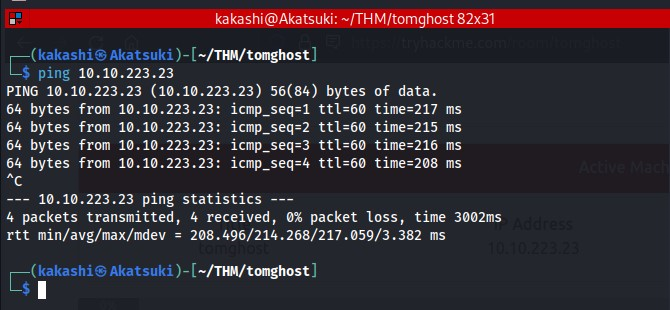
CTF Writeups

Try Hack Me

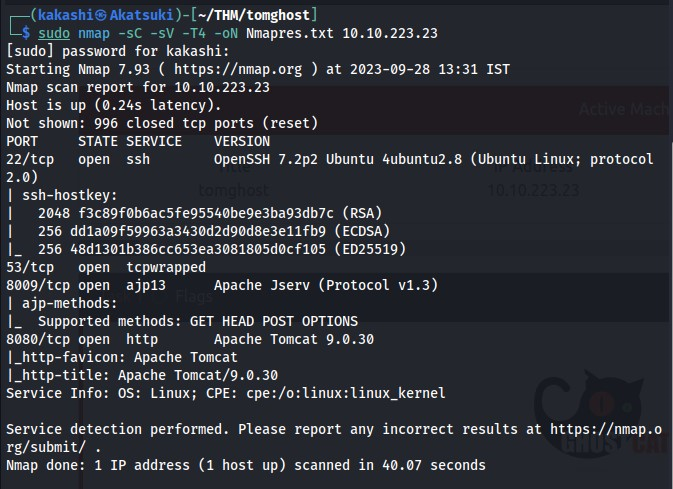
TomGhost

Machine IP: 10.10.223.23

Checking the Connectivity of the target machine.

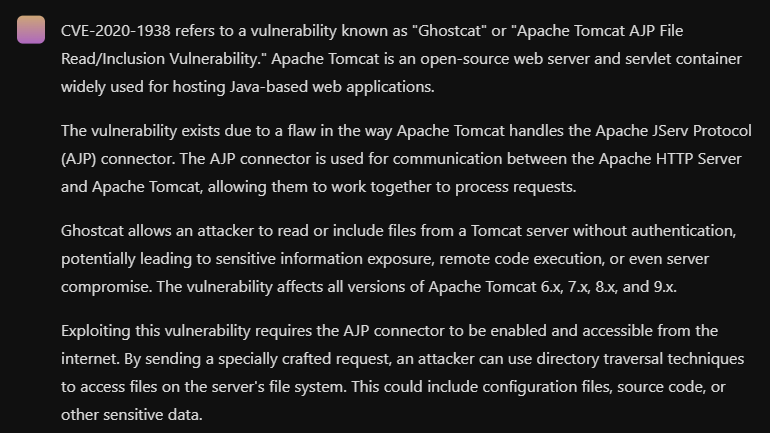


The Target Host is up, Lets check whether there is any open ports that can be useful for exploiting using nmap tool.

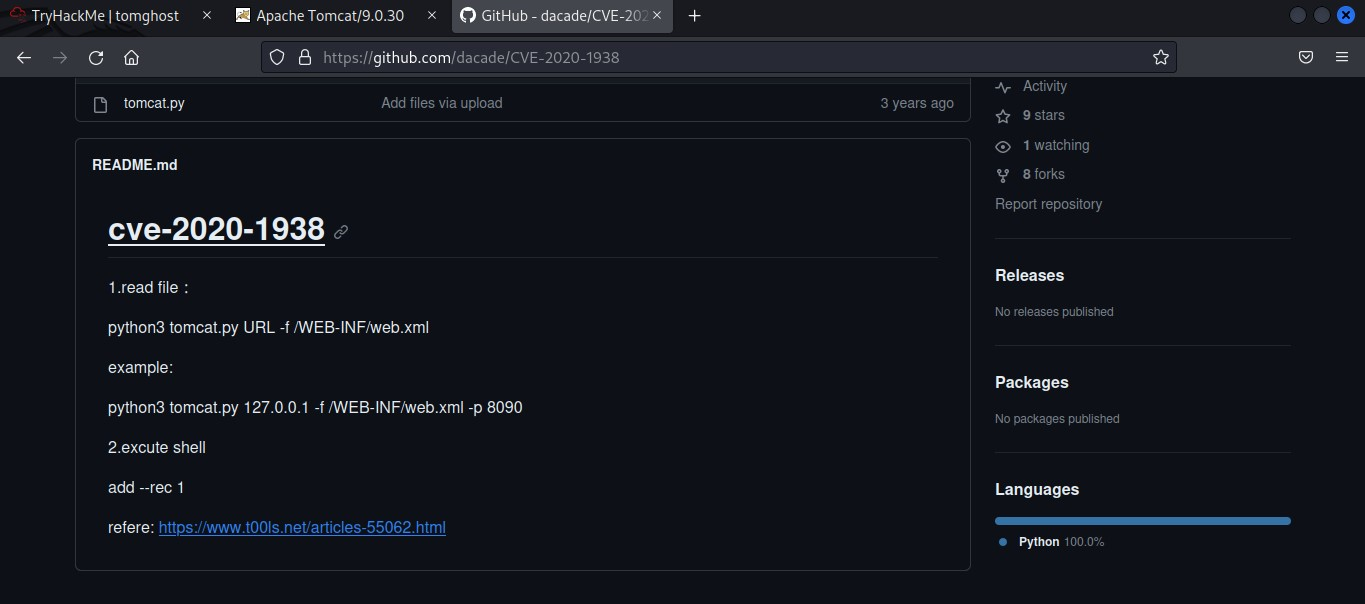


Port **8009** and **8080** is only open, Lets check in browser with this port numbers, We don’t get any information to exploit. Lets surf in browser to check whether there is any vulnerability or exploit related to Apache Jserv or Apache Tomcat 9.0.30. We found this,

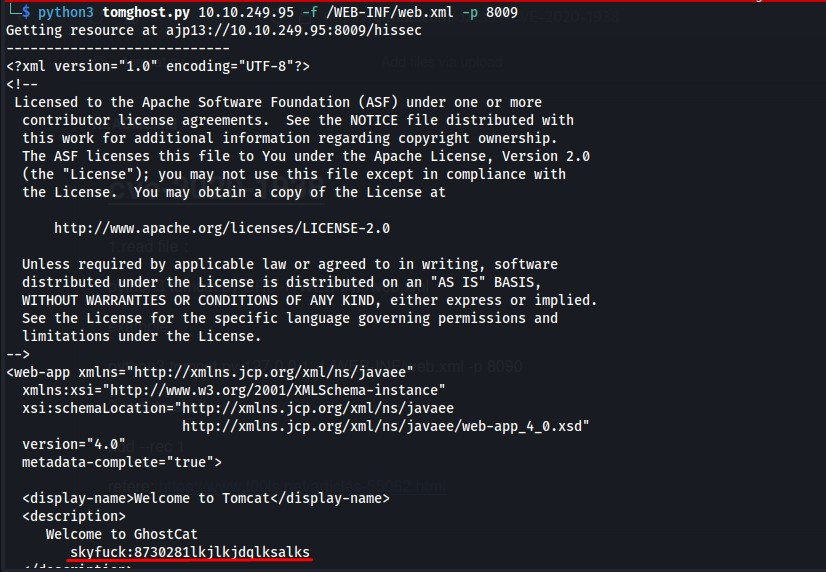
Vulnerability : **CVE-2020-1938**

****

We found this github page where there is python code to exploit the **Ghostcat** Vulnerability.



Run the Python Exploit Code:

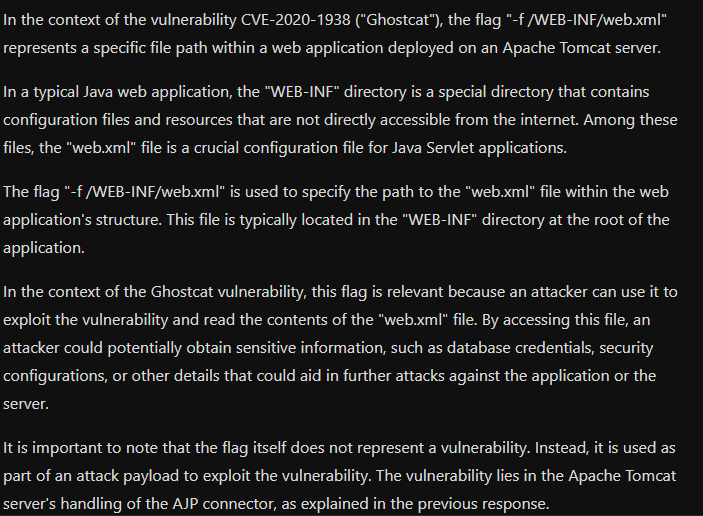


We found the following Credentials,

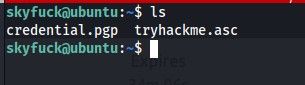
Username : **skyfuck**

Password : **8730281lkjlkjdqlksalks**

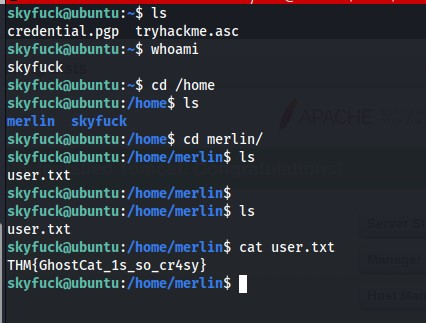
Explaining the Purpose of /WEB-INF/web.xml



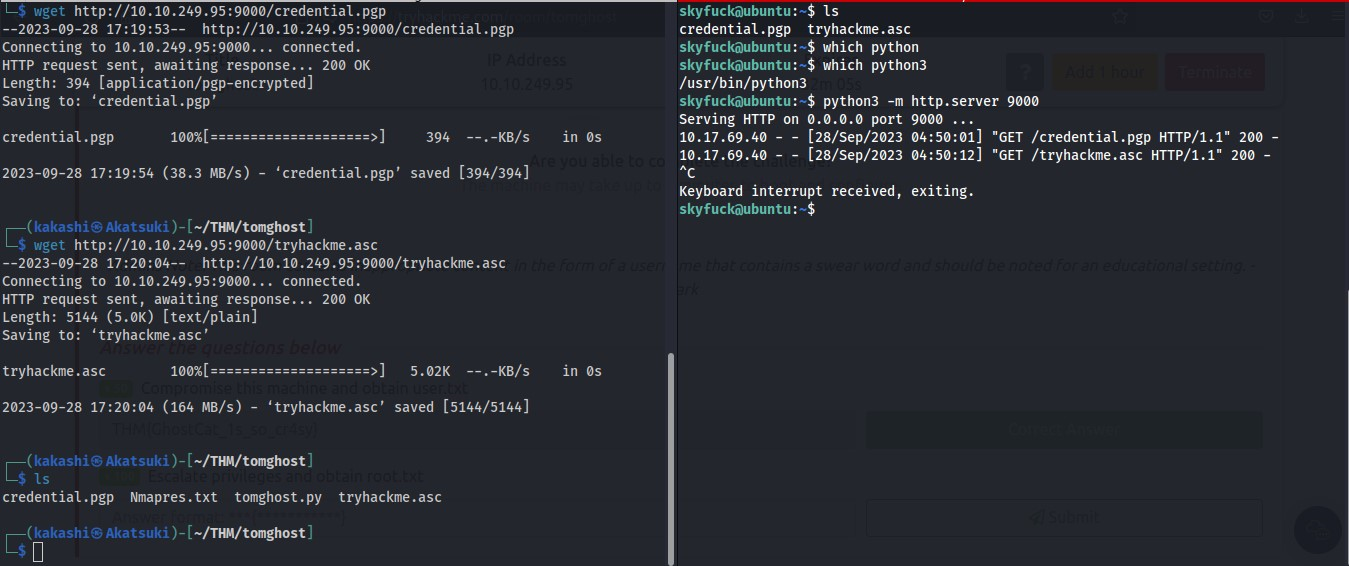
From the Nmap File only open ports are **ssh,** Lets try to login with the above credentials:



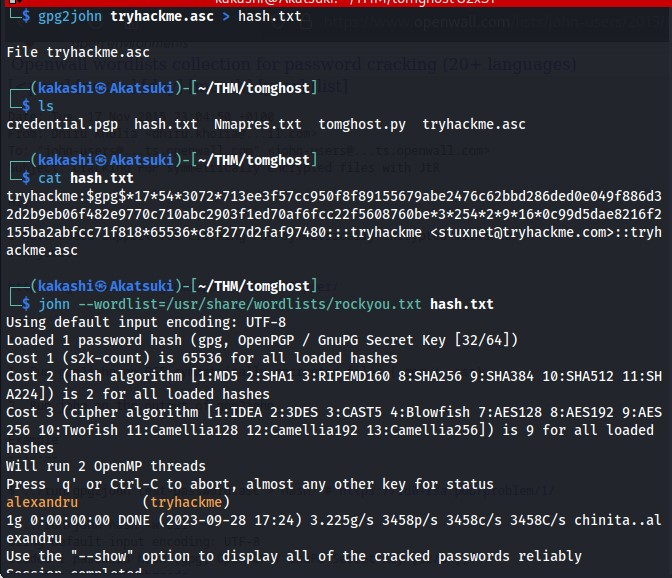
We were able to login as skyuser user, we found 2 files where one file is pgp extension file which means pretty good privacy a data encryption and decryption program. The "credentials.pgp" file likely contains encrypted credentials or sensitive information. To work with this file, you typically need the corresponding private key to decrypt it. and another one is with asc extension means ASCII file, It is likely an ASCII-armored file containing cryptographic keys, Lets keep it aside and dig the file system to check whether flags are there,



We found the user.txt flag. Now lets come to the 2 files mentioned in the above, First download those two files to our attack system using python http.server module.



Lets use **gpg2john** extension in the johntheripper tool to extract the cryptographic key from the tryhackme.asc file,



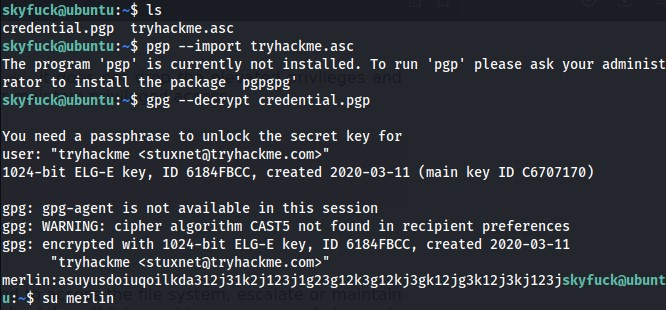
We Found the Password for the crential.pgp file.

Password : **alexandru**

Lets decrypt the credential.pgp file with following commands:

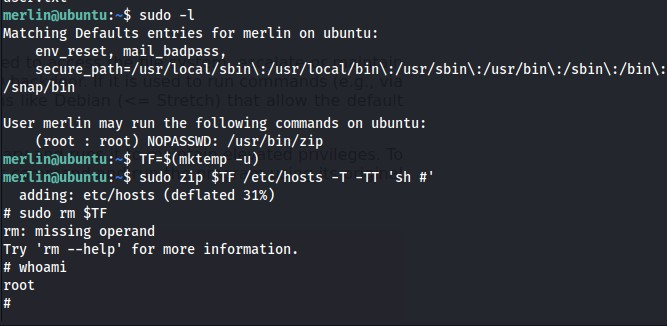
**pgp –import tryhackme.asc**

**gpg –decrypt credential.pgp**

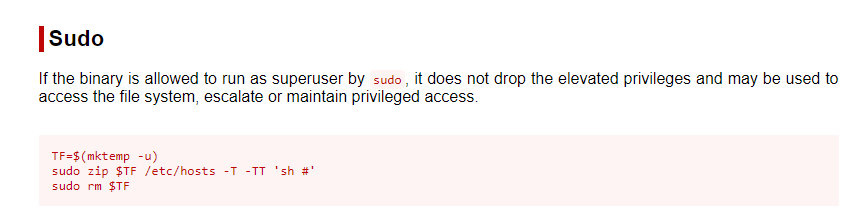


We Found the Credentials for the another user merlin above,

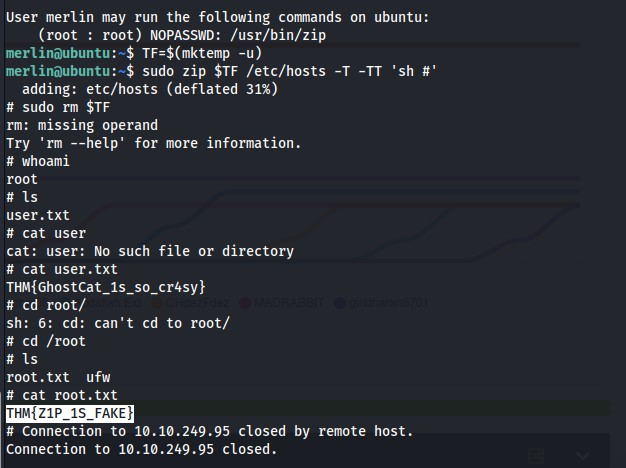
Lets login to that account to find any useful information.



We found that we can escalate privilege to root as the merlin account is vulnerable to zip command. By exploiting the zip command we can spawn a root shell. To find the Privilege Escalation Code for the zip command visit **https://gtfobins.github.io/#** and search for zip command sudo privilege commands.



We have been escalated to root shell, we can search the root flag:



We found the Root Flag.