SUBJECT: NTAL **Experiment 4**

Name :
Roll No:

Aim: 1. Working of **Wireshark** tool as Packet Sniffer tools : To capture data over the network.
2. Use **nmap / zenmap** for IP Spoofing and port sanning.

Theory:

1. **Wireshark**:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

Few filters which can be used with Wireshark:

- ip.addr == 10.0.0.1 [Sets a filter for any packet with 10.0.0.1, as either the source or dest]
- ip.addr==10.0.0.1 && ip.addr==10.0.0.2 [sets a conversation filter between the two defined IP addresses]
- http or dns [sets a filter to display all http and dns]
- tcp.port==4000 [sets a filter for any TCP packet with 4000 as a source or dest port]
- tcp.flags.reset==1 [displays all TCP resets]
- http.request [displays all HTTP GET requests]
- tcp contains traffic [displays all TCP packets that contain the word 'traffic'. Excellent when searching on a specific string or user ID]
- !(arp or icmp or dns) [masks out arp, icmp, dns, or whatever other protocols may be background noise. Allowing you to focus on the traffic of interest]
- udp contains 33:27:58 [sets a filter for the HEX values of 0x33 0x27 0x58 at any offset]
- tcp.analysis.retransmission [displays all retransmissions in the trace. Helps when tracking down slow application performance and packet loss]

2. **nmap**

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
Few of the commands to use nmap are listed down:

<u>Nmap Target Selection</u>

Scan a single IP // nmap 192.168.1.1
Scan a host // nmap www.testhostname.com
Scan a range of IPs // nmap 192.168.1.1-20
Scan a subnet // nmap 192.168.1.0/24
Scan targets from a text file // nmap -iL list-of-ips.txt
These are all default scans, which will scan 1000 TCP ports. Host discovery will take place.

Nmap Port Selection

Scan a single Port // nmap -p 22 192.168.1.1
Scan a range of ports // nmap -p 1-100 192.168.1.1
Scan 100 most common ports (Fast) // nmap -F 192.168.1.1
Scan all 65535 ports // nmap -p- 192.168.1.1

Nmap Port Scan types

Scan using TCP connect // nmap -sT 192.168.1.1
Scan using TCP SYN scan (default) // nmap -sS 192.168.1.1
Scan UDP ports // nmap -sU -p 123,161,162 192.168.1.1
Scan selected ports - ignore discovery // nmap -Pn -F 192.168.1.1

Privileged access is required to perform the default SYN scans.

Service and OS Detection

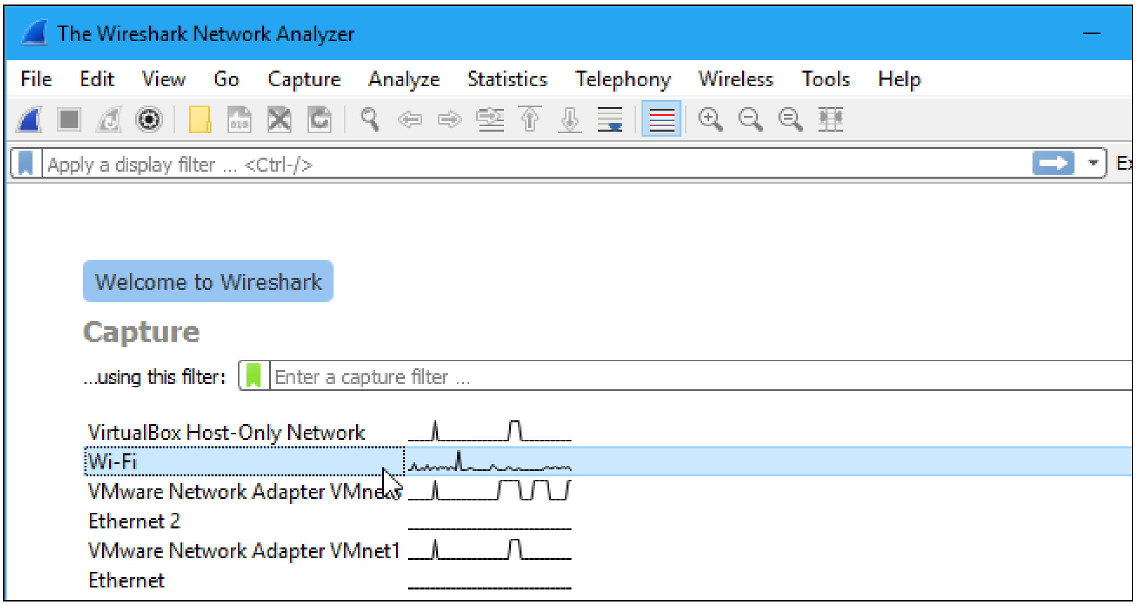
Detect OS and Services // nmap -A 192.168.1.1
Standard service detection // nmap -sV 192.168.1.1
More aggressive Service Detection // nmap -sV --version-intensity 5 192.168.1.1
Lighter banner grabbing detection // nmap -sV --version-intensity 0 192.168.1.1

Conclusion :

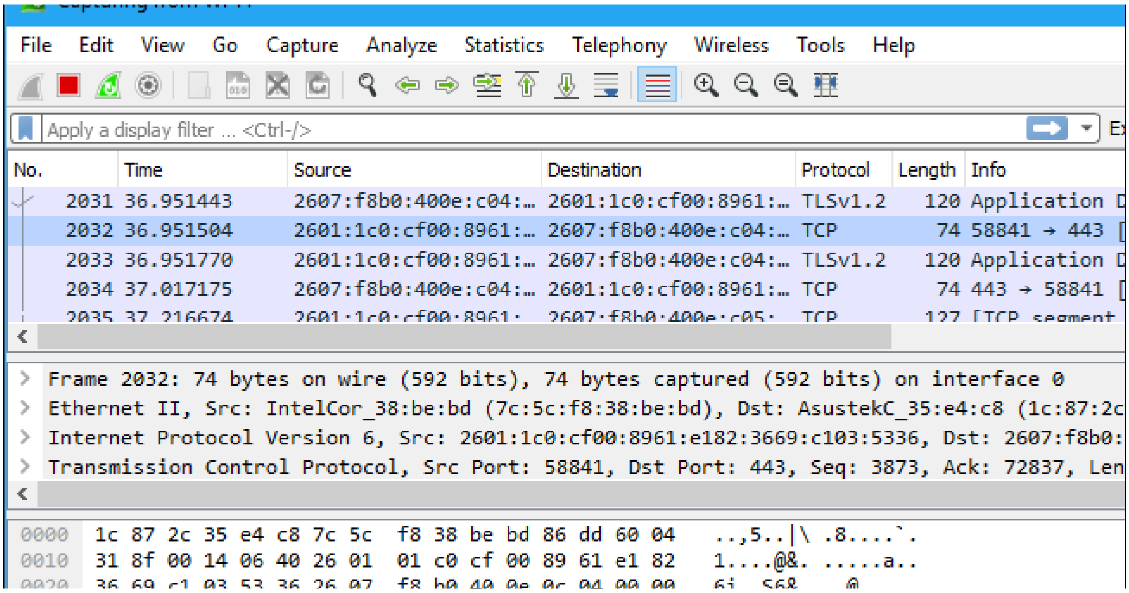
OUTPUT:

Wireshark

1. Capturing Packets : Capture > Option .. Select Interface

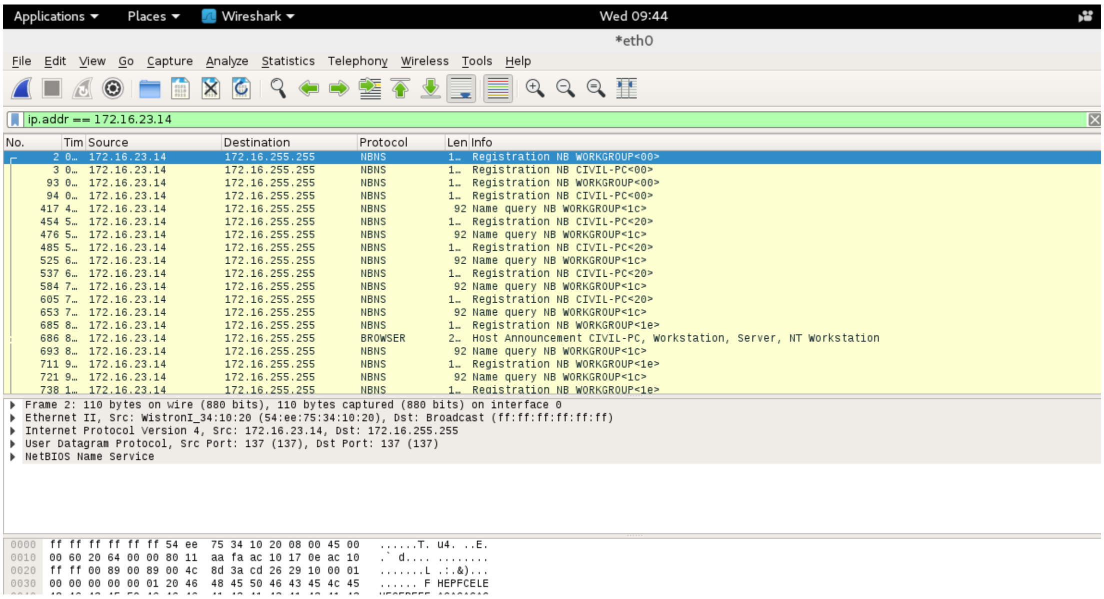

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
VirtualBox Host-Only Network
Wi-Fi
VMware Network Adapter VMnet8
Ethernet 2
VMware Network Adapter VMnet1
Ethernet

2. Capturing from wifi


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

```
No.   Time       Source                  Destination             Protocol  Length Info
 2031 36.951443  2607:f8b0:400e:c04:…   2601:1c0:cf00:8961:…   TLSv1.2     120 Application D
 2032 36.951504  2601:1c0:cf00:8961:…   2607:f8b0:400e:c04:…   TCP          74 58841 → 443 [
 2033 36.951770  2601:1c0:cf00:8961:…   2607:f8b0:400e:c04:…   TLSv1.2     120 Application D
 2034 37.017175  2607:f8b0:400e:c04:…   2601:1c0:cf00:8961:…   TCP          74 443 → 58841 [
 2035 37.216674  2601:1c0:cf00:8961:…   2607:f8b0:400e:c05:…   TCP         127 [TCP segment

> Frame 2032: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
> Internet Protocol Version 6, Src: 2601:1c0:cf00:8961:e182:3669:c103:5336, Dst: 2607:f8b0:
> Transmission Control Protocol, Src Port: 58841, Dst Port: 443, Seq: 3873, Ack: 72837, Len

0000  1c 87 2c 35 e4 c8 7c 5c  f8 38 be bd 86 dd 60 04   ..,5..|\ .8....`.
0010  31 8f 00 14 06 40 26 01  01 c0 cf 00 89 61 e1 82   1....@&. .....a..
0020  36 69 c1 03 53 36 26 07  f8 b0 40 0e 0c 04 00 00   6i..S6&. ..@.....
```

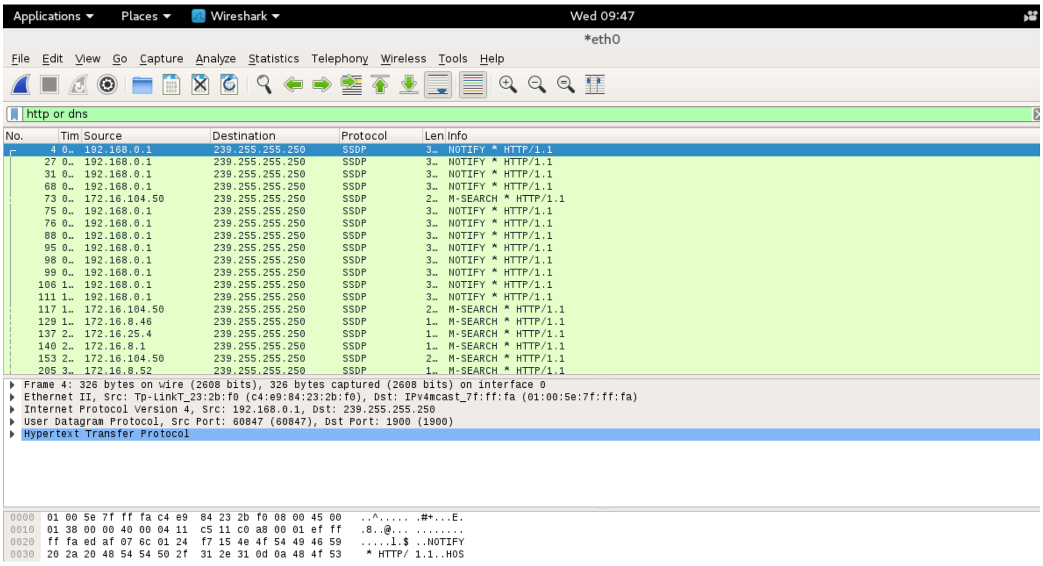
3. Applying filters : ip.addr == 172.16.23.14


Applications ▾ Places ▾ Wireshark ▾ Wed 09:44
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.23.14

```
No.    Tim Source          Destination       Protocol  Len Info
     2 0… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB WORKGROUP<00>
     3 0… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB CIVIL-PC<00>
    93 0… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB WORKGROUP<00>
    94 0… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB CIVIL-PC<00>
   417 4… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   454 5… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB CIVIL-PC<20>
   476 5… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   485 5… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB CIVIL-PC<20>
   525 6… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   537 6… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB CIVIL-PC<20>
   584 7… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   605 7… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB CIVIL-PC<20>
   653 7… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   685 8… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB WORKGROUP<1e>
   686 8… 172.16.23.14    172.16.255.255    BROWSER   2…  Host Announcement CIVIL-PC, Workstation, Server, NT Workstation
   693 8… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   711 9… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB WORKGROUP<1e>
   721 9… 172.16.23.14    172.16.255.255    NBNS       92 Name query NB WORKGROUP<1c>
   738 1… 172.16.23.14    172.16.255.255    NBNS      1…  Registration NB WORKGROUP<1e>

▸ Frame 2: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▸ Ethernet II, Src: WistronI_34:10:20 (54:ee:75:34:10:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 172.16.23.14, Dst: 172.16.255.255
▸ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
▸ NetBIOS Name Service

0000  ff ff ff ff ff ff 54 ee  75 34 10 20 08 00 45 00   ......T. u4. ..E.
0010  00 60 20 64 00 00 80 11  aa fa ac 10 17 0e ac 10   .` d.... ........
0020  ff ff 00 89 00 89 00 4c  8d 3a cd 26 29 10 00 01   .......L .:.&)...
0030  00 00 00 00 00 01 20 46  48 45 50 46 43 45 4c 45   ...... F HEPFCELE
```

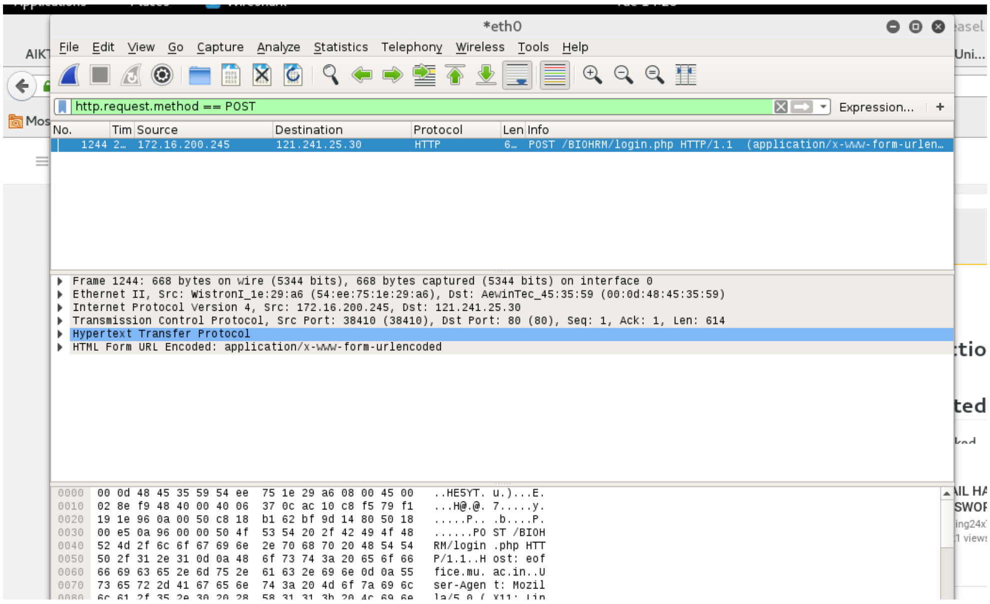
4. Scanning particular protocol


Applications ▾ Places ▾ Wireshark ▾ Wed 09:47
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http or dns

```
No.    Tim Source          Destination       Protocol  Len Info
     4 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    27 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    31 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    68 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    73 0… 172.16.104.50   239.255.255.250   SSDP      2…  M-SEARCH * HTTP/1.1
    75 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    76 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    88 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    95 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    98 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
    99 0… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
   106 1… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
   111 1… 192.168.0.1     239.255.255.250   SSDP      3…  NOTIFY * HTTP/1.1
   117 1… 172.16.104.50   239.255.255.250   SSDP      2…  M-SEARCH * HTTP/1.1
   129 1… 172.16.8.46     239.255.255.250   SSDP      1…  M-SEARCH * HTTP/1.1
   137 2… 172.16.25.4     239.255.255.250   SSDP      1…  M-SEARCH * HTTP/1.1
   140 2… 172.16.8.1      239.255.255.250   SSDP      1…  M-SEARCH * HTTP/1.1
   153 2… 172.16.104.50   239.255.255.250   SSDP      2…  M-SEARCH * HTTP/1.1
   205 3… 172.16.8.52     239.255.255.250   SSDP      1…  M-SEARCH * HTTP/1.1

▸ Frame 4: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface 0
▸ Ethernet II, Src: Tp-LinkT_23:2b:f0 (c4:e9:84:23:2b:f0), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
▸ User Datagram Protocol, Src Port: 60847 (60847), Dst Port: 1900 (1900)
▸ Hypertext Transfer Protocol

0000  01 00 5e 7f ff fa c4 e9  84 23 2b f0 08 00 45 00   ..^..... .#+...E.
0010  01 38 00 00 40 00 04 11  c5 11 c0 a8 00 01 ef ff   .8..@... ........
0020  ff fa ed af 07 6c 01 24  f7 15 4e 4f 54 49 46 59   .....l.$ ..NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 4f 53    * HTTP/ 1.1..HOS
```

5. Filtering POST method


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

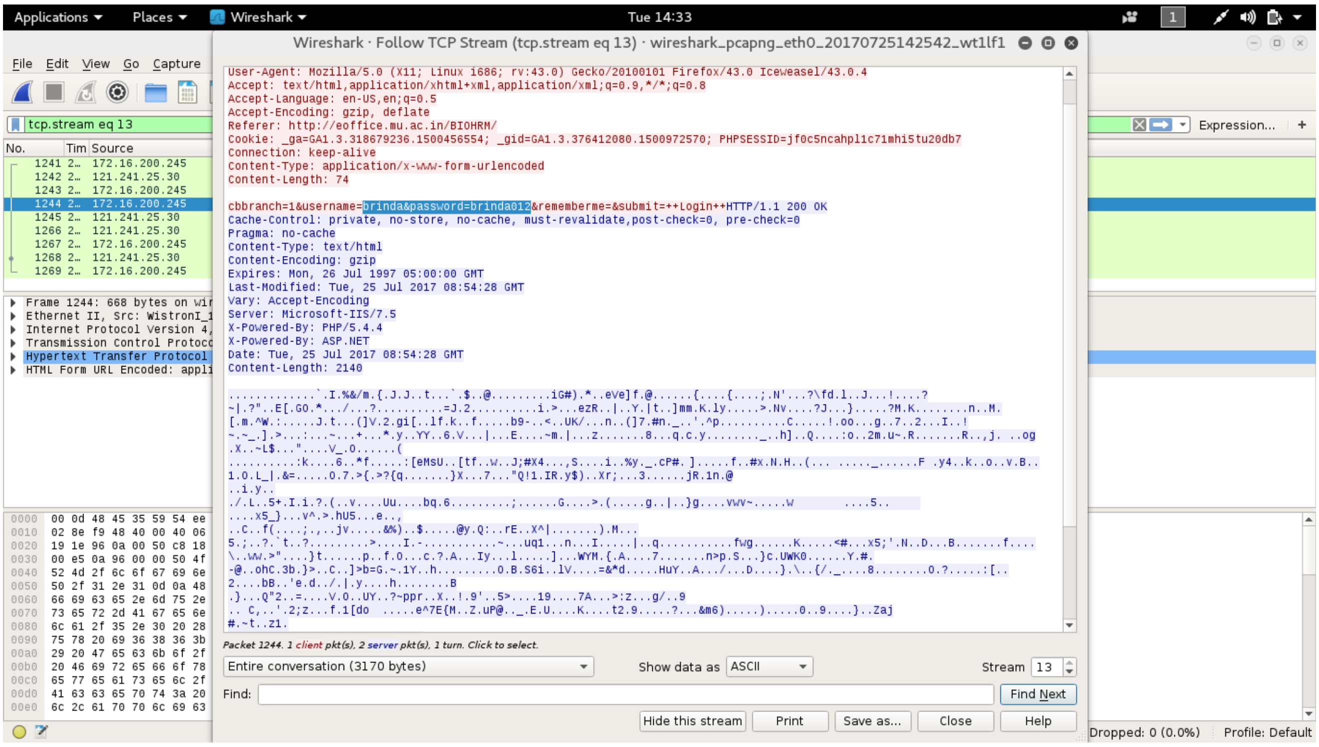
```
http.request.method == POST
```

```
No.    Tim Source          Destination     Protocol  Len Info
  1244 2…  172.16.200.245  121.241.25.30   HTTP      6…  POST /BIOHRM/login.php HTTP/1.1  (application/x-www-form-urlen…
```

```
▶ Frame 1244: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface 0
▶ Ethernet II, Src: WistronI_1e:29:a6 (54:ee:75:1e:29:a6), Dst: AewinTec_45:35:59 (00:0d:48:45:35:59)
▶ Internet Protocol Version 4, Src: 172.16.200.245, Dst: 121.241.25.30
▶ Transmission Control Protocol, Src Port: 38410 (38410), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 614
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  00 0d 48 45 35 59 54 ee  75 1e 29 a6 08 00 45 00   ..HE5YT. u.)...E.
0010  02 8e f9 48 40 00 40 06  37 0c ac 10 c8 f5 79 f1   ...H@.@. 7.....y.
0020  19 1e 96 0a 00 50 c8 18  b1 62 bf 9d 14 80 50 18   .....P.. .b....P.
0030  00 e5 0a 96 00 00 50 4f  53 54 20 2f 42 49 4f 48   ......PO ST /BIOH
0040  52 4d 2f 6c 6f 67 69 6e  2e 70 68 70 20 48 54 54   RM/login .php HTT
0050  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 65 6f 66   P/1.1..H ost: eof
0060  66 69 63 65 2e 6d 75 2e  61 63 2e 69 6e 0d 0a 55   fice.mu. ac.in..U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
0080  6c 61 2f 35 2e 30 20 28  58 31 31 3b 20 4c 69 6e   la/5.0 ( X11; Lin
```

6. Capturing TCP Stream



```
tcp.stream eq 13
```

```
No.    Tim Source
  1241 2…  172.16.200.245
  1242 2…  121.241.25.30
  1243 2…  172.16.200.245
  1244 2…  172.16.200.245
  1245 2…  121.241.25.30
  1266 2…  121.241.25.30
  1267 2…  172.16.200.245
  1268 2…  121.241.25.30
  1269 2…  172.16.200.245
```

```
▶ Frame 1244: 668 bytes on wir
▶ Ethernet II, Src: WistronI_1
▶ Internet Protocol Version 4,
▶ Transmission Control Protoco
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: appli
```

```
0000  00 0d 48 45 35 59 54 ee
0010  02 8e f9 48 40 00 40 06
0020  19 1e 96 0a 00 50 c8 18
0030  00 e5 0a 96 00 00 50 4f
0040  52 4d 2f 6c 6f 67 69 6e
0050  50 2f 31 2e 31 0d 0a 48
0060  66 69 63 65 2e 6d 75 2e
0070  73 65 72 2d 41 67 65 6e
0080  6c 61 2f 35 2e 30 20 28
0090  75 78 20 69 36 38 36 3b
00a0  29 20 47 65 63 6b 6f 2f
00b0  20 46 69 72 65 66 6f 78
00c0  65 77 65 61 73 65 6c 2f
00d0  41 63 63 65 70 74 3a 20
00e0  6c 2c 61 70 70 6c 69 63
```

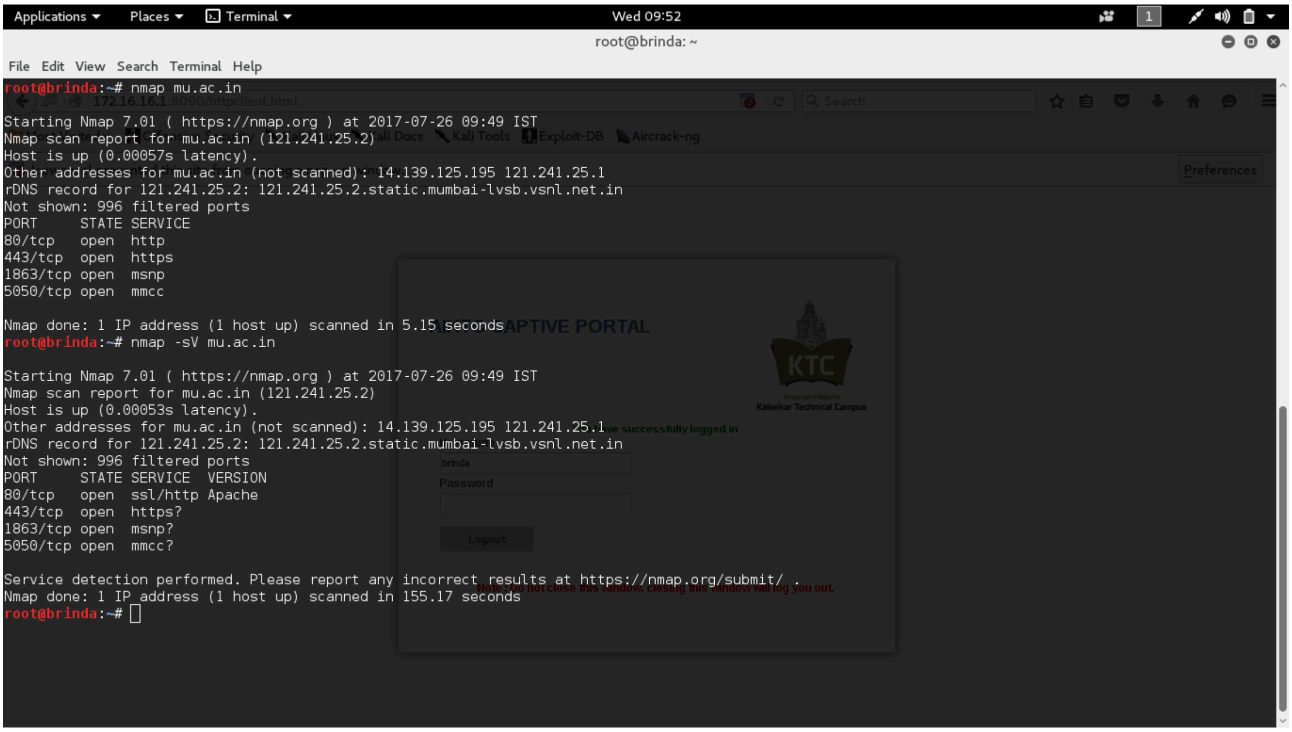
```
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://eoffice.mu.ac.in/BIOHRM/
Cookie: _ga=GA1.3.318679236.1500456554; _gid=GA1.3.376412080.1500972570; PHPSESSID=jf0c5ncahpl1c71mhi5tu20db7
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 74

cbbranch=1&username=brinda&password=brinda012&rememberme=&submit=++Login++HTTP/1.1 200 OK
Cache-Control: private, no-store, no-cache, must-revalidate,post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html
Content-Encoding: gzip
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Tue, 25 Jul 2017 08:54:28 GMT
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-Powered-By: PHP/5.4.4
X-Powered-By: ASP.NET
Date: Tue, 25 Jul 2017 08:54:28 GMT
Content-Length: 2140

............`.I.%&/m.{.J.J..t...`.$..@.........iG#).*..eVe]f.@......{....{....;.N'...?\fd.l..J...!....?
~|.?"..E[.GO.*.../...?.........=J.2.........i.>...ezR..|..Y.|t..]mm.K.ly.....>.Nv....?J...}.....?M.K........n..M.
[.m.^W.:.....J.t...(]V.2.gi[..lf.k..f.....b9-..<..UK/...n..(]7.#n._..'.^p..........C.....!.oo...g..7..2...I..!
~.~_.].>...:...~...+...*.y..YY..6.V...|...E....~m.|...z.......8...q.c.y........_..h]..Q....:o..2m.u~.R.......R..,j. ..og
.X..~L$..."....V_.O......(
..........:k....6..*f.....:[eMsU..[tf..w..J;#X4...,S....i..%y._.cP#. ].....f..#x.N.H..(... ....._......F .y4..k..o..v.B..
1.O.L_|.&=.....0.7.>{.>?{q.......}X...7..."Q!1.IR.y$)..Xr;...3......jR.1n.@
..i.y..
./.L..5+.I.i.?.(..v....Uu....bq.6.........;......G....>.(.....g..|..}g....vwv~.....w       ....5..
....x5_}...v^.>.hU5...e..,
..C..f(....;.,..jv.....&%)..$.....@y.Q:..rE..X^|.......).M...
5.;..?.`t..?.........>....I.-...........~...uq1...n...I.....|..q...........fwg......K.....<#...x5;'.N..D...B.......f....
\..ww.>"....}t......p..f.O...c.?.A...Iy...l.....]...WYM.{.A....7.......n>p.S...}c.UWK0......Y.#.
-@..ohC.3b.}>..C..]>b=G.~.1Y..h.........O.B.S6i..lV....=&*d.....HuY..A.../...D....}.\..{/._....8........O.?.....:[..
2....bB..'e.d../.|.y....h........B
.}...Q"2..=....V.O..UY..?~ppr..X..!.9'..5>....19....7A...>:z...g/..9
.. C,..'.2;z...f.1[do  .....e^7E{M..Z.uP@.._.E.U....K....t2.9.....?...&m6).....).....0..9....}..Zaj
#.~t..z1.
```

Packet 1244. 1 client pkt(s), 2 server pkt(s), 1 turn. Click to select.

Entire conversation (3170 bytes)

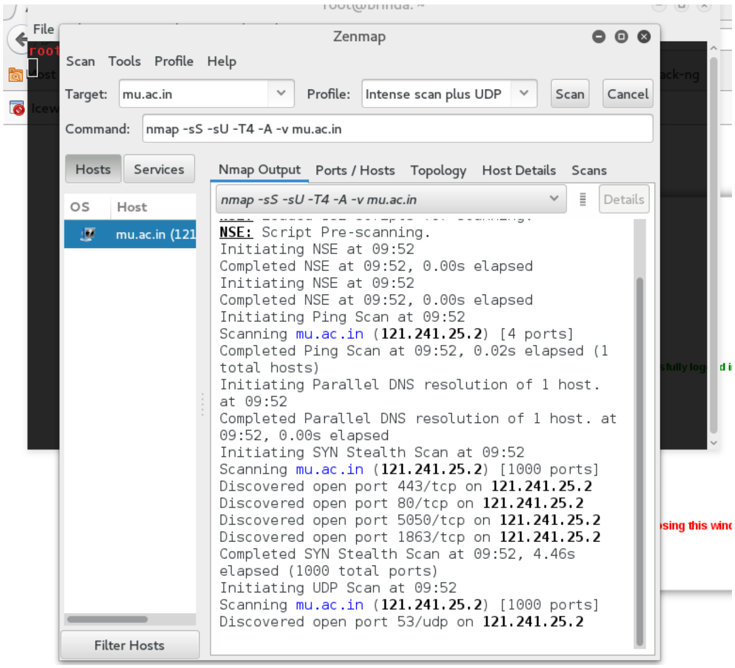
nmap and zenmap

1. Scanning for open ports using nmap



```
root@brinda:~# nmap mu.ac.in

Starting Nmap 7.01 ( https://nmap.org ) at 2017-07-26 09:49 IST
Nmap scan report for mu.ac.in (121.241.25.2)
Host is up (0.00057s latency).
Other addresses for mu.ac.in (not scanned): 14.139.125.195 121.241.25.1
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
1863/tcp open  msnp
5050/tcp open  mmcc

Nmap done: 1 IP address (1 host up) scanned in 5.15 seconds
root@brinda:~# nmap -sV mu.ac.in

Starting Nmap 7.01 ( https://nmap.org ) at 2017-07-26 09:49 IST
Nmap scan report for mu.ac.in (121.241.25.2)
Host is up (0.00053s latency).
Other addresses for mu.ac.in (not scanned): 14.139.125.195 121.241.25.1
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  ssl/http Apache
443/tcp  open  https?
1863/tcp open  msnp?
5050/tcp open  mmcc?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 155.17 seconds
root@brinda:~#
```

2. Intense scan for udp stream using zenmap



Target: mu.ac.in

Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v mu.ac.in

```
nmap -sS -sU -T4 -A -v mu.ac.in
NSE: Script Pre-scanning.
Initiating NSE at 09:52
Completed NSE at 09:52, 0.00s elapsed
Initiating NSE at 09:52
Completed NSE at 09:52, 0.00s elapsed
Initiating Ping Scan at 09:52
Scanning mu.ac.in (121.241.25.2) [4 ports]
Completed Ping Scan at 09:52, 0.02s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host.
at 09:52
Completed Parallel DNS resolution of 1 host. at
09:52, 0.00s elapsed
Initiating SYN Stealth Scan at 09:52
Scanning mu.ac.in (121.241.25.2) [1000 ports]
Discovered open port 443/tcp on 121.241.25.2
Discovered open port 80/tcp on 121.241.25.2
Discovered open port 5050/tcp on 121.241.25.2
Discovered open port 1863/tcp on 121.241.25.2
Completed SYN Stealth Scan at 09:52, 4.46s
elapsed (1000 total ports)
Initiating UDP Scan at 09:52
Scanning mu.ac.in (121.241.25.2) [1000 ports]
Discovered open port 53/udp on 121.241.25.2
```