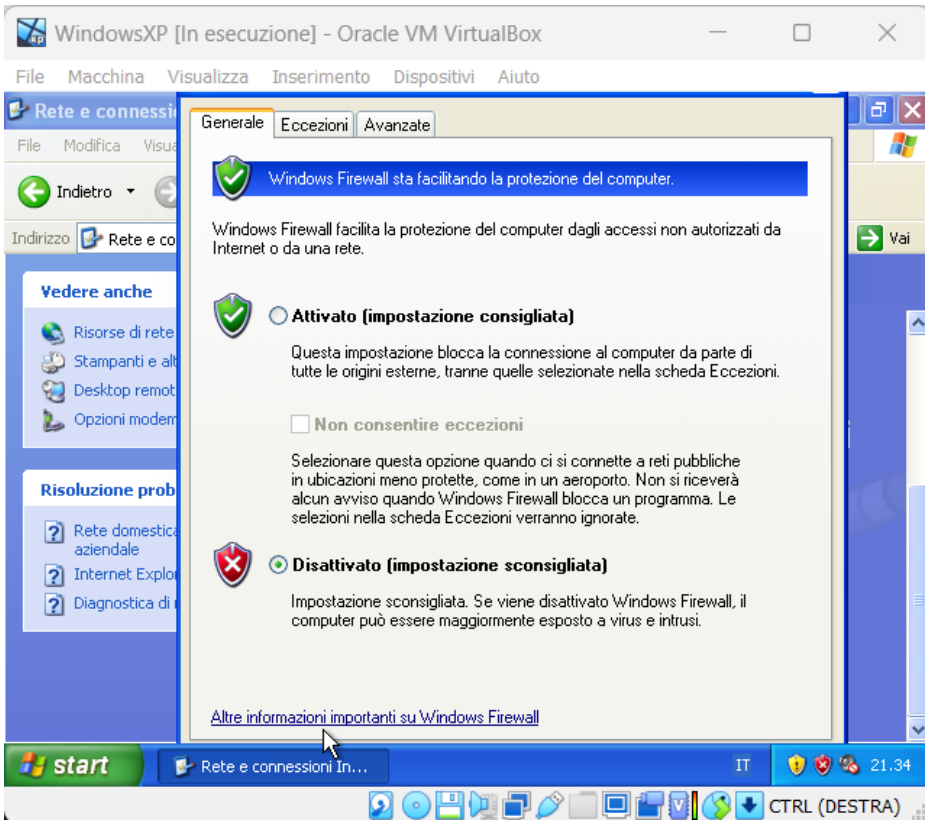
Buon divertimento

Pratica:

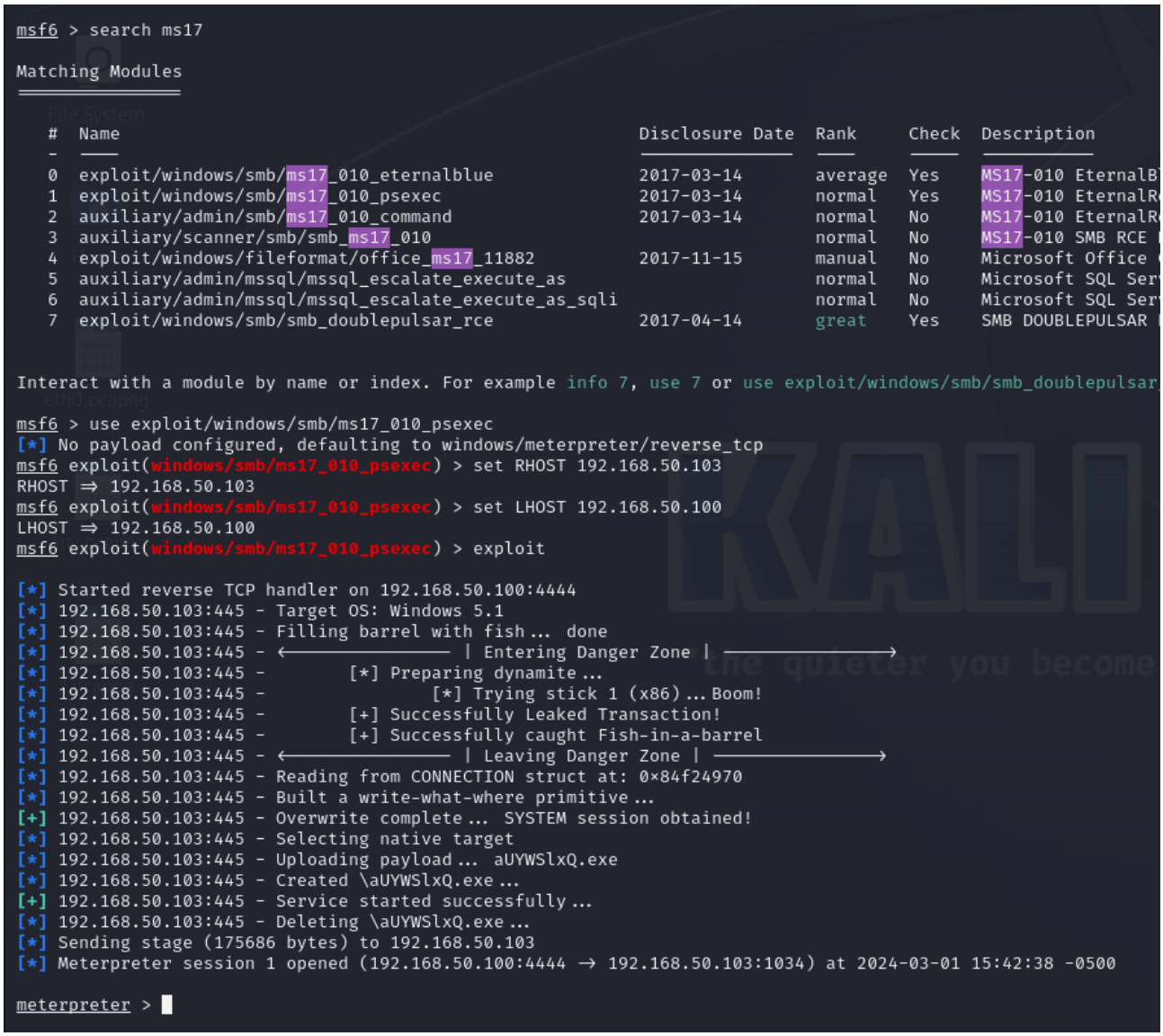
1) Installazione della VM e cambio IP su Windows XP:



2) Disattivazione del Firewall su WinXP:



3) Avvio Metasploit su Kali Linux, ricerca dell'exploit, configurazione dell'RHOST (WindowsXP) E LHOST (Kali Linux):



4) Avvio Meterpreter e controllo tramite ifconfig

```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:95:05:0b
MTU          : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0

meterpreter > sysinfo
Computer        : WINDOWSXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/kali/SKCHkJkx.jpeg
meterpreter > cd /home/kali/SKCHJKx.jpg
[-] stdapi_fs_chdir: Operation failed: The system cannot find the path specified.
meterpreter > cd /home/kali/SKCHJKx.jpeg
[-] stdapi_fs_chdir: Operation failed: The system cannot find the path specified.
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```