**Introducción**

El propósito de esta actividad es realizar la explotación de una vulnerabilidad en la máquina virtual *Metasploitable 2* utilizando un script en Python con la librería **pymetasploit3** y la plataforma Metasploit. Esta actividad ilustra el proceso de automatización de un exploit, permitiendo que Metasploit ejecute comandos para comprometer una máquina vulnerable en un entorno controlado.

La vulnerabilidad elegida fue el backdoor del servicio de FTP *vsftpd 2.3.4*, una de las vulnerabilidades más comunes en la máquina Metasploitable 2. El objetivo fue establecer una conexión con la máquina víctima, ejecutar comandos para obtener información y crear un archivo en el sistema comprometido.

**Desarrollo de la Actividad**

**1. Preparación del Entorno de Trabajo**

Se utilizaron dos máquinas virtuales en este proyecto:

* **Kali Linux (atacante)**: La máquina atacante fue configurada para correr Metasploit y realizar la explotación. Se utilizó *msfconsole* para ejecutar el cliente RPC (Remote Procedure Call) y la librería *pymetasploit3* en Python para la automatización del ataque.
* **Metasploitable 2 (víctima)**: Una máquina virtual vulnerable creada con UTM y configurada para simular un entorno inseguro. La máquina tenía varios servicios vulnerables en ejecución, entre ellos el servicio *vsftpd 2.3.4*, que es un servicio FTP con una puerta trasera (backdoor).

**2. Configuración de las Máquinas Virtuales**

* **Configuración de Kali Linux en MacOS**: Para configurar la máquina atacante, se instaló Kali Linux utilizando UTM con arquitectura ARM y se usó qemu, que se instaló con *Homebrew* para convertir las imágenes de disco a un formato compatible con UTM.
* **Configuración de Metasploitable 2**: Se configuró Metasploitable 2 como una máquina víctima. Para obtener la dirección IP de esta máquina, se usó el comando ifconfig, resultando en la IP 192.168.0.110. **A screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generatedA blue screen with white text

  Description automatically generated**

**3. Ejecución de Metasploit**

En la máquina atacante (Kali Linux), se inició Metasploit con el comando msfconsole y se ejecutó el siguiente comando para lanzar el servicio RPC, necesario para que el script en Python pudiera interactuar con Metasploit:

**Preparación del Entorno de Ataque**

1. **Iniciar Metasploit en Kali Linux**:  
   Dentro de la máquina virtual de Kali Linux, se inició Metasploit usando el comando msfconsole. Para habilitar la comunicación entre Python y Metasploit, también se inició el servicio RPC de Metasploit con el siguiente comando: A screenshot of a computer

   Description automatically generated

A computer screen with white text

Description automatically generated

**4. Automatización del Exploit con Python**

Se desarrolló un script en Python utilizando la librería pymetasploit3, el cual permitió automatizar el ataque. El script se conectó al cliente RPC de Metasploit, configuró el exploit *vsftpd 2.3.4*, y ejecutó el payload para interactuar con la máquina víctima.

A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated

En la mquina virtual con Kali Linux se inicio metasploit con msfconsole y creo un cliente RPC para luego con un proyecto con python con la libreria pymetasploit3 conectarse a metasploit y ejecutar un exploit dirigido a la maquina virtual victima metasploit 2, este caso su ip era 192.168.0.110 RHOST

**5. Verificación del Éxito de la Explotación**

Tras ejecutar el exploit, se comprobó si se había abierto una sesión activa en la máquina víctima. El script mostró un listado de las sesiones activas y se ejecutaron varios comandos en la sesión abierta, como whoami, ls y hostname. También se creó un archivo en la máquina víctima llamado *hacked.txt* para demostrar el control adquirido sobre el sistema.

**Capturas de Pantalla**

A screenshot of a computer

Description automatically generated

**Capturas de Pantalla**