

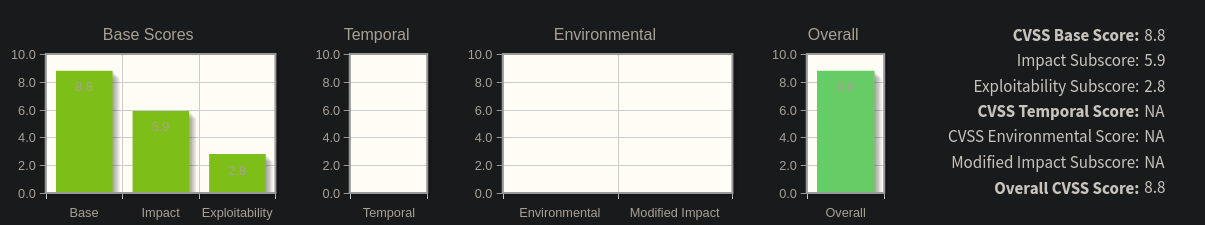
**EJERCICIO 1**

**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.

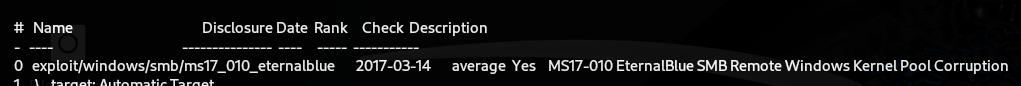
* MS17-010 EternalBlue SMB Remoto de Windows Kernel Pool Corruption para Win8

***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:

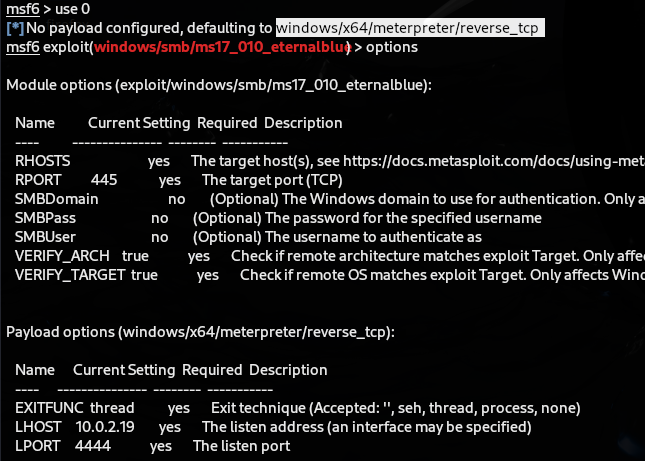
* Módulos de exploit en metasploit:

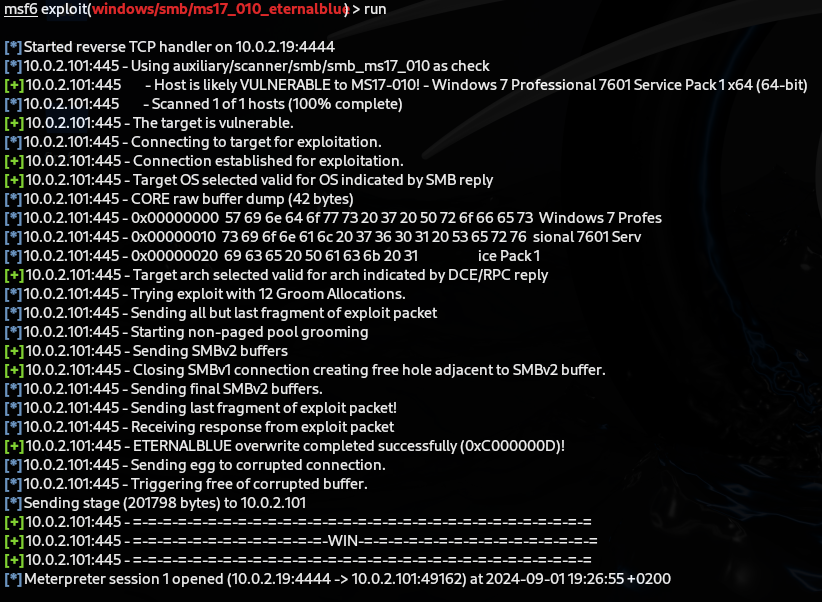


* Payload utilizados:

1. ***windows/x64/meterpreter/reverse\_tcp***

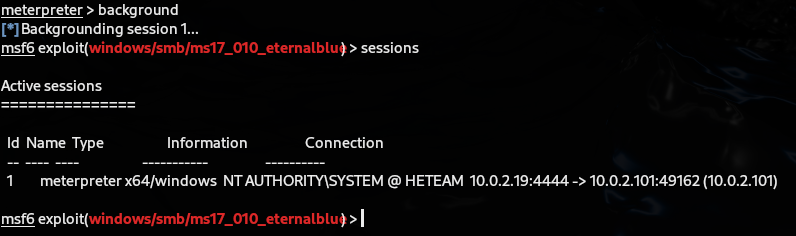
* Configurar y explotar con *meterpreter*



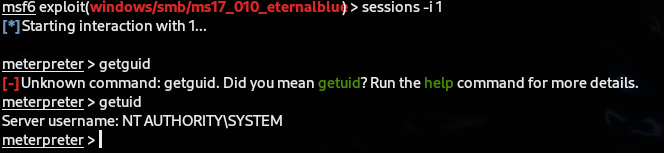




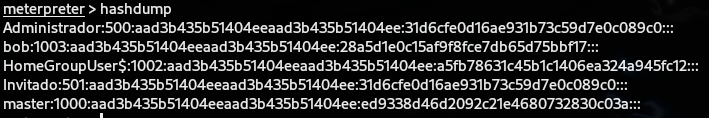
* Dejar la sesión en background y demostrar que la sesión está así.

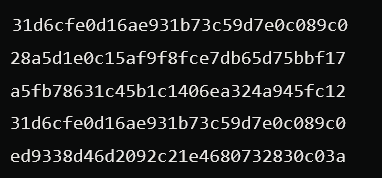


* Recuperación de la sesión

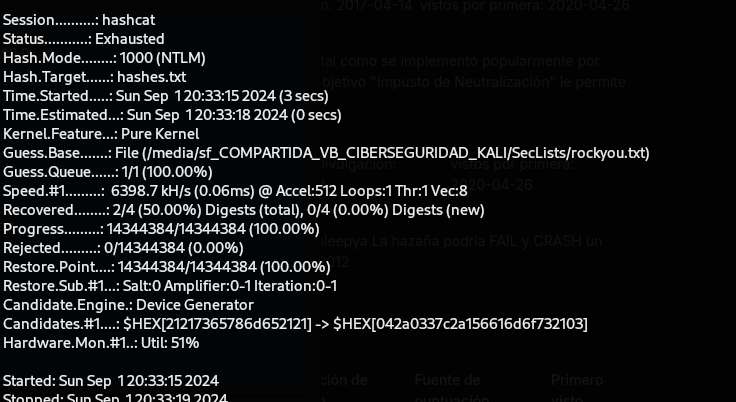


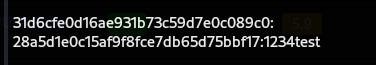
* Realizar volcado de hashes y hacer cracking











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