Network Traffic Analysis Using Wireshark

Submitted By: Deepak

Internship Program: Cyber Security Internship

Organization: Codectechnologies

Tools Used: Wireshark, Kali Linux

Declaration

I hereby declare that this project titled 'Network Traffic Analysis Using Wireshark' is my original work carried out as part of my cybersecurity internship. All activities were performed in a controlled and ethical environment for learning purposes only.

1. Introduction

Network traffic analysis is a critical component of cybersecurity that involves monitoring, capturing, and inspecting network packets to detect malicious activities and performance issues. This project focuses on analyzing network traffic using Wireshark.

2. Objective

- Capture live network traffic
- Analyze TCP, HTTP, and DNS protocols
- Detect suspicious patterns such as port scanning and http plain texts
- Understand attacker behavior

3. Tools and Environment

Tools Used:
- Kali Linux
- Wireshark

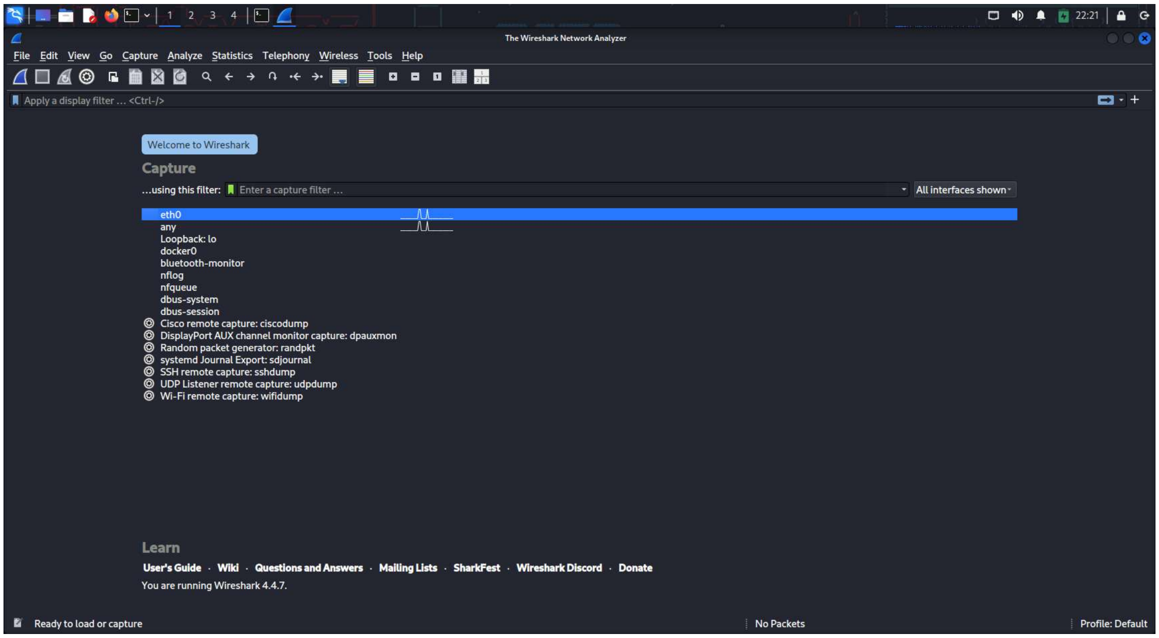
Environment:
- Local controlled lab setup
- No real-world systems targeted

4. Methodology

1. Selected network interface
2. Captured live traffic
3. Generated different traffic types
4. Applied Wireshark filters
5. Analyzed captured packets

5. Traffic Capture

Wireshark was used to capture live network traffic.


1 2 3 4
22:21
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

```
Capture
…using this filter: Enter a capture filter …
eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
```

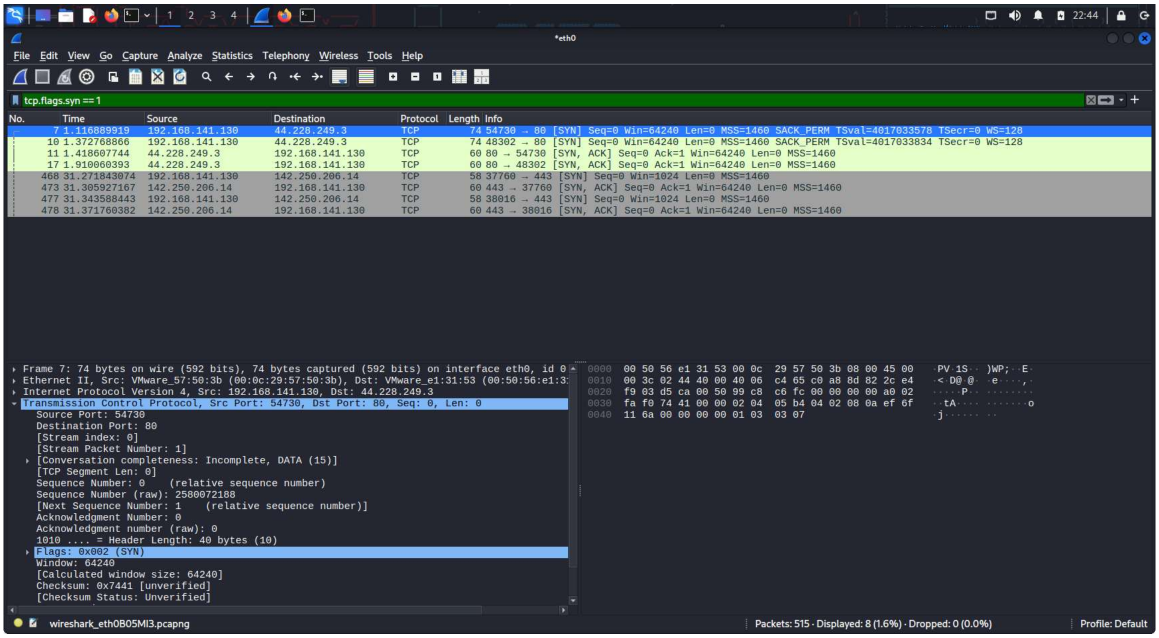
You are running Wireshark 4.4.7.

Ready to load or capture | No Packets | Profile: Default

6.1 TCP Three-Way Handshake Analysis

Filter Used: tcp.flags.syn == 1

Explanation of SYN, SYN-ACK, and ACK packets.


1 2 3 4
22:44
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1

No.  Time          Source           Destination      Protocol Length Info
   7 1.116889919   192.168.141.130  44.228.249.3     TCP      74 54730 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4017033578 TSecr=0 WS=128
  10 1.372768866   192.168.141.130  44.228.249.3     TCP      74 48302 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4017033834 TSecr=0 WS=128
  11 1.418607744   44.228.249.3     192.168.141.130  TCP      60 80 → 54730 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  17 1.910060393   44.228.249.3     192.168.141.130  TCP      60 80 → 48302 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 468 31.271843074  192.168.141.130  142.250.206.14   TCP      58 37760 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 473 31.305927167  142.250.206.14   192.168.141.130  TCP      60 443 → 37760 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 477 31.343588443  192.168.141.130  142.250.206.14   TCP      58 38016 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 478 31.371760382  142.250.206.14   192.168.141.130  TCP      60 443 → 38016 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
```

```
› Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_57:50:3b (00:0c:29:57:50:3b), Dst: VMware_e1:31:53 (00:50:56:e1:3:
› Internet Protocol Version 4, Src: 192.168.141.130, Dst: 44.228.249.3
⌄ Transmission Control Protocol, Src Port: 54730, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 54730
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
  › [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2580072188
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  › Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x7441 [unverified]
    [Checksum Status: Unverified]
```

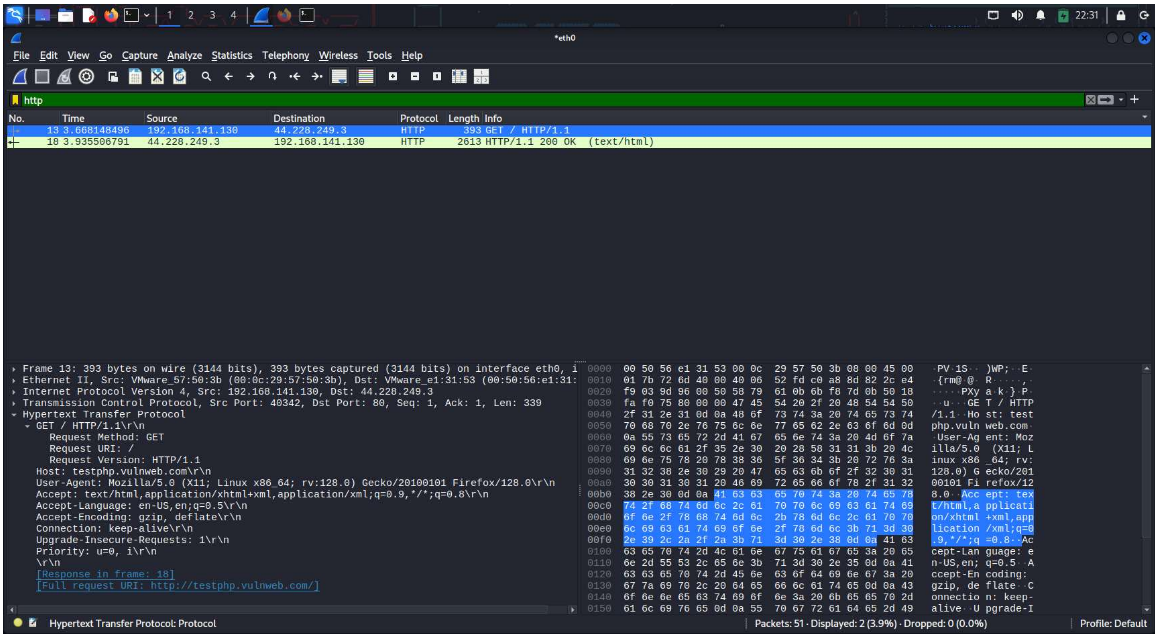
```
0000  00 50 56 e1 31 53 00 0c  29 57 50 3b 08 00 45 00   ·PV·1S··)WP;··E·
0010  00 3c 02 44 40 00 40 06  c4 65 c0 a8 8d 82 2c e4   ·<·D@·@··e····,·
0020  f9 03 d5 ca 00 50 99 c8  c6 fc 00 00 00 00 a0 02   ·····P··········
0030  fa f0 74 41 00 00 02 04  05 b4 04 02 08 0a ef 6f   ··tA···········o
0040  11 6a 00 00 00 00 01 03  03 07                     ·j········
```

wireshark_eth0B05MI3.pcapng | Packets: 515 · Displayed: 8 (1.6%) · Dropped: 0 (0.0%) | Profile: Default

6.2 HTTP Traffic Analysis

Filter Used: http

HTTP traffic is transmitted in plaintext.


22:31
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Profile: Default

```
No.  Time         Source           Destination      Protocol Length Info
  13 3.668148496  192.168.141.130  44.228.249.3     HTTP      393 GET / HTTP/1.1
  18 3.935506791  44.228.249.3     192.168.141.130  HTTP     2613 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 13: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface eth0, i
› Ethernet II, Src: VMware_57:50:3b (00:0c:29:57:50:3b), Dst: VMware_e1:31:53 (00:50:56:e1:31:
› Internet Protocol Version 4, Src: 192.168.141.130, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 40342, Dst Port: 80, Seq: 1, Ack: 1, Len: 339
⌄ Hypertext Transfer Protocol
  ⌄ GET / HTTP/1.1\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 18]
    [Full request URI: http://testphp.vulnweb.com/]
```

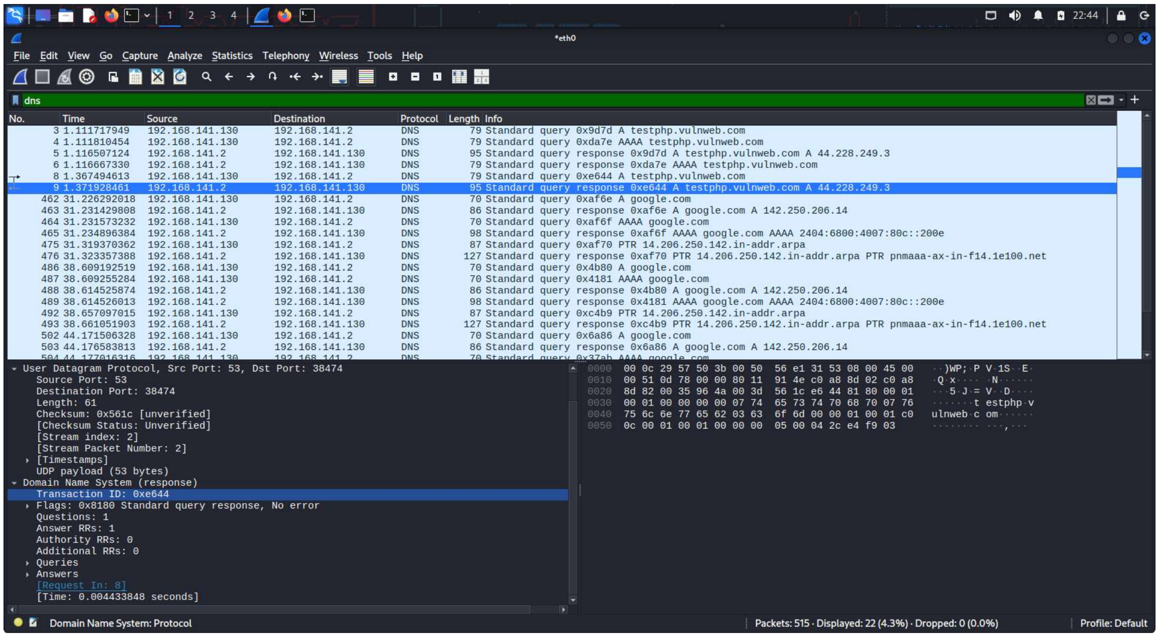
```
0000  00 50 56 e1 31 53 00 0c  29 57 50 3b 08 00 45 00   ·PV·1S·· )WP;··E·
0010  01 7b 72 6d 40 00 40 06  52 fd c0 a8 8d 82 2c e4   ·{rm@·@· R·····,·
0020  f9 03 9d 96 00 50 58 79  61 0b 6b f8 7d 0b 50 18   ·····PXy a·k·}·P·
0030  fa f0 75 80 00 00 47 45  54 20 2f 20 48 54 54 50   ··u···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74   /1.1··Ho st: test
0050  70 68 70 2e 76 75 6c 6e  77 65 62 2e 63 6f 6d 0d   php.vuln web.com·
0060  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0070  69 6c 6c 61 2f 35 2e 30  20 28 58 31 31 3b 20 4c   illa/5.0  (X11; L
0080  69 6e 75 78 20 78 38 36  5f 36 34 3b 20 72 76 3a   inux x86 _64; rv:
0090  31 32 38 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   128.0) G ecko/201
00a0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 32   00101 Fi refox/12
00b0  38 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   8.0··Acc ept: tex
00c0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
00d0  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
00e0  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
00f0  2e 39 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   .9,*/*;q =0.8··Ac
0100  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0110  6e 2d 55 53 2c 65 6e 3b  71 3d 30 2e 35 0d 0a 41   n-US,en; q=0.5··A
0120  63 63 65 70 74 2d 45 6e  63 6f 64 69 6e 67 3a 20   ccept-En coding: 
0130  67 7a 69 70 2c 20 64 65  66 6c 61 74 65 0d 0a 43   gzip, de flate··C
0140  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0150  61 6c 69 76 65 0d 0a 55  70 67 72 61 64 65 2d 49   alive··U pgrade-I
```

Packets: 51 · Displayed: 2 (3.9%) · Dropped: 0 (0.0%)

6.3 DNS Traffic Analysis

Filter Used: dns

DNS queries reveal domain requests.


22:44
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Domain Name System: Protocol
Profile: Default

```
No.  Time          Source           Destination      Protocol Length Info
   3 1.111717949   192.168.141.130  192.168.141.2    DNS       79 Standard query 0x9d7d A testphp.vulnweb.com
   4 1.111810454   192.168.141.130  192.168.141.2    DNS       79 Standard query 0xda7e AAAA testphp.vulnweb.com
   5 1.116507124   192.168.141.2    192.168.141.130  DNS       95 Standard query response 0x9d7d A testphp.vulnweb.com A 44.228.249.3
   6 1.116667330   192.168.141.2    192.168.141.130  DNS       79 Standard query response 0xda7e AAAA testphp.vulnweb.com
   8 1.367494613   192.168.141.130  192.168.141.2    DNS       79 Standard query 0xe644 A testphp.vulnweb.com
   9 1.371928461   192.168.141.2    192.168.141.130  DNS       95 Standard query response 0xe644 A testphp.vulnweb.com A 44.228.249.3
 462 31.226292018  192.168.141.130  192.168.141.2    DNS       70 Standard query 0xaf6e A google.com
 463 31.231429808  192.168.141.2    192.168.141.130  DNS       86 Standard query response 0xaf6e A google.com A 142.250.206.14
 464 31.231573232  192.168.141.130  192.168.141.2    DNS       70 Standard query 0xaf6f AAAA google.com
 465 31.234896384  192.168.141.2    192.168.141.130  DNS       98 Standard query response 0xaf6f AAAA google.com AAAA 2404:6800:4007:80c::200e
 475 31.319370362  192.168.141.130  192.168.141.2    DNS       87 Standard query 0xaf70 PTR 14.206.250.142.in-addr.arpa
 476 31.323357388  192.168.141.2    192.168.141.130  DNS      127 Standard query response 0xaf70 PTR 14.206.250.142.in-addr.arpa PTR pnmaaa-ax-in-f14.1e100.net
 486 38.609192519  192.168.141.130  192.168.141.2    DNS       70 Standard query 0x4b80 A google.com
 487 38.609255284  192.168.141.130  192.168.141.2    DNS       70 Standard query 0x4181 AAAA google.com
 488 38.614525874  192.168.141.2    192.168.141.130  DNS       86 Standard query response 0x4b80 A google.com A 142.250.206.14
 489 38.614526013  192.168.141.2    192.168.141.130  DNS       98 Standard query response 0x4181 AAAA google.com AAAA 2404:6800:4007:80c::200e
 492 38.657097015  192.168.141.130  192.168.141.2    DNS       87 Standard query 0xc4b9 PTR 14.206.250.142.in-addr.arpa
 493 38.661051903  192.168.141.2    192.168.141.130  DNS      127 Standard query response 0xc4b9 PTR 14.206.250.142.in-addr.arpa PTR pnmaaa-ax-in-f14.1e100.net
 502 44.171506328  192.168.141.130  192.168.141.2    DNS       70 Standard query 0x6a86 A google.com
 503 44.176583813  192.168.141.2    192.168.141.130  DNS       86 Standard query response 0x6a86 A google.com A 142.250.206.14
 504 44.177016316  192.168.141.130  192.168.141.2    DNS       70 Standard query 0x37ab AAAA google.com
```

```
⌄ User Datagram Protocol, Src Port: 53, Dst Port: 38474
    Source Port: 53
    Destination Port: 38474
    Length: 61
    Checksum: 0x561c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 2]
  › [Timestamps]
    UDP payload (53 bytes)
⌄ Domain Name System (response)
    Transaction ID: 0xe644
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  › Answers
    [Request In: 8]
    [Time: 0.004433848 seconds]
```

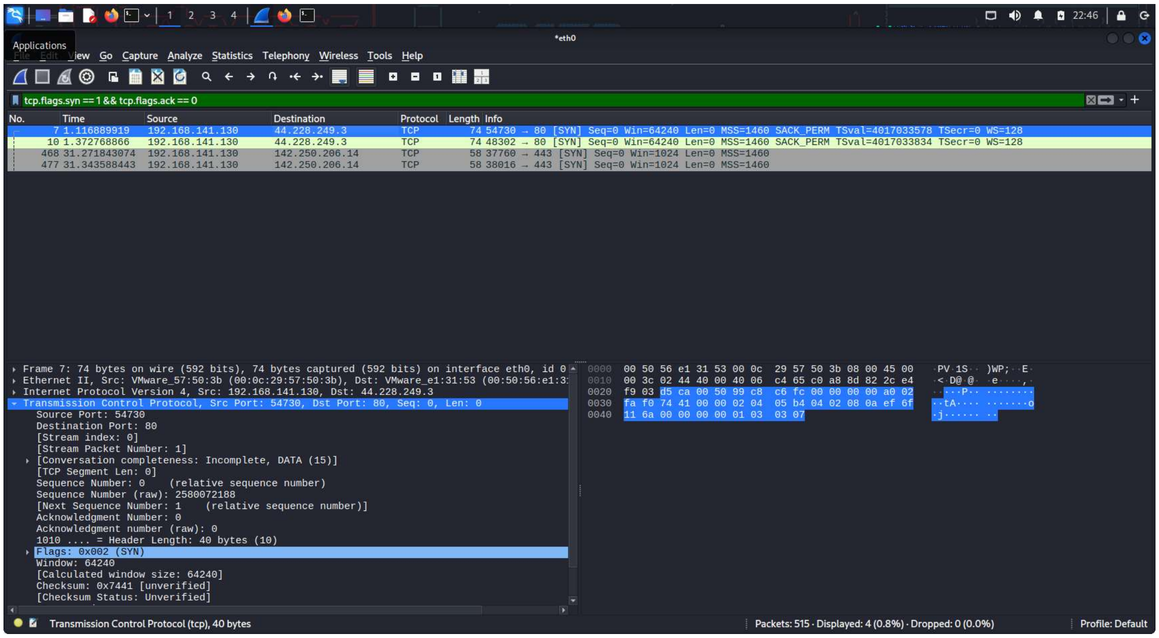
```
0000  00 0c 29 57 50 3b 00 50  56 e1 31 53 08 00 45 00   ··)WP;·P V·1S··E·
0010  00 51 0d 78 00 00 80 11  91 4e c0 a8 8d 02 c0 a8   ·Q·x···· ·N······
0020  8d 82 00 35 96 4a 00 3d  56 1c e6 44 81 80 00 01   ···5·J·= V··D····
0030  00 01 00 00 00 00 07 74  65 73 74 70 68 70 07 76   ·······t estphp·v
0040  75 6c 6e 77 65 62 03 63  6f 6d 00 00 01 00 01 c0   ulnweb·c om······
0050  0c 00 01 00 01 00 00 00  05 00 04 2c e4 f9 03      ········ ···,···
```

Packets: 515 · Displayed: 22 (4.3%) · Dropped: 0 (0.0%)

6.4 Port Scanning Detection

Filter Used: tcp.flags.syn == 1 && tcp.flags.ack == 0

Multiple SYN packets indicate scanning.


22:46
Applications
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1 && tcp.flags.ack == 0

No.  Time          Source           Destination      Protocol  Length Info
   7 1.116889919   192.168.141.130  44.228.249.3     TCP       74 54730 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4017033578 TSecr=0 WS=128
  10 1.372768866   192.168.141.130  44.228.249.3     TCP       74 48302 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4017033834 TSecr=0 WS=128
 468 31.271843074  192.168.141.130  142.250.206.14   TCP       58 37760 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 477 31.343588443  192.168.141.130  142.250.206.14   TCP       58 38016 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

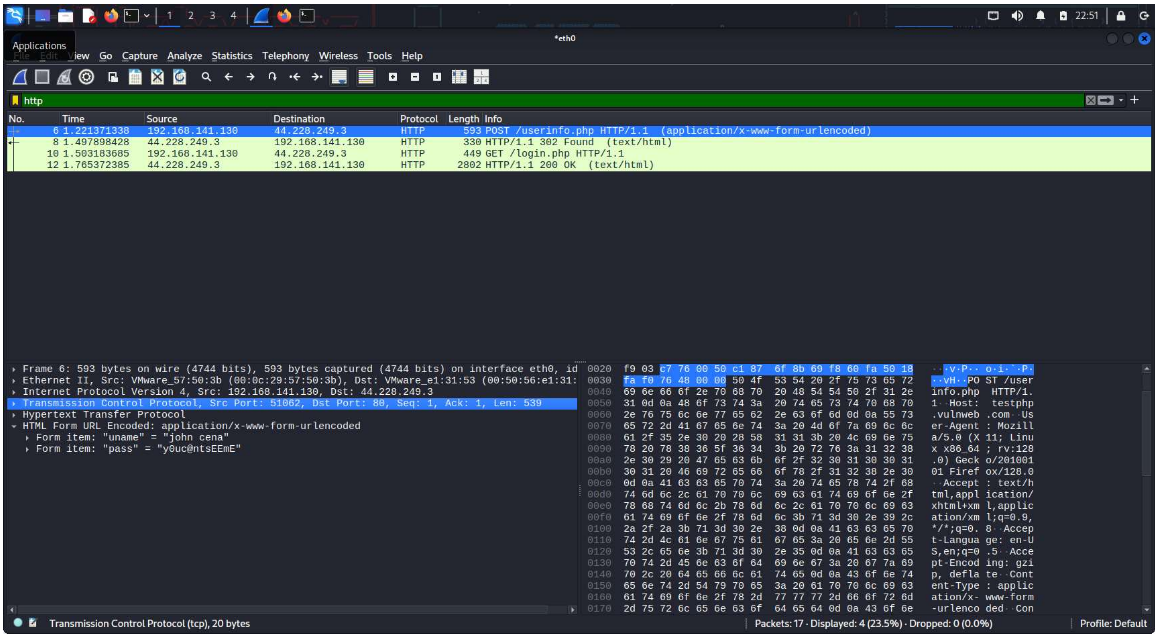
```
› Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_57:50:3b (00:0c:29:57:50:3b), Dst: VMware_e1:31:53 (00:50:56:e1:3
› Internet Protocol Version 4, Src: 192.168.141.130, Dst: 44.228.249.3
⌄ Transmission Control Protocol, Src Port: 54730, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 54730
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
  › [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2580072188
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  › Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x7441 [unverified]
    [Checksum Status: Unverified]
```

```
0000   00 50 56 e1 31 53 00 0c  29 57 50 3b 08 00 45 00   ·PV·1S·· )WP;··E·
0010   00 3c 02 44 40 00 40 06  c4 65 c0 a8 8d 82 2c e4   ·<·D@·@· ·e····,·
0020   f9 03 d5 ca 00 50 99 c8  c6 fc 00 00 00 00 a0 02   ·····P·· ········
0030   fa f0 74 41 00 00 02 04  05 b4 04 02 08 0a ef 6f   ··tA···· ·······o
0040   11 6a 00 00 00 00 01 03  03 07                     ·j······ ··
```

```
Transmission Control Protocol (tcp), 40 bytes    Packets: 515 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%)    Profile: Default
```

6.5 http Plain Text Credential Detection

http protocol transfers data as plain text.


22:51
Applications
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.  Time          Source           Destination      Protocol  Length Info
   6 1.221371338   192.168.141.130  44.228.249.3     HTTP      593 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
   8 1.497898428   44.228.249.3     192.168.141.130  HTTP      330 HTTP/1.1 302 Found  (text/html)
  10 1.503183685   192.168.141.130  44.228.249.3     HTTP      449 GET /login.php HTTP/1.1
  12 1.765372385   44.228.249.3     192.168.141.130  HTTP     2802 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 6: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits) on interface eth0, id
› Ethernet II, Src: VMware_57:50:3b (00:0c:29:57:50:3b), Dst: VMware_e1:31:53 (00:50:56:e1:31:
› Internet Protocol Version 4, Src: 192.168.141.130, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 51062, Dst Port: 80, Seq: 1, Ack: 1, Len: 539
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "john cena"
  › Form item: "pass" = "y0uc@ntsEEmE"
```

```
0020   f9 03 c7 76 00 50 c1 87  6f 8b 69 f8 60 fa 50 18   ···v·P·· o·i·`·P·
0030   fa f0 76 48 00 00 50 4f  53 54 20 2f 75 73 65 72   ··vH··PO ST /user
0040   69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050   31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060   2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070   65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080   61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090   78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64 ; rv:128
00a0   2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0   30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef ox/128.0
00c0   0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0   74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0   78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0   61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100   2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0110   74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0120   53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0130   70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140   70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
0150   65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0160   61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x- www-form
0170   2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco ded··Con
```

```
Transmission Control Protocol (tcp), 20 bytes    Packets: 17 · Displayed: 4 (23.5%) · Dropped: 0 (0.0%)    Profile: Default
```

7. Suspicious Activity Identified

- Port Scanning
- Plain HTTP traffic
- Excessive SYN packets

8. Security Recommendations

- Use HTTPS
- Deploy IDS/IPS
- Monitor network traffic
- Implement firewall rules

9. Conclusion

This project demonstrated how network traffic analysis helps detect anomalies and improves cybersecurity monitoring.