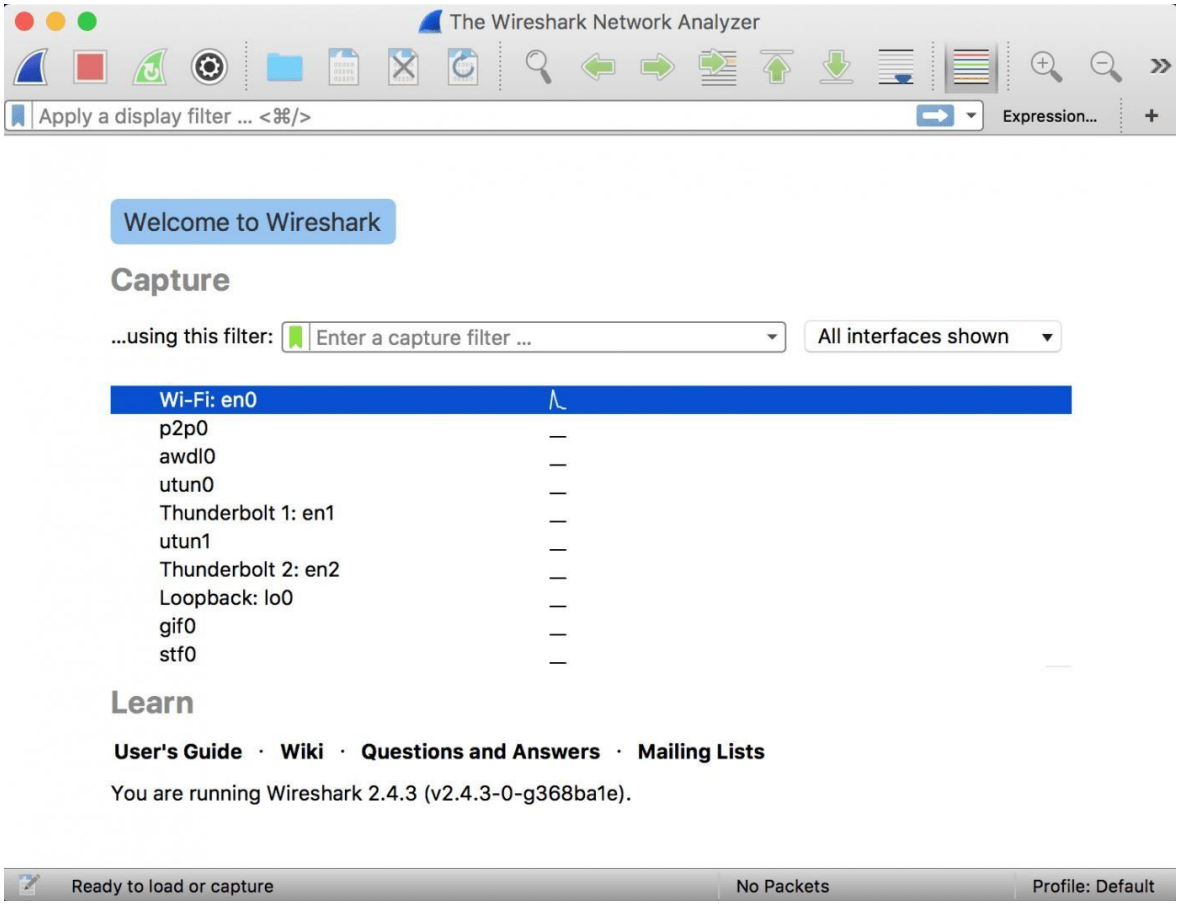
Practical No 5

Aim: Network Traffic Capture and DoS Attack with Wireshark and Nemesy

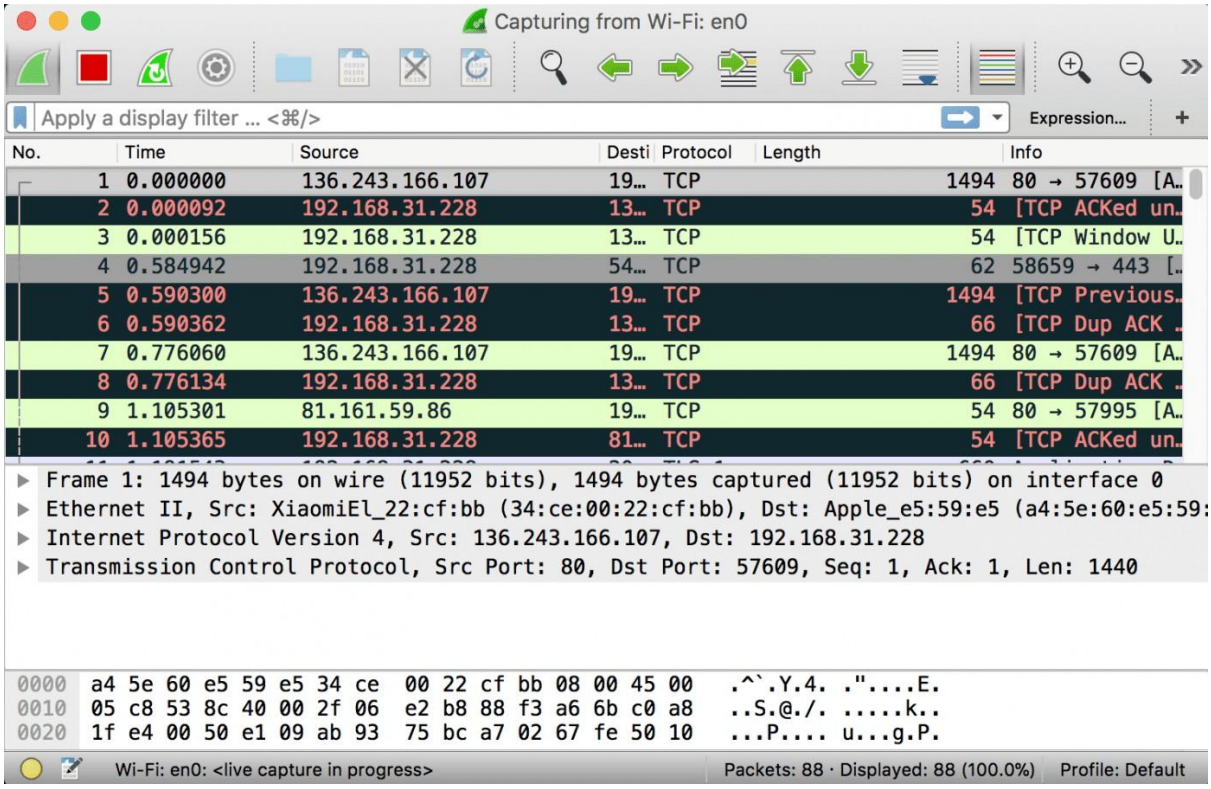
Network Traffic Capture:

- Use Wireshark to capture network traffic on a specific network interface.
- Analyze the captured packets to extract relevant information and identify potential security issues.
- Denial of Service (DoS) Attack:
- Use Nemesy to launch a DoS attack against a target system or network.
- Observe the impact of the attack on the target's availability and performance.



As soon as you single-click on your network interface‟s name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says “Enable promiscuous mode on all interfaces”.



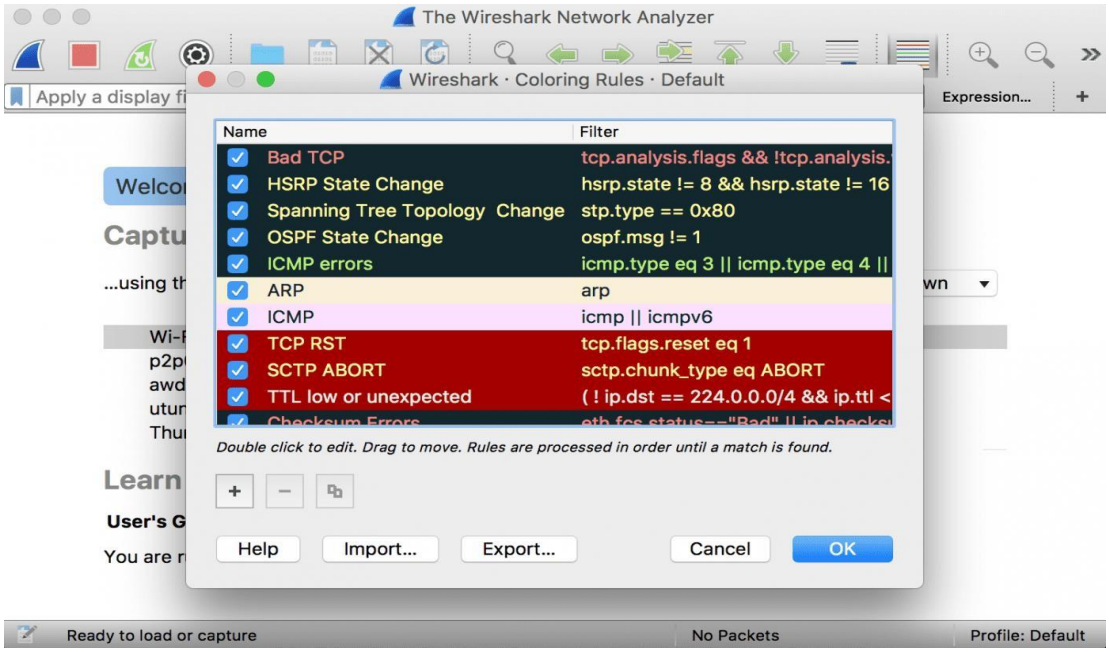
The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark‟s way of displaying traffic to help you easily identify the types of it. Default colors are:

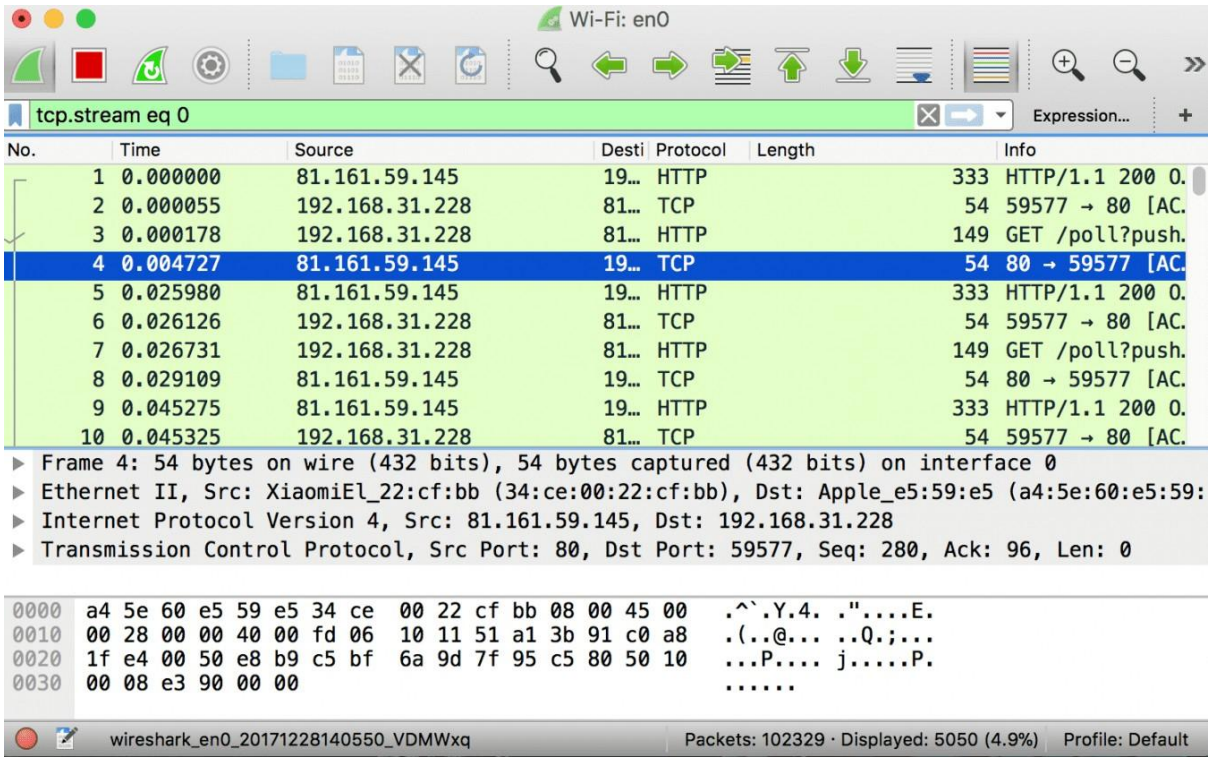
- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

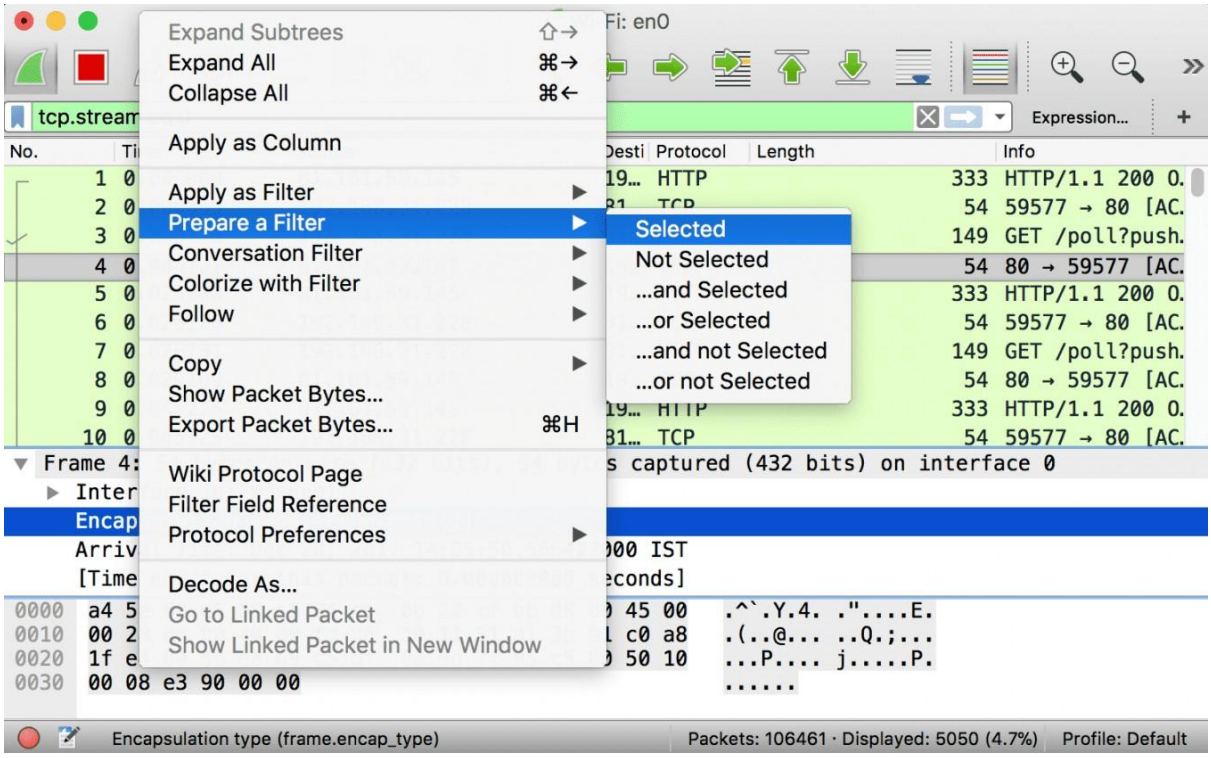


Analyze the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



(B) Using NEMESIS tool, launch DOS Attack.

Theory: A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Nemesis is a command-line network packet crafting and injection utility for UNIX-like and Windows systems. Nemesis, is well suited for testing Network Intrusion Detection Systems, firewalls, IP stacks and a variety of other tasks. As a command-line driven utility, Nemesis is perfect for automation and scripting.

Procedure:

Download NEMESIS tool from “nemesis.sourceforge.net” and unzip the contents in a drive.

Launch the NEMESIS.exe application from command prompt as shown below.

Select Command Prompt

```
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\admin>D:

D:\>nemesis
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

nemesis.exe - NEMESIS DDoS Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:
-------------------
-T, --usetor    Use TOR
-h, --host      Specify a host without http://
-p, --port      Specify webserver port
-t, --threads   Specify number of threads
-?, --help      Shows the help screen.
```

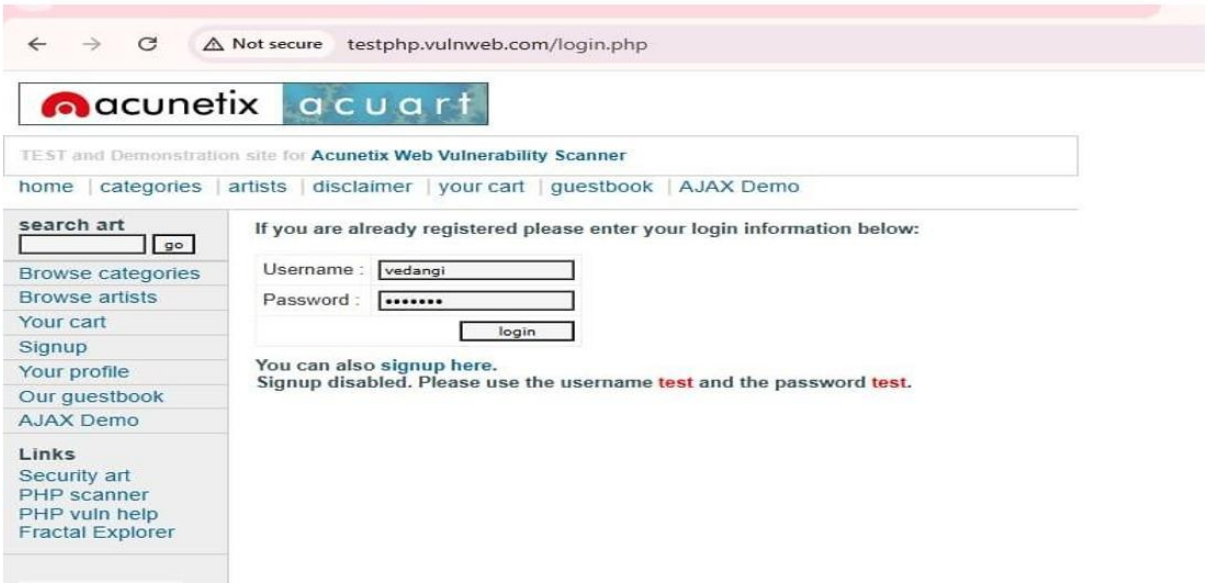
After launching NEMESIS, provide host and port of webserver on which attack is to be done.

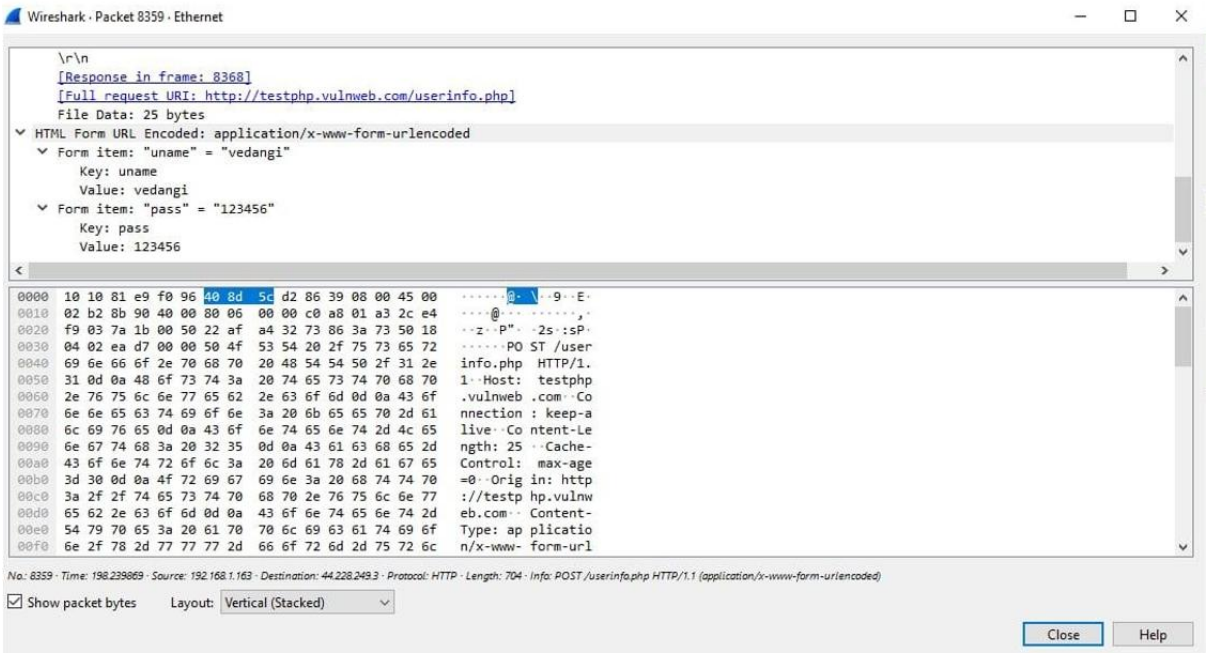
Select Command Prompt

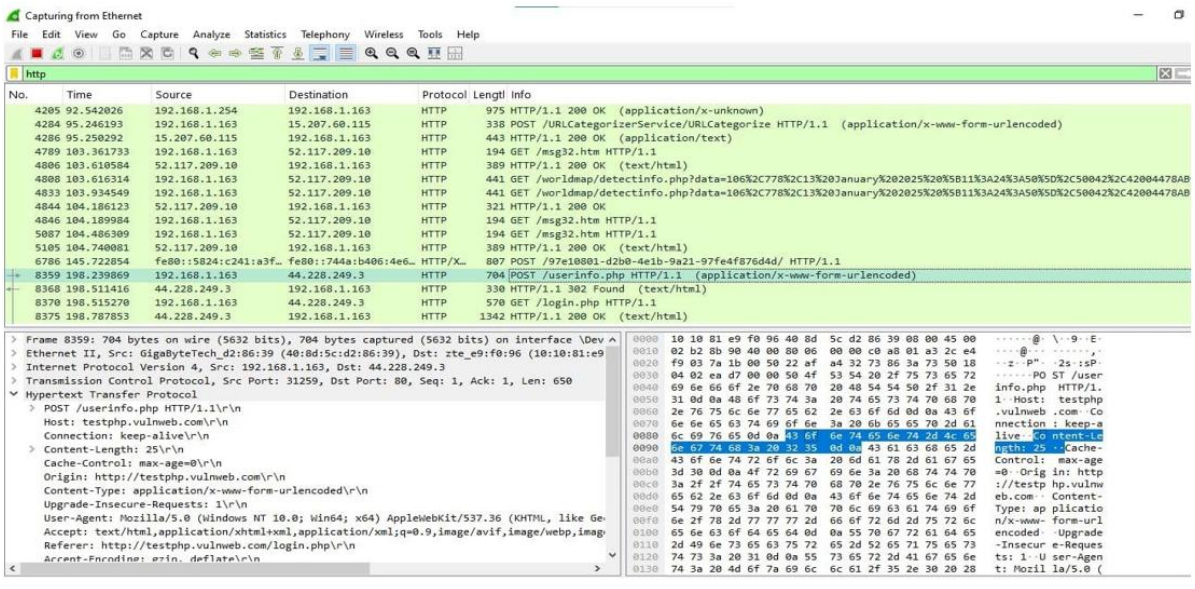
```
.

D:\>nemesis -h www.google.com -p 80 -t 10
.
.
.
.
.
.
.
.
.
.

D:\>
```


Not secure
testphp.vulnweb.com/login.php
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username : vedangi
Password : •••••••
login
You can also signup here.
Signup disabled. Please use the username test and the password test.


Wireshark · Packet 8359 · Ethernet
\r\n
[Response in frame: 8368]
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
File Data: 25 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "vedangi"
Key: uname
Value: vedangi
Form item: "pass" = "123456"
Key: pass
Value: 123456
0000 10 10 81 e9 f0 96 40 8d 5c d2 86 39 08 00 45 00
0010 02 b2 8b 90 40 00 80 06 00 00 c0 a8 01 a3 2c e4
0020 f9 03 7a 1b 00 50 22 af a4 32 73 86 3a 73 50 18
0030 04 02 ea d7 00 00 50 4f 53 54 20 2f 75 73 65 72
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65
0090 6e 67 74 68 3a 20 32 35 0d 0a 43 61 63 68 65 2d
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65
00b0 3d 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70
00c0 3a 2f 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77
00d0 65 62 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d
00e0 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f
00f0 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c
No.: 8359 · Time: 198.239869 · Source: 192.168.1.163 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 704 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Show packet bytes
Layout: Vertical (Stacked)
Close
Help


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengtl Info
4205 92.542026 192.168.1.254 192.168.1.163 HTTP 975 HTTP/1.1 200 OK (application/x-unknown)
4284 95.246193 192.168.1.163 15.207.60.115 HTTP 338 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
4286 95.250292 15.207.60.115 192.168.1.163 HTTP 443 HTTP/1.1 200 OK (application/text)
4789 103.361733 192.168.1.163 52.117.209.10 HTTP 194 GET /msg32.htm HTTP/1.1
4806 103.610584 52.117.209.10 192.168.1.163 HTTP 389 HTTP/1.1 200 OK (text/html)
4808 103.616314 192.168.1.163 52.117.209.10 HTTP 441 GET /worldmap/detectinfo.php?data=106%2C778%2C13%20January%202025%20%5B11%3A24%3A50%5D%2C50042%2C42004478AB
4833 103.934549 192.168.1.163 52.117.209.10 HTTP 441 GET /worldmap/detectinfo.php?data=106%2C778%2C13%20January%202025%20%5B11%3A24%3A50%5D%2C50042%2C42004478AB
4844 104.186123 52.117.209.10 192.168.1.163 HTTP 321 HTTP/1.1 200 OK
4846 104.189984 192.168.1.163 52.117.209.10 HTTP 194 GET /msg32.htm HTTP/1.1
5087 104.486309 192.168.1.163 52.117.209.10 HTTP 194 GET /msg32.htm HTTP/1.1
5105 104.740081 52.117.209.10 192.168.1.163 HTTP 389 HTTP/1.1 200 OK (text/html)
6786 145.722854 fe80::5824:c241:a3f… fe80::744a:b406:4e6… HTTP/X… 807 POST /97e10801-d2b0-4e1b-9a21-97fe4f876d4d/ HTTP/1.1
8359 198.239869 192.168.1.163 44.228.249.3 HTTP 704 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
8368 198.511416 44.228.249.3 192.168.1.163 HTTP 330 HTTP/1.1 302 Found (text/html)
8370 198.515270 192.168.1.163 44.228.249.3 HTTP 570 GET /login.php HTTP/1.1
8375 198.787853 44.228.249.3 192.168.1.163 HTTP 1342 HTTP/1.1 200 OK (text/html)
Frame 8359: 704 bytes on wire (5632 bits), 704 bytes captured (5632 bits) on interface \Dev
Ethernet II, Src: GigaByteTech_d2:86:39 (40:8d:5c:d2:86:39), Dst: zte_e9:f0:96 (10:10:81:e9
Internet Protocol Version 4, Src: 192.168.1.163, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 31259, Dst Port: 80, Seq: 1, Ack: 1, Len: 650
Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Content-Length: 25\r\n
Cache-Control: max-age=0\r\n
Origin: http://testphp.vulnweb.com\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n