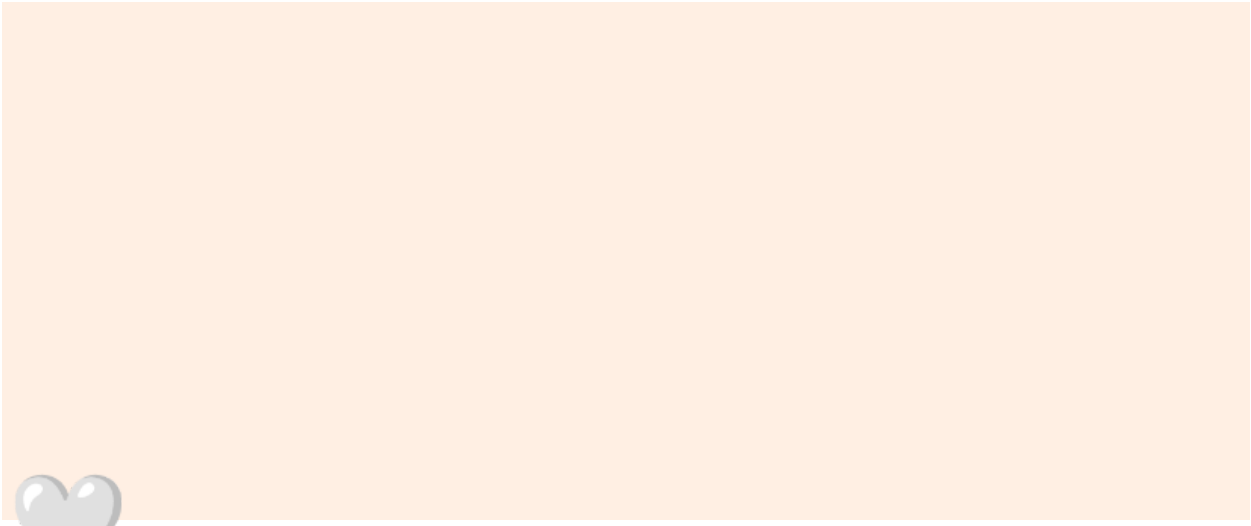


WriteUp Hack The Box Cap

https://github.com/diurs/Hackthebox-Writeups

🗨 Box

Name : Cap

Profile: www.hackthebox.eu

Difficulty: Easy

Os: Linux

📌 Penetration Testing Methodology

1. **Recon**
    - Nmap
2. **Enumeration**
    - Web Enumeration
    - Wireshark
    - SSH
3. **Privilege Escalation**

- Capabilities Binary

Начнем со сканирования NMAP. Это первый и самый важный шаг при изучении машины.

```
nmap -T4 -sC -sV 10.10.10.245 -Pn
```

21/tcp open ftp   vsftpd 3.0.3

22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2

80/tcp open http   gunicorn

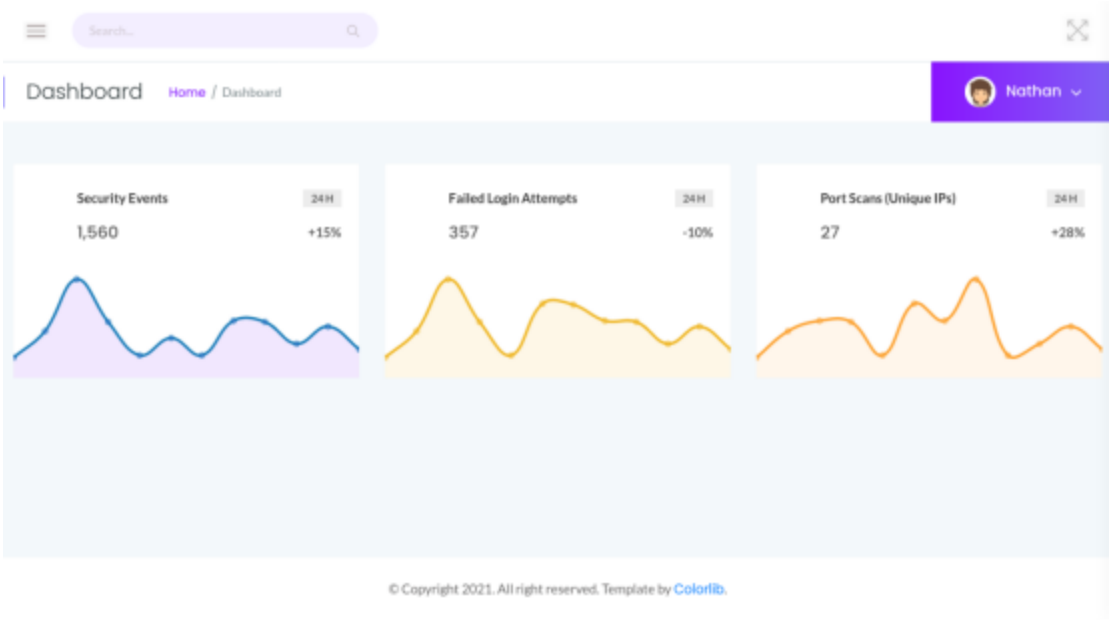
Результат сканирования показывает, что у нас есть 3 важных порта :

21 - ftp-сервер22 - ssh-соединение

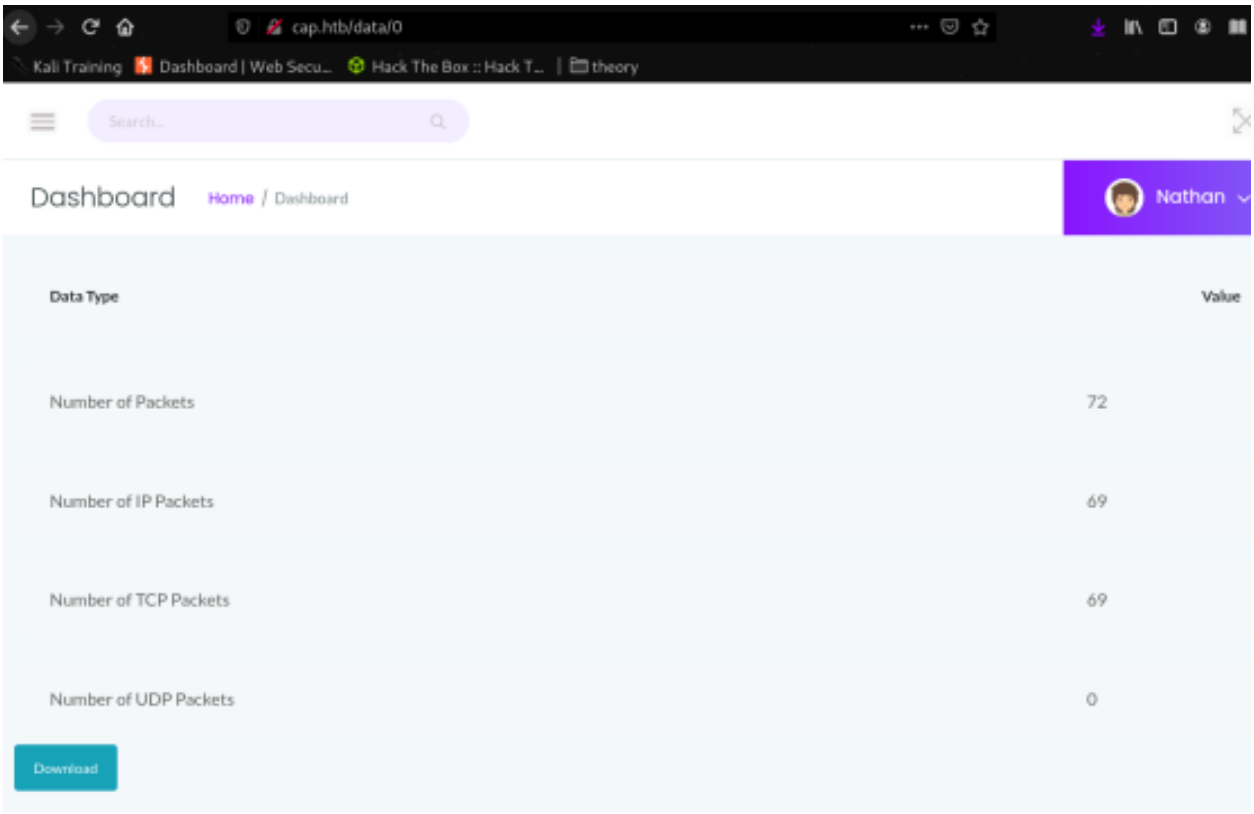
80 - служба HTTP

У нас нет анонимного доступа к ftp. Перейдем к веб-серверу. Добавим ip 10.10.10.245 в /etc/hosts и откроем веб-страницу.

Мы видим перед собой dashboard , который показывает результат мониторинга сети.



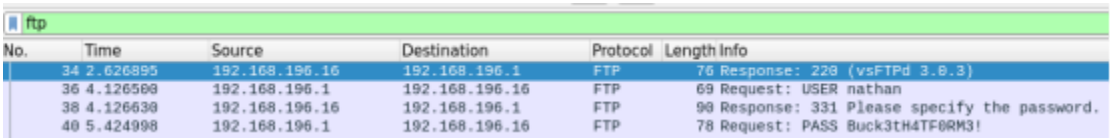
При дальнейшем изучении мы находим информацию о пакетах с возможностью скачать PCAP. В будущем мы можем проанализировать их через Wireshark. Загрузим PCAP и обнаружим , что он не содержит никакой интересной информации. Заметим, что изменение цифры в конце URL-адреса приводит к новой информации о пакете.



По адресу cap.htb/data/0 пакет выглядит интересным, загрузим его и откроем в Wireshark.

```
wireshark 0.pcap
```

Удача нам улыбнулась и мы видим учетные данные для FTP

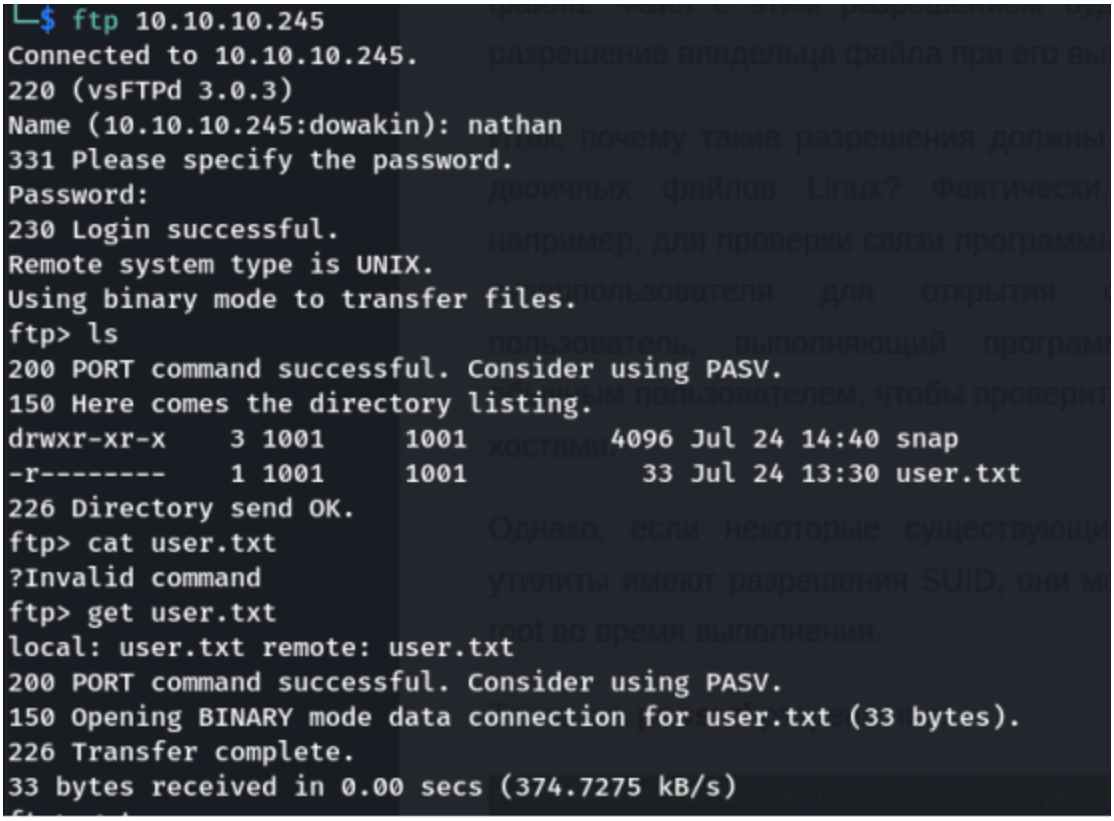


```
USER nathan
 331 Please specify the password.
PASS Buck3tH4TF0RM3!
 230 Login successful.
```

💡 Имя пользователя: nathan и пароль: Buck3tH4TF0RM3!

Подключимся к FTP, используя указанные выше учетные данные. Похоже, FTP-сервер обслуживает домашний каталог пользователя.

```
ftp 10.10.10.245
```



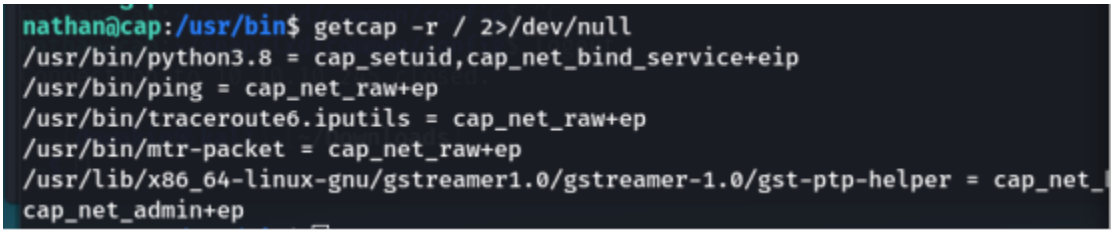
Сразу получаем пользовательский флаг

```
cat user.txt
```

Мы входим в SSH, используя те же учетные данные FTP, и это работает

```
ssh nathan@10.10.10.245
```

Я искала SUID биты, разрешения sudo , другие возможности, которые могли бы повысить привилегии.
Удалось найти cap_setuid в двоичном файле Python 3.8

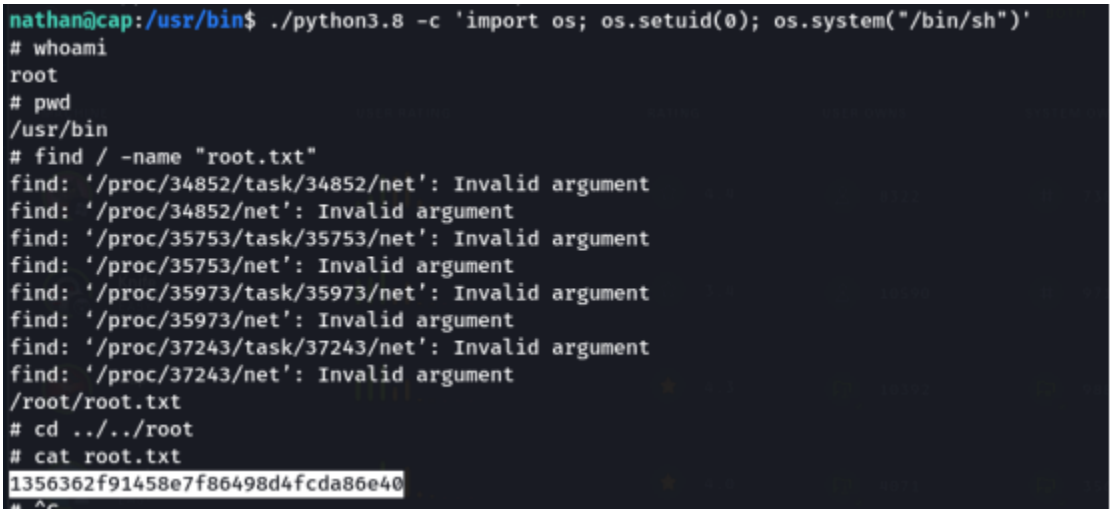


GTFOBins поможет с оболочкой. https://gtfobins.github.io/gtfobins/python/#capabilities

Так же можно использовать linPEAS для автоматизации.
https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

```
./python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

Теперь мы root




```
cat root.txt
```