## 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



(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

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	3
Chapter 1. Introduction	4
(a) Formulation of Problem	
(b) Tool and Technology Used	
Chapter 2. Literature Survey/	7
Chapter 3. Working	9
Chapter 4. Result/Conclusion	12

#### 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.



## 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.

is Tot Yes No.	Capture Analyze Statistics	s Telephony Wreless	Iools He	p	- 0	×
( H Z @ ] 🗎	₹ ≧ + + P S 8	15 3 9 9 9 9	Щ			
Accity & display Titler <0	205/08				5	1 - +
o. Time	Source	Destination	Protocol	Length 3rds		
48498 736.628388	13.107.136.9	10.0.0.252	TCP	60 443 = 57115 [ACK] Seq=56920 Ack=71089 Win=1020 Len=0		
48491 736.626839	13,107.136.9	10.0.0.252	TCP	60 443 - 57115 [ACK] Seq=56920 Ack+71472 Win+1026 Len+0		
48492 736.697628	13.107.136.9	10.0.0.252	TLSv1.2	1330 Application Data		
40493 736.737809	10.0.0.252	13.107.136.9	TCP	54 57115 = 443 [ACK] Seq=71472 Ack=58196 Win=1029 Len=0		
48494 737.105440	2601:603:4e80:afb0:_	2001:558:feed:11	ONS	96 Standard query 0x16a4 A wpad.comptia.org		
48495 737.106664	2601:603:4e80:afb0:_	. 2001:558:feed::1	ONS	95 Standard query 0xbd9a AAAA wpad.comptia.org		
48496 737.137846	2601:603:4e80:afb0:	20011558:feed112	ONS	96 Standard query Rxbd9a AAAA wpad.comptia.org		
48497 737.137847	2601:603:4e80:afb0:_	2001:558:feed::2	ONS	96 Standard query 0x16a4 A wpad.coeptia.org		
48498 737.142095	2001:558:feed::1	2601:603:4e80:afb8:.	DNS	151 Standard query response 0x16a4 No such name A wpad.comptia.org SOA haven		
48499 737.142447	2601:603:4e80:afb0:_	. 2001:558:feed::1	DNS	104 Standard query 0x502F A wpad.hsdl.wa.comcast.net		
48588 737.142618	2601:603:4e80:afb8:_	2001:558:feed::1	DNS	105 Standard query 0x82ba AAAA wpad.hsdl.wa.comcast.net		
40501 737.143251	2001:558:feed::1	2601:603:4e80:afb0:_	016	151 Standard query response Bxbd9a No such name AAAA wpad.coeptia.org SOA haven		
48502 737.143284	2601:603:4e80:afb0:_	. 20011558:feed:11	109996	199 Destination Unreachable (Port unreachable)		
40503 737.161361	2001:558:feed:11	2601:603:4e80:afb0:.	. DNS	156 Standard query response 0x502f No such name A upad.hsdl.wa.comcast.net SOA dhs101.comcast.net		
40504 737.166361	2001:558:feed::1	2601:603:4e80:afb0:.	ONS	156 Standard query response 0x82ba No such name AAAA wpad.hsdl.wa.comcast.met SGA dns101.comcast.net		
40505 737.181369	2001:558:feed:12	2601:603:4e80:afb0:.	. DNS	151 Standard query response Rxbd9a No such name AAAA wpad.coeptia.org 50A haven		
40506 737.181456	2601:603:4e80:afb0:_	2001:558:feed1:2	109996	199 Destination Unreachable (Port unreachable)	1	
48587 737.182435	2001:558:feed:12	2601:603:4e80:afb0:.	016	151 Standard query response 0x16a4 No such name A spad.comptia.org SGA haven		
48588 739,468531	fe88::902e:6cff:fea_	ff02::1	ICMPv6	174 Router Advertisement from 0c:02:27:f7:be:49		
48509 739.917615	Technico_f7:be:49	Microsof_e81f917b	ARP	60 Who has 10.0.0.252? Tell 10.0.0.1		
48510 739.917651	Microsof_e8:f9:7b	Technico_f7:be:49	189	42 10.0.0.252 is at c4:9d:ed:e8:f9:75		-
Transmission Cont Transmission Cont Transport Layer S • TLSV1.2 Record Content Type Version: TLS Length: 1271 Encrypted Ap	Version 4, Sec: 13.107 rol Protocol, Sec Port: Northy Layer: Application Data (23) 1.2 (\$x8303) plication Data: 0000000	0012/19/00149/0000000000	+100501 52 -t1s 88044f518	_mo:179.79 (co:me:co:co:179.70) 9200, Ack: 71472, Len: 1276 660;96687c267		
	76 8c 82 27 f7 be 49 i	08 00 45 00 ( 88 09 04 00 \$ 0 v	Hg k NSFu 2P			1
0000         c4 9d         ed ef f9           010         00 74         16 fd         40           00 8         24 16 fd         40         40           00 4         02 39 67         00         60           00 90         00 90         24 42         56 67         60           00 6         00 90         24 42         56 67         60           6d 63 77         13 5a         5a         6f 67         63 64 67           70 60         64 61 21 21 42 12         10         5a         5a           60 70 66 66 74 43         24 20         7b         66 43 24 20         6a           60 67 66 33 47 23         33 47 20         5a         5a         5a	000 76 06. 48 67 06 660 15 30 44 25 53 46 75 0 00 17 03 03 04 67 00 78 76 30 27 68 52 44 65 78 58 50 27 44 12 47 65 78 58 50 27 44 12 47 65 78 58 50 27 44 12 47 10 35 10 7 66 71 48 71 70 35 17 33 48 68 48 68 61 45 48 68 48 68 45 48 48 49 42 20 20 00 11 40 90 15 44 47 25 20 00 21 15 44 47 27 20 00 21 15 47 20 00	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	2 D - p; 6 h 88p			

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.

The Wireshark Network Analy     File Edit View Go Captur	rzer e Analyze Statistics Telephony Wireless Tools Help				-	o ×
🖌 🔳 🦽 💿 📘 🗎 🗙 🏹	९ ಈ ⇒ ≝ क ± 🔜 🔳 ९ ९ ९ छ					
Apply a display filter <ctrl-></ctrl->						
	Welcome to Wireshark					
	Capture					
	using this filter: Enter a capture filter		× Al	I interfaces shown -		
	Local Area Connection* 9	No addresses No capture filter				
	Learn User's Golds · Wiki · Questions and Answers · Mailing Lists You are nonno Wretlark 3.4.7 (0.4.7-0-ost2d/dise15), You regime automatic undates.					
	а с а станција се стана од около од око Стана од около од окол					
Ready to load or capture			No Packets			Profile: Default

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.

Username	anshbhawnani(	@gmail.c		
Password				
		ogin		
′ou can al	so signup here.			
Signup dis	sabled. Please u	se the userr	ame test and	the passwo

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.

Applic	ations 🔻	Places 🔻	🙍 Wiresh	ark 🕶							Wed	19:09		<b>j</b> # 1	1 1	0.
											*e	ethO			0	0
<u>File</u>	dit <u>V</u> iew	<u>G</u> o <u>C</u> apt	ure <u>A</u> nalyze	<u>Statis</u>	tics T	elephon	<u>y W</u> ir	reless <u>T</u>	ools	lelp						
	10	0	S X	۹. •	*	.) H	• •>		•	Q		Ĩ				
<mark> </mark> http	i i													B B	pression	1 +
No.	Time		Source			Desti	nation		_	Protoco	l Le	ingth Info				
+	427 67.71	2503024	192.168.	121.12	28	176.	28.50	9.165		HTTP		667 POST /userinfo.php HTTP/:	1.1 (application/x-	www-form-urlend	oded)	
÷	438 68.12	4978109	176.28.5	0.165		192.	168.1	121.128		HTTP		298 HTTP/1.1 302 Found (text	t/html)			
•	439 68.12	8175769	192.168.	121.12	28	176.	28.56	9.165		HTTP		511 GET /login.php HTTP/1.1				
	442 68.51	5573537	176.28.5	0.165		192.	168.1	121.128		HTTP		935 HTTP/1.1 200 OK (text/ht	tml)			
	444 68.53	1560161	192.168.	121.12	28	176.	28.50	9.165		HTTP		470 GET /style.css HTTP/1.1				
	446 68.53	8190005	192.168.	121.12	28	176.	28.50	9.165		HTTP		497 GET /images/logo.gif HTTF	P/1.1			
	448 68.86	8379089	176.28.5	0.165		192.	168.1	121.128		HTTP		234 HTTP/1.1 304 Not Modified	d			
	451 68.94	4784082	176.28.5	0.165		192.	168.1	121.128		HTTP		234 HTTP/1.1 304 Not Modified	d			
<ul> <li>Fra</li> <li>Eth</li> <li>Int</li> <li>Tra</li> <li>Hyp</li> <li>HTM</li> <li>F</li> <li>F</li> </ul>	me 427: 6 ernet II, ernet Pro nsmission ertext Tr L Form UF orm item: orm item:	67 byte: Src: Vi tocol Vi Contro: ansfer I L Encode "uname "pass"	s on wire mware_4f:8 ersion 4, l Protocol Protocol ed: applic " = "anshi = "passwo	(5336 33:be ( Src: 1 L, Src cation/ bhawnai ord123	bits) (00:0c 192.16 Port: /x-www ni@gma	, 667 ::29:41 :8.121 4990: -form ail.co	byte: f:83:1 .128, 3, Ds1 •urle m"	s captu be), Ds Dst: 1 t Port: ncoded	ured ( st: Vm 176.28 : 80,	5336 b ware_f .50.16 Seq: 1	its) p:ad 5 Acl	on interface 0 :47 (00:50:56:fb:ad:47) k: 1, Len: 613				
01f0	2f 2a 3	o 71 3d	30 2e 38	0d 0a	52 65	5 66 6	5 72	65 /	*;q=0	8Re	fere	)				4
0200	72 3a 2	0 68 74	74 70 3a	21 21	74 6	5737	4 70	68 r	: http	): //te	stph	1				
0210	10 2e /	0 /5 60	60 70 0d	62 2e	62 6	F 60 2	T 6C	or p	.VUIN	le D.CC	m/10 opt	)				
0220	15 69 6	2 6f 64	60 60 67	0d 41 3a 20	67 7	0007 007	0 74	20 y	ncodi;	)ACC	ept- in					
0230	64 65 6	5 6c 61	74 65 0d	0a 41	63 63	a 05 7 3 65 7	0 74	20 L 2d d	eflate		⊥μ, ent-					
0250	4c 61 6	e 67 75	61 67 65	3a 20	65 66	e 2d 5	5 53	20 L	angua	ie : er	-US.					
0260	65 6e 3	o 71 3d	30 2e 39	0d 0a	0d 0a	a 75 6	e 61	6d e	n;q=0	9	unam					
0270	65 3d 6:	1 6e 73	68 62 68	61 77	6e 6:	1 6e 6	9 25	34 e	=anshl	oh awna	ni%4					
0280	30 67 6	61 69	6c 2e 63	6f 6d	26 70	0 61 7	3 73	3d 0	gmail	c om&p	ass=					
0290	70 61 7	3 73 77	6f 72 64	31 32	33			р	asswoi	d 123						-
0 7	HTML For	m URL End	oded (urlend	oded-fo	orm), 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.