A Project ETE Report on

A PACKET SNIFFING DETECTOR FOR WIRELESS NETWORK

Submitted in partial fulfillment of the
requirement for the award of the degree of

Bachelor of Technology in

Computer Science & Engineering

Under The Supervision of
Mr. Mukesh Kumar Jha
Assistant Proff.

.

Submitted By

Aman Attri

19SCSE1010231

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA
INDIA
OCTOBER, 2021

Table Of Content

Abstract

Packet sniffing, a network attack strategy, captures network traffic at the Ethernet frame level. After capture, this data can be analyzed and sensitive information can be retrieved. Many types of traffic on your network are passed as unencrypted data even passwords and other sensitive data. Obviously, this situation represents a danger to our corporate data. So this is a big problem for many users.

We can avoid packet sniffing by creating a software with the help of some tools or ideas like VPN -it will encrypt your traffic and hide your IP and most important tool- Wireshark tool .Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, and so forth.

First of all a VPN tool facility will be provide Then , Wireshark packet sniffing tool .In this tool we use capture filter field display filter Wireshark Colorization Options , Wireshark Promiscuous Mode.

By the help of above given tools we can find attackers activities and prevent our data and information .Statistics menu provides capture file properties.

Wireshark is a powerful tool and technically can be used for eavesdropping. It can help many private organizations, government organizations , small or big companies in the future .

Chapter 1
Introduction

When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called data packets and reassembled at receiver's node in original format. It is the smallest unit of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packet across the computer network is called packet sniffing. It is similar to as wire tapping to a telephone network. It is mostly used by crackers and hackers to collect information illegally about network. It is also used by ISPs, advertisers and governments.
ISPs use packet sniffing to track all your activities such as:

- who is receiver of your email
- what is content of that email
- what you download
- sites you visit
- what you looked on that website
- downloads from a site
- streaming events like video, audio, etc

To prevent packet sniffing from attackers we can use wireshark tool. Formerly known as Ethereal, Wireshark is an open-source program with many free features that provides the following functionality:

- Helps you to decode over 750 protocols.
- Is compatible with many other sniffers.
- Has plenty of online resources available.
- Supports the command-line and GUI interfaces.
- Offers the TShark command-line interface that has the following three components:

- Edit cap: Reads the captured packets from the infile and reads and writes the same capture files that are supported by Wireshark.
- Merge cap: Combines multiple saved capture files into a single output file.
- Text2pcap: Reads in an ASCII hex dump and writes the data described into a `pcap` or `pcapng` capture file. Text2pcap can read hex dumps with multiple packets in them and build a capture file of multiple packets.

Protocols vulnerable to sniffing

The following protocols are vulnerable to sniffing:

- HTTP
- Telnet
- rlogin
- POP
- IMAP
- SMTP and NNTP
- FTP

Users of network analyzers

The following roles use network analyzers:

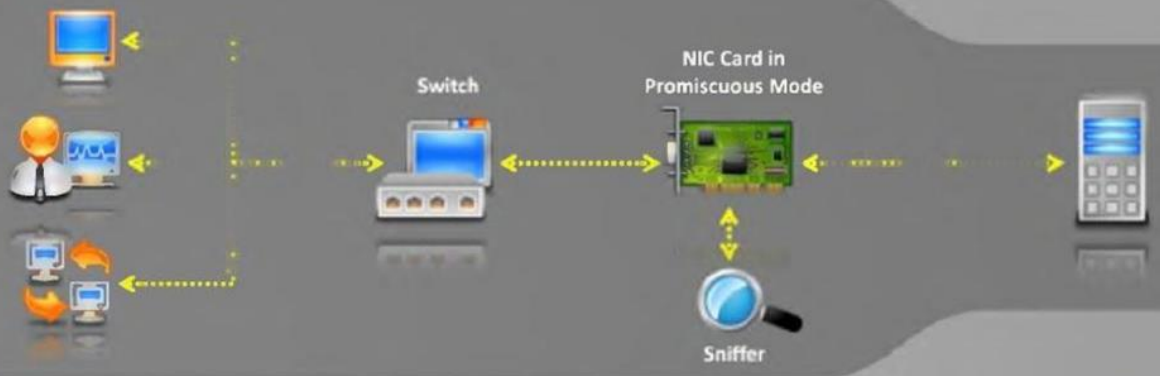
- System administrators
- Understand system problems and performance
- Malicious individuals (intruders)
- Capture cleartext data
- Passively collect data on the following vulnerable protocols: FTP, POP3, IMAP, SMATP, rlogin, HTTP, and so on.
- Capture VoIP data
- Map the target network
- Discover traffic patterns
- Actively break into the network (backdoor techniques)

Filters

You can use filters to analyze captured data.

Promiscuous Mode

Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment



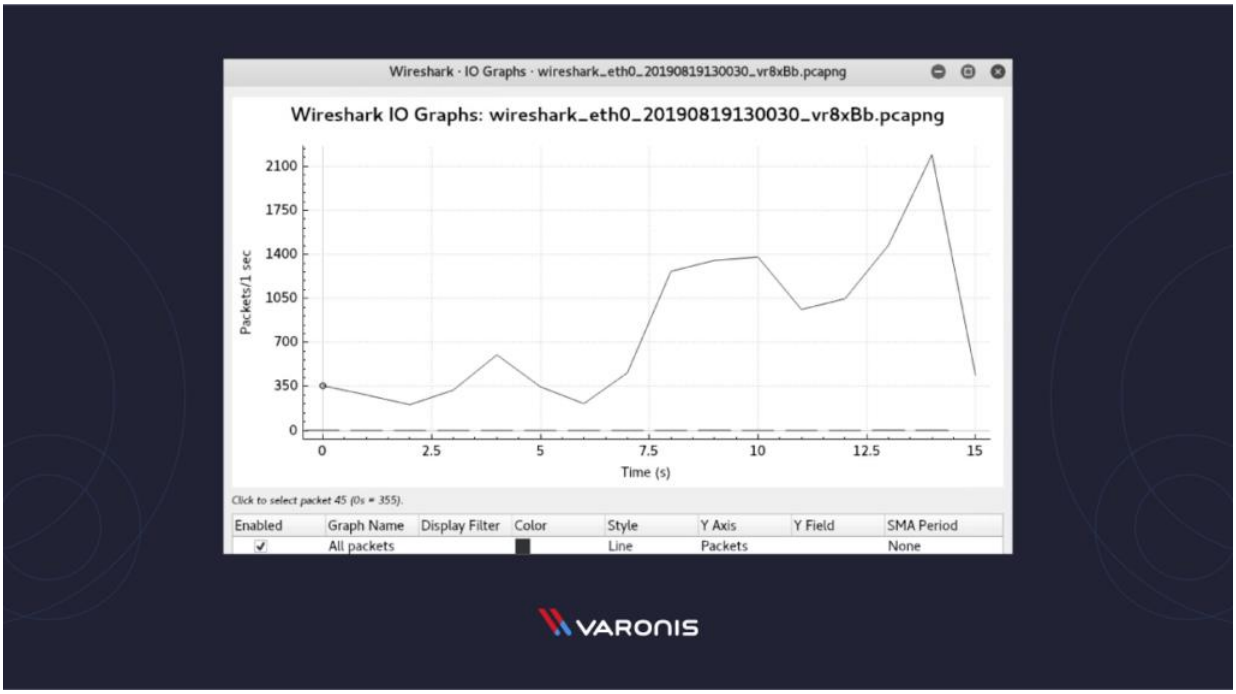
A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet

Decode Information

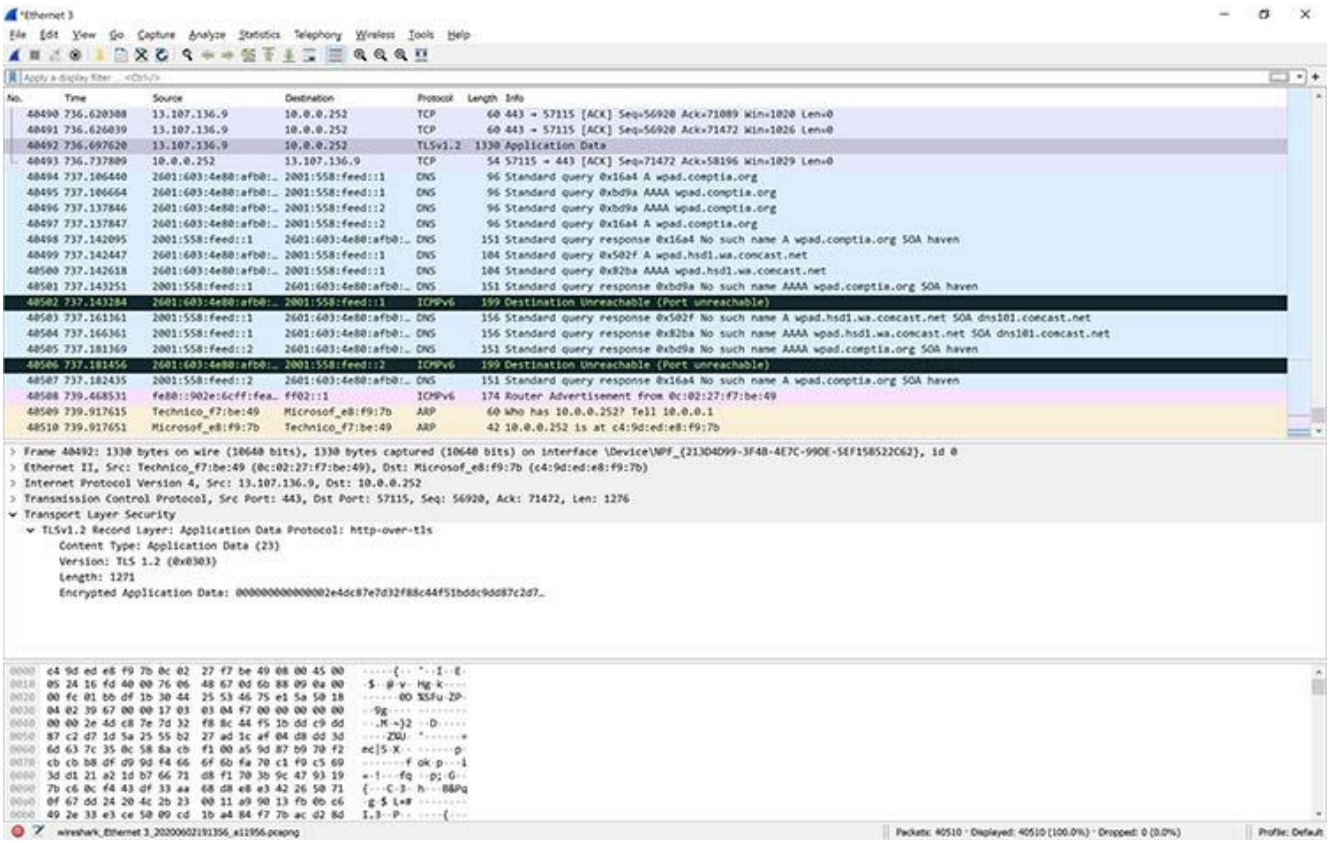
Chapter 2
Literature Survey

Wireshark a is very popular network analyzer tool, which is used by network administrators to capture packets traversing through a network. Administrators mostly use it to identify network problems, but hackers also use it to decode secure information.

Wireshark I/O Graph:



These days, many attacks happen through packet sniffing. Packet sniffers are placed in cyber cafes and on open wifi in restaurants, hotels, and public places. You can protect your data with a little caution. You should never use open wifi and should stop using open text protocols like ftp, http, IMAP, Telnet, and SNMP V1 and V2. You must install SSL certificates in your websites, use Secure File Transfer Protocol (sftp) instead of ftp, and use SSH instead of telnet. You should use SNMP V3 and opt for the strongest encryption.



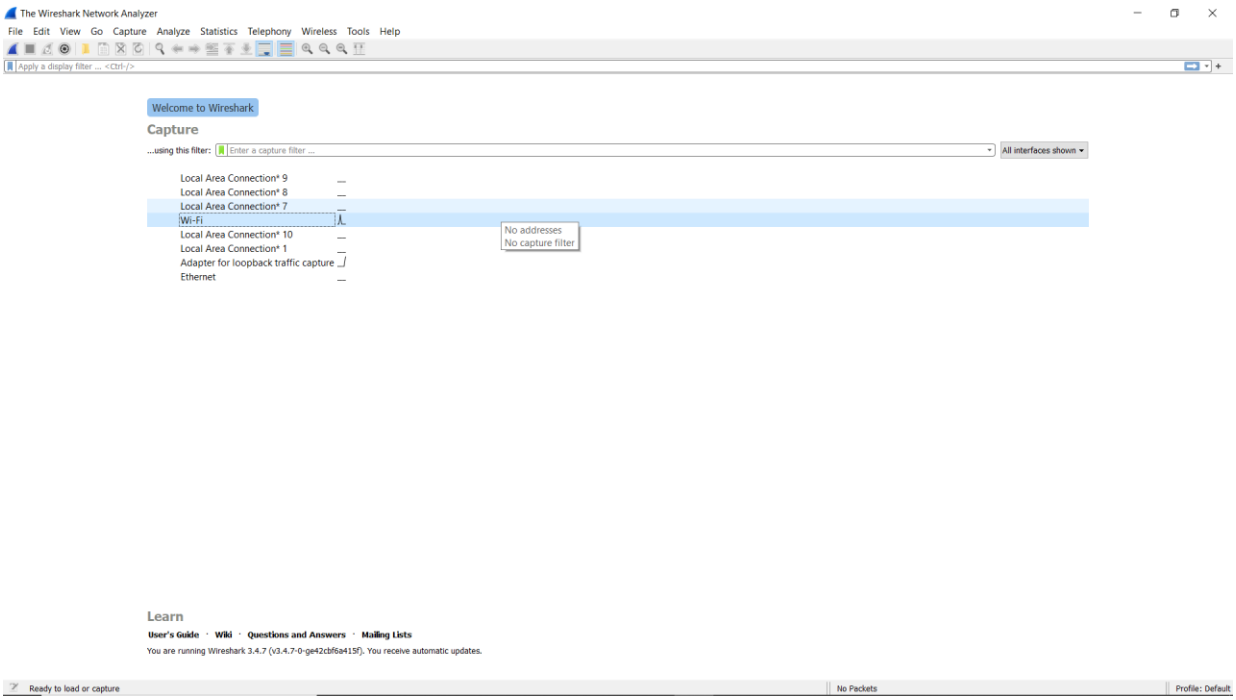
As the figure shows, the router thought a common destination was unreachable. This was discovered by drilling down into the IPv6 Internet Message Control Protocol (ICMP) traffic, which is marked in black. In Wireshark, any packet marked in black is considered to reflect some sort of issue.

In this above case, Wireshark helped determine that the router wasn't working properly and couldn't find YouTube very easily. The problem was resolved by restarting the cable modem. Of course, while this particular problem didn't necessitate using Wireshark, it's kind of cool to authoritatively finalize the issue.

Chapter 3

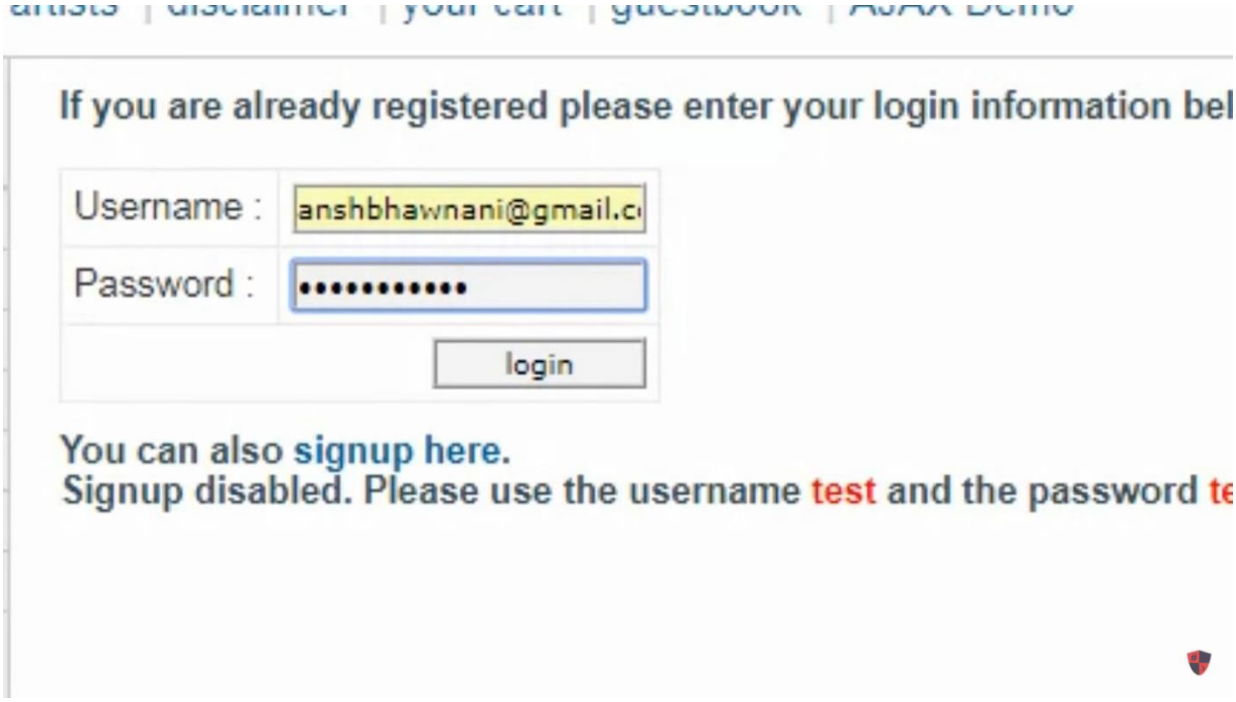
Working

First of all we have to install Wireshark tool then after open it .You will see this kind of interface as shown in screenshot.

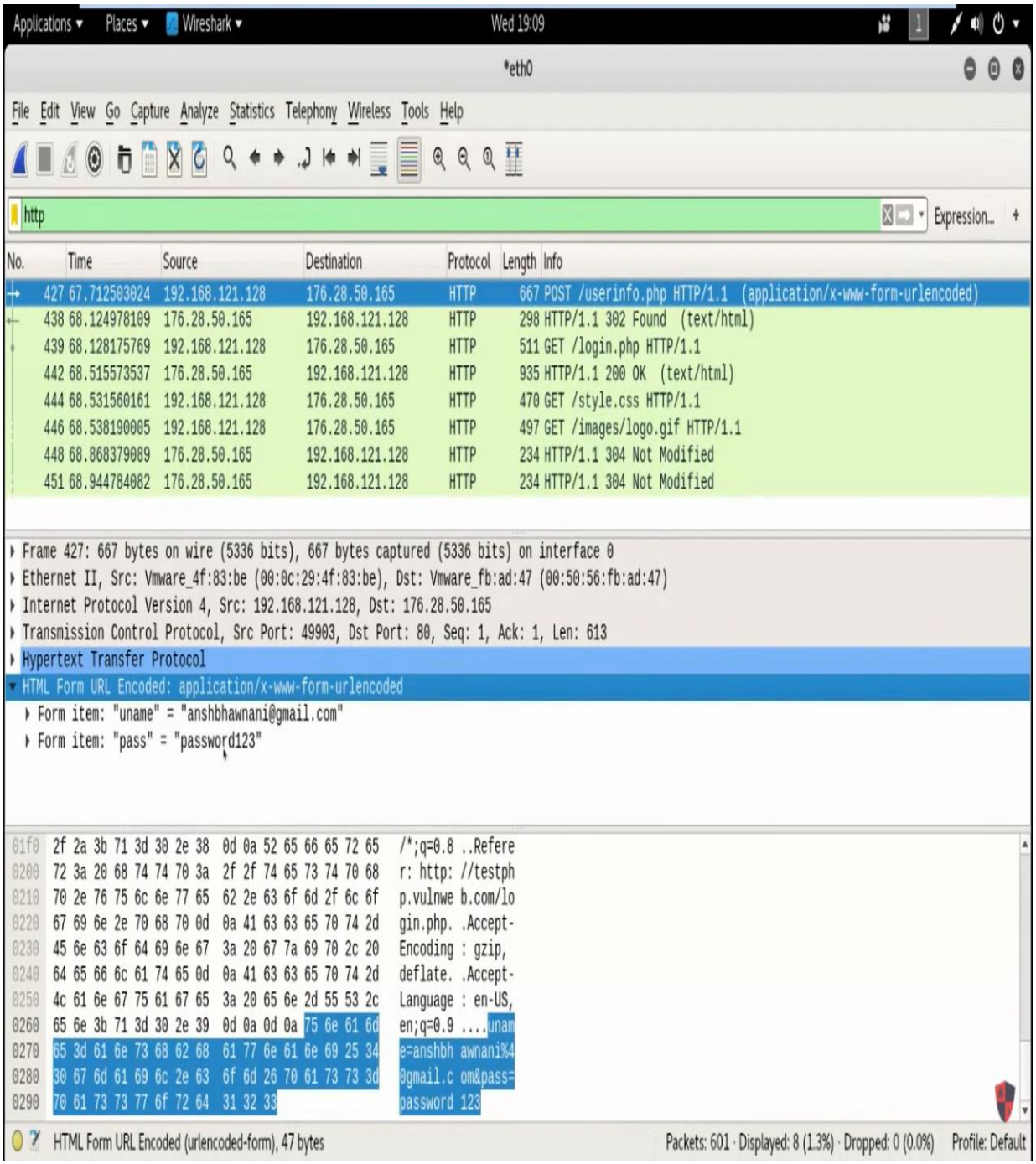


Next you have to select type of network . Here we will select wifi network because our project is on the basis of wireless network . By clicking shark button for capturing wifi network we will enter in the nextf window which shows wifi connected users Numbers , Informations, Ip addresses,sources , protocols ,Destination etc.

Now we will do a practical what an attacker performing activities in our wifi network.
Let Suppose Attacker wants to login for a website .For this we created a dummy html form shown in the screenshot.



Here attacker fills his/her details that is username and password and click on log in.
Now we are monitoring his/her activities on our wireshark tool.
For capturing information we will use a filter called http then we will select user post information .In below we will drop down HTML form url encoded then it will shows the attacker user name and password details that is anshbhawani@gmail.com and password123.


Applications
Places
Wireshark
Wed 19:09
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Length Info
427 67.712503024 192.168.121.128 176.28.50.165 HTTP 667 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
438 68.124978109 176.28.50.165 192.168.121.128 HTTP 298 HTTP/1.1 302 Found (text/html)
439 68.128175769 192.168.121.128 176.28.50.165 HTTP 511 GET /login.php HTTP/1.1
442 68.515573537 176.28.50.165 192.168.121.128 HTTP 935 HTTP/1.1 200 OK (text/html)
444 68.531560161 192.168.121.128 176.28.50.165 HTTP 470 GET /style.css HTTP/1.1
446 68.538190005 192.168.121.128 176.28.50.165 HTTP 497 GET /images/logo.gif HTTP/1.1
448 68.868379089 176.28.50.165 192.168.121.128 HTTP 234 HTTP/1.1 304 Not Modified
451 68.944784082 176.28.50.165 192.168.121.128 HTTP 234 HTTP/1.1 304 Not Modified
Frame 427: 667 bytes on wire (5336 bits), 667 bytes captured (5336 bits) on interface 0
Ethernet II, Src: Vmware_4f:83:be (00:0c:29:4f:83:be), Dst: Vmware_fb:ad:47 (00:50:56:fb:ad:47)
Internet Protocol Version 4, Src: 192.168.121.128, Dst: 176.28.50.165
Transmission Control Protocol, Src Port: 49903, Dst Port: 80, Seq: 1, Ack: 1, Len: 613
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "anshbhawnani@gmail.com"
Form item: "pass" = "password123"
01f0 2f 2a 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72 65 /*;q=0.8 ..Refere
0200 72 3a 20 68 74 74 70 3a 2f 2f 74 65 73 74 70 68 r: http: //testph
0210 70 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 2f 6c 6f p.vulnwe b.com/lo
0220 67 69 6e 2e 70 68 70 0d 0a 41 63 63 65 70 74 2d gin.php. .Accept-
0230 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 Encoding : gzip,
0240 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d deflate. .Accept-
0250 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c Language : en-US,
0260 65 6e 3b 71 3d 30 2e 39 0d 0a 0d 0a 75 6e 61 6d en;q=0.9 ....unam
0270 65 3d 61 6e 73 68 62 68 61 77 6e 61 6e 69 25 34 e=anshbh awnani%4
0280 30 67 6d 61 69 6c 2e 63 6f 6d 26 70 61 73 73 3d 0gmail.c om&pass=
0290 70 61 73 73 77 6f 72 64 31 32 33 password 123
HTML Form URL Encoded (urlencoded-form), 47 bytes
Packets: 601 · Displayed: 8 (1.3%) · Dropped: 0 (0.0%)
Profile: Default

Chapter 4
Result

By performing wireshark tool we captured the information about attacker that is username and password. “uname” = “anshbhawani@gmail.com”
“pass” = “password123”

Conclusion

Wireshark is a program that is used to capture data packets to allow a more precise analysis. The main focus of this tool is observing the data traffic within a network. Such a tool allows the user to examine his/her own computer for protocol errors and problems within the network architecture. Accordingly, Wireshark is also gaining significance within the information technology and network-internal communication, because by finding discrepancies, risks to the PC and its components can be prevented. From a security aspect it must be taken into account that such a program is helpful in discovering and stopping hacker attacks. Especially among people working in the industry, this can be of an advantage if sensitive data is stored on their computer that should never reach third parties.