TRACCIA 5: BWII

Exploit Windows con Metasploit Traccia Giorno 5:

Sulla macchina Windows XP (o in alternativa Windows 7) ci sono diversi servizi in ascolto vulnerabili.

Si richiede allo studente di:

Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows XP (o in alternativa Windows 7)

Sfruttare la vulnerabilità identificata dal codice MS17-010 con Metasploit.

Requisiti laboratorio Giorno 5:

IP Kali Linux: 192.168.198.100

IP Windows XP (o 7): 192.168.198.200

Listen port (payload option): 9999

Evidenze laboratorio Giorno 5:

Una volta ottenuta una sessione Meterpreter, eseguite una fase di test per confermare di essere sulla macchina target.

Recuperate le seguenti informazioni:

1) se la macchina target è una macchina virtuale oppure una macchina fisica

2) le impostazioni di rete della macchina target

3) se la macchina target ha a disposizione delle webcam attive

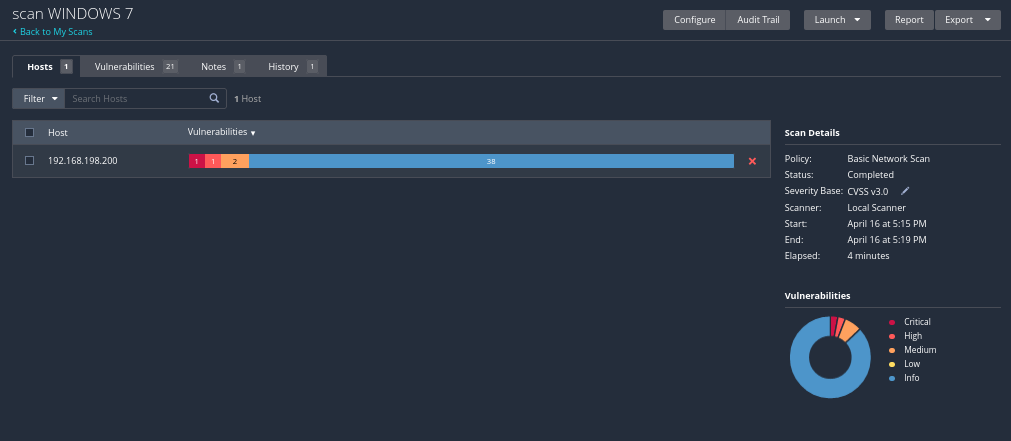
4) recuperate uno screenshot del desktop

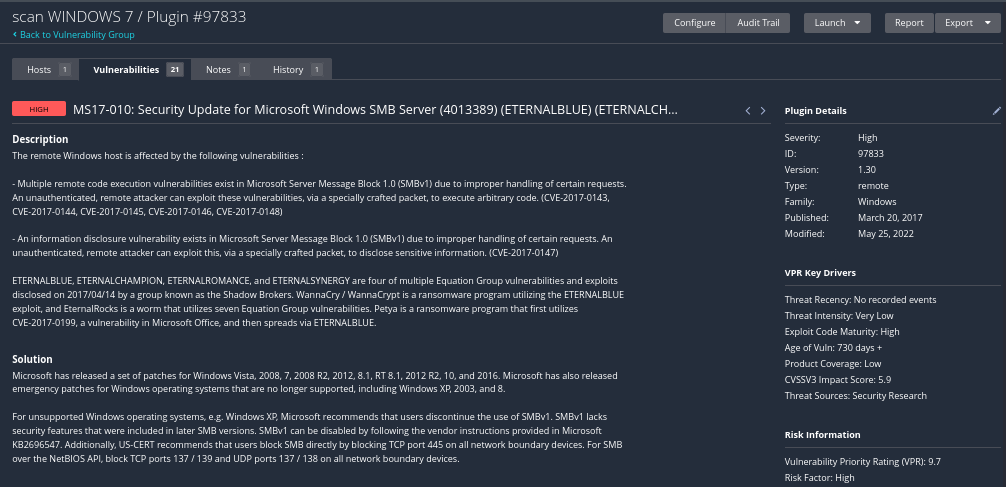
5) i privilegi dell’utente

6) creare una backdoor, iniettarla nel sistema, intercettare la connessione ed avviarla.

GUIDA:

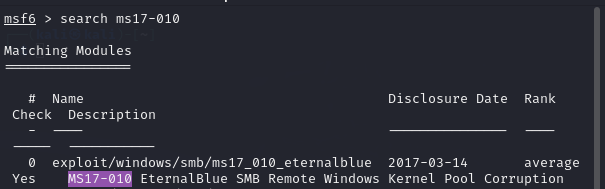
Per prima cosa, facciamo uno scanner delle vulnerabilità con Nessus sulla macchina target Windows 7:



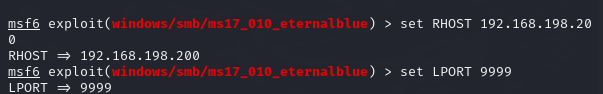


Una volta trovata la vulnerabilità, sfruttiamo msfconsole per creare una sessione meterpreter che ci ridarà varie informazioni sulla macchina target:

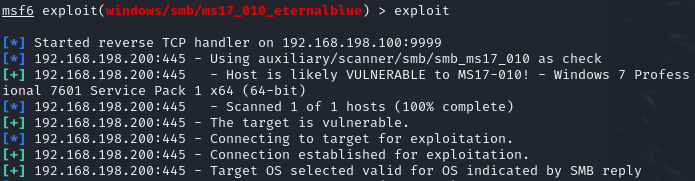
Una volta avviato msfconsole utilizziamo il comando ‘search’ per cercare la vulnerabilità che abbiamo trovato:



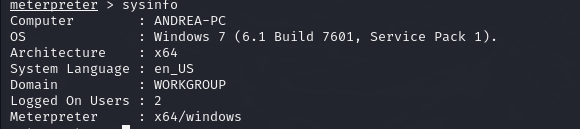
Con ‘use 0’ utilizziamo l’exploit e settiamo come da traccia il RHOST e LPORT.



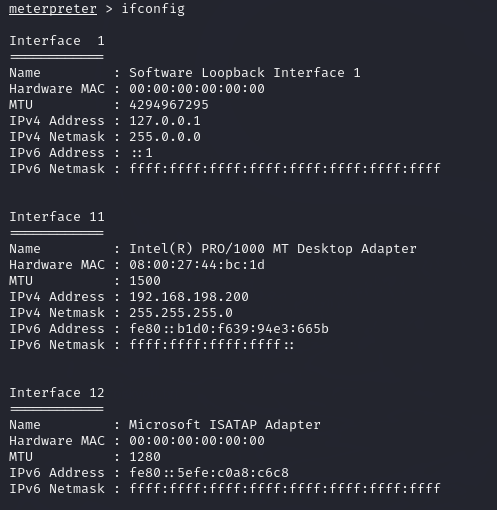
Dopodiché, usiamo ‘run/exploit’ per creare una sessione meterpreter sulla macchina target:



Come prima cosa, facciamo sysinfo per reperire tutte le informazioni di sistema di Windows 7



In seguito, per vedere la configurazione di rete, utilizziamo ifconfig:



Poi, vediamo di recuperare uno screenshot del Desktop della macchina Windows e proviamo a vedere se il target ha a disposizione webcam attive, rispettivamente con i comandi:

-screenshot

-webcam\_list



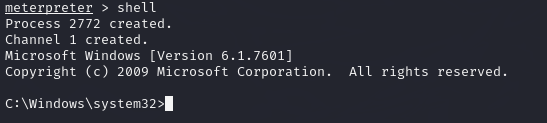


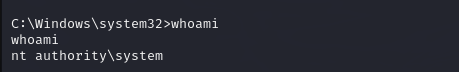
Per ottenere i privilegi d’utente, bisogna utilizzare il comando ‘getuid’, che:



Come vediamo ci restituisce il nome utente e l’ID utente, che sta a indicare che la sessione Meterpreter ha ottenuto i privilegi di sistema

Una volta fatto questo, utilizzeremo il comando ‘shell’, che avvierà una nuova shell interattiva che ti permetterà di eseguire comandi direttamente sul sistema operativo di destinazione:







Dato che con sysinfo non siamo riusciti a vedere se la macchina fosse virtuale, nella shell di Windows che abbiamo creato usare il comando SYSTEMINFO e andando sul BIOS version ci dirà se è una macchina virtuale o meno.



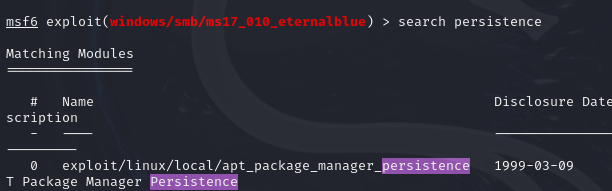
Perfetto, abbiamo ottenuto i privilegi di sistema, mettiamo la sessione in background e continuiamo

Ora, dobbiamo creare una backdoor, iniettarla nel sistema, intercettare la connessione ed avviarla:

Prima di tutto volendo creare una persistenza, cerchiamo su msf6, con il comando ‘search’:

-search persistence

E ci restituirà una serie di payloads:

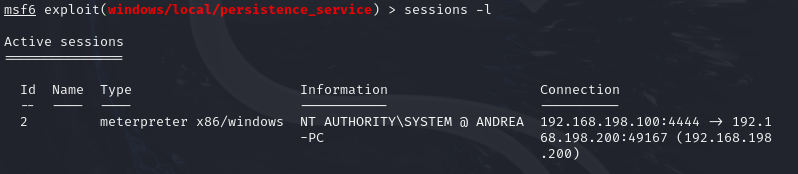


Noi utilizzeremo il 18° che ha il nome:

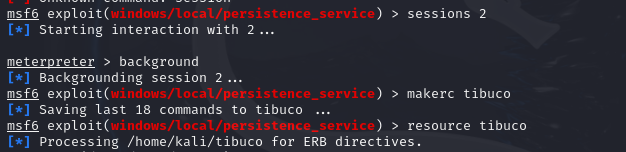
* Windows/local/persistence\_service

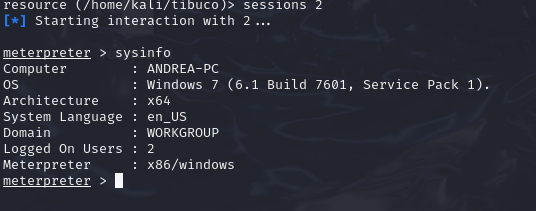


Con ‘sessions –l’, vedo le sessioni attive:

(N.B. Avendo fatto varie prove la sessione negli screenshot può risultare diversa, infatti in seguito userò sessions 2, ma in base alla vostra sessione usate il comando ’sessions [id della vostra sessione], mi scuso per l’incorgruenza)

Infatti, con sessions 2 riesco ad entrare nella sessione di meterpreter.

Come si vede dallo screenshot, una volta fatto ciò, con il comando ’makerc + <path> ’ mfsconsole ci salva gli ultimi comandi che abbiamo usato per entrare in sessione, e con ’resource + <path> ’ avvia esattamente i comandi dati in precedenza, in questo caso il <path> che ho dato è tibuco .(I comandi sono 18 perché ho fatto errori di sintassi)



Come vediamo, siamo rientrati nella sessione di Meterpreter.

mandando il comando ‘resource/-r + <path>’ ci ricollegheremo a questa sessione.