# *Tomghost*

IP: 10.10.195.16
Name: Tomghost
Goal: Get user.txt and root.txt
LInk: https://tryhackme.com/room/tomghost

user.txt: THM{GhostCat_1s_so_cr4sy}

root.txt: THM{Z1P_1S_FAKE}

# *Enum*

## Obtaining OS

Before performing the scan we must know what we are dealing with and although there are several ways to do it,
we can send an ICMP packet and based on the TTL we can know if it is a machine a LInux or Windows machine.

**ping -c 1 10.10.195.16 => TTL => 61 => Linux**

Linux machines will respond with a TTL of 64 and Windows machines will respond with a TTL of 128.
machines with a TTL of 128.

## Port Scan

After knowing the operating system, we need to know which services are running on the victim machine, but I always divide it into
but I always divide it into two scans, a super fast one and a much deeper and more detailed one.
and detailed.

## Quick scan

**sudo nmap -p- -sS --min-rate 5000 -vvv --open 10.10.195.16 -oA enum/all/allPorts**

Open ports:

- 22 SSH
- 53 Domain
- 8009 ajp13
- 8080 http

Once I know which ports are 100% open, I need to get more information about what is running on each of them, such as the versions,
and this is what the second scan is for, plus I save time by focusing only on the  I save time by concentrating only on the open ports.

## Deep scan

**sudo nmap -p 22,53,8009,8080 -sC -sV 10.10.195.16 -vvvv -T5 -oA enum/deep/deepScan.**

Versions:

- 22 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
- 53 tcpwrapped
- 8009 Apache Jserv (Protocol v1.3)
- 8080 Apache Tomcat 9.0.30

With this scan **I now know that the operating system is Ubuntu**, as well as the versions that could be vulnerable to exploits already done. be vulnerable to exploits already made.

## Scanning the web page

Also this machine is a web server so I will try to get more information using the
following tools:

- whatweb
- wappayzer

**whatweb http://10.10.195.16:8009**

**whatweb http://10.10.195.16:8080**

With the whatwebb tool I couldn't get much information so I'll use the browser and
wappalyzer.

Wappalyzer didn't help me to get more information either, so I will search for directories. Another thing that is
worth noting is that port 8009 won't let me in. So I will concentrate on port
8080.

## Directory lookup

**gobuster -u http://10.10.195.16:8080 -w ~/SecLists-master/-Discovery/Web-Content/common.txt -t 100 -o enum/directories.txt**

Discovered directories:

- docs
- examples
- favicon.ico
- host-manager
- manager

The directories helped me to remember that tomcat has some default credentials and that with them I could log in to the
the administration page.

username: tomcat
password: s3cret

These default credentials are shown by default when you get an error or something in the software, since
they were NOT removed by the administrator.

After searching for a while how to enter the administration page and not succeeding I went back to tryhackme and
saw an image that caught my attention, it was a ghost cat, so I searched the internet and saw that it was a tomcat vulnerability.

# Ghostcat - CVE-2020-1938

It is a vulnerability that affects versions 6.x,7.x,8.x and 9.x that **allows the remote execution of commands or RCE**.
RCE, **to execute this vulnerability correctly we must use port 8009 and ajp.** It also allows
the **reading of files to which a user should not be authorized**, the files could be:

- WEB-INF
- META-INF

Or really any file, for this we must take the following via ServletContext.getResourceAsStream().

The reality is that RCE is not "enabled" by default, to achieve this we must have a vulnerable version of tomcat
which allows arbitrary file uploads and in conjunction with reading files, we could gain access to the system.
access to the system.

# *FootHold*

I found the following exploit on Github, although there are many available on the internet, but this one is very good because it
it uses python3.

https://github.com/Digitemis/Ghostcat/blob/master/exploit.py

**In order to use it you need to give as argument the file to read and the IP of the victim server, as follows:**

**python3 exploit.py read /WEB-INF/web.xml 10.10.195.16**

I ran the script and got some credentials!

**user: skyfuck**
**password: 8730281lkjlkjdqlksalks**

These credentials might work with SSH, if they don't work I will try to

exploit ghostcat in a more complex way!

The credentials were correct and now I'm inside the system, also I found the first flag!

# *PrivEsc*

To get the next flag I need to escalate my privileges, although I don't think it can be directly to root, since there is another user called merlin.

Something that caught my attention were the following two files:

- credential.pgp
- tryhackme.asc

Maybe they can contain very useful information, especially the first one, I will try to decipher it!

The first file **may contain some kind of password** and I tried to decrypt it with the following
command:

**gpg --decrypt credential.pgp**

But I got the following error, which confirms that I need a word or something to decrypt it:

**gpg: decryption failed: secret key not available.**

I think I will have to get the password with both files and with JohnTheRIpper, but first I need to get the two files.

**scp skyfuck@10.10.39.193:/home/skyfuck/credential.pgp .**
**scp skyfuck@10.10.39.193:/home/skyfuck/tryhackme.asc .**

But before cracking the password I need to combine the files to get a hash that john can understand.

**/data/src/john-1.9.0-jumbo-1/run/gpg2john tryhackme.asc > gpg.hash**

Now that I have the hash I can try to crack the password:

**/data/src/john-1.9.0-jumbo-1/run/john gpg.hash --wordlist=/data/-src/wordlists/rockyou.txt**

**The password is alexandru**, with this password now we can decrypt what is in the file crendential.pgp file.

What the file contains are the credentials of the user merlin:

**merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12**

Once in the **/home directory of the user merlin we can find the first flag**, but we still need to escalate privileges to be the root user.

As always I will run sudo -l to see if I can run something as the root user!

**sudo -l => /usr/bin/zip**

I can **run zip WITHOUT password and as root, to escalate my privileges** I'll look at https://gtfobins.github.io/ is a great resource for privilege escalation!

These are the commands I need to use to escalate privileges:

1. **TF=$$(mktemp -u**
2. **sudo zip $TF /etc/hosts -T -TT 'sh #'**

And that's it, so I could read the next and last flag!