# Capability of Wireshark as Intrusion Detection System

Nitesh Kumar Laljani Student School of CSIT Symbiosis Skills & Professional University Pune, Maharashtra India niteshlbh@gmail.com

Dashrath Suthar Student School of CSIT Symbiosis Skills & Professional University Pune, Maharashtra India Rachit Nandwana Student School of CSIT Symbiosis Skills & Professional University Pune, Maharashtra India rachitnandwana4@gmail.com

Hitesh Sharma Student School of CSIT Symbiosis Skills & Professional University Pune, Maharashtra India

## ABSTRACT

The rise of networks has increased very fastly in this modern world. Our day to- day life mostly depends on the internet. It can be in the form of education, banking, research, business, journalism and many more. This dependency also leads to various types of intrusions. To identify intrusions on the grid, the system must have a detection engine that can detect intrusions automatically without any human intervention. Wireshark is an important tool for the analysis of network packets. But Wireshark lacks the feature of intrusion detection. In this paper, we will show that Wireshark can be considered not only as troubleshooting tool, network analyzer, protocol analyzer, packet sniffer but also a network intrusion detection tool because if the user has appropriate knowledge about attacks and data packets, then he could easily identify an attack by observing a specific data packet pattern. In this paper, an attack pattern dictionary will be created using which captured livedata packets will be manually mapped in order to detect intrusions. We will also identify various attacks captured by Wireshark using this process.

Keywords- Attacks; Attack pattern dictionary; Intrusion; Intrusion detection; Wireshark

## I. INTRODUCTION

The intrusion detection system is the system that tracks any security policy breaches. It is a software application that scans a malicious operation or regulation violation network or device. These are categorized into the Network Intrusion Detection System (NIDS) and the Host Intrusion Detection System (HIDS). Wireshark is a software tool that uses a network interface to track network traffic. It is the most widely used method for tracking the network. Wireshark is commonly used by the following:

- Network administrators use it to review TCP retransmission, troubleshoot network problems, visually understand packet loss and graph high latency packet responses.
- Network Security controller uses it to inspect security problems like detecting anomalous behavior that could indicate malware, searching for unusual domains or IP address endpoints, using the IO graph to discover regular connections to command and control servers and extracting large DNS responses and another oddness which may indicate malware.
- Quality Assurance engineers use it to validate network applications.

- Engineers use it to test the implementation of protocols.
- People use it to understand internal network protocol.

It is used to develop and enlighten protocols for troubleshooting, analysis, software, and communications. It runs on Linux, OS X, BSD, Solaris and some other operating systems like UNIX and Windows like Microsoft. Wireshark supports a wide range of protocols such as TCP,UDP, HTTP, and even specialized AppleTalk protocols. It has a range of advance choices such as packet filtering, packet export, and name resolutions. Wireshark is capable of capturing live network data. The sniffing [1] of the Wireshark network uses the promiscuous mode. Next, Wireshark converts the code of the network into a promiscuous mode where it can collect raw binary data that flows through the network. Then the chunks of the captured binary data will be translated into a readable form. Depending on their numbers, the packets are also re- assembled. Eventually, it analyzes the data collected and reassembled. The initial analysis includes defining the type of protocol [2], the medium of communication, port numbers, etc.

## **II. Literature Review**

Vivens Ndatinya [3] demonstrated network protocol analysis on Wireshark and discovered various attacks using conventional network attack discovery methods, such as hidden FTP and IRC channels, port inspection, ICMP attacks, Bit Torrent services, etc. He also showed that a wide range of security threats and attacks on networkedcomputer networks can be found in Wireshark's packet review. Sameena Naaz [4] used Wireshark to study andinvestigate the DHCP and DNS protocols. Using cisco packet tracer student, she had configured two computerswith DHCP and DNS servers and dynamically assigned them network parameters with the servers. She also researched the Rogue DHCP server identification. She studied all LAN and home network DNS packets and observed delays in DNS errors. Wolf-Bastian and Lars Wolf [5] demonstrated without hardware modifications the modification of the sky wireless sensor node into a packet sniffer. The critical timing parameters were evaluated by them.

In Wireshark, which offers a wide range of existing dissectors for different protocols, packets obtained by the sniffer node can be analyzed according to them. Therefore, for a custom MAC protocol, they developed their dissector. Mohsin Khan [6] had researched and examined that when an IP address is allocated using DHCP, what exactly happened in the back panel.

He introduced the DHCP client-server model and then captured DHCP packets exchanged between DHCP client and server using Wireshark. He studied and examined their contents thoroughly to promote and appreciate the entire contact process. In packet data interpretation and data handling, Usha Banerjee [7] highlighted the capabilities of Wireshark. She reiterated the need for IDS / IPS devices in any network in her experiment. In ACL (Access Control List) scanning, she used Wireshark. According to her, Wireshark can be built into a comprehensive program for intrusion detection by using filtering commands and supplementing utilities properly. Rashmi Hebbar [8] collected live network traffic and used Wireshark and Snort to conduct a detailed analysis of captured packets. She spoke about Wireshark alone being unable to produce an alert or take security measures against unauthorized access. The Snort intrusion detection tool will prevent the device from any intrusion, and warnings for these suspicious activities will be created. The graph of captured files shows the network structure information and insight into the issues.

S. Pavithirakini [9] addressed Wireshark's work briefly, its benefits, and the Wireshark tool improved. By using the ping command on the OS (Operating System), his idea triggered a ping flood scenario. Wireshark was installed on the victim's network to calculate the number of ping packets identified over a given timeline with a threshold orientation dependent on the identification of a flood attack. Ming-Hsing Chin [10] has shown an aggressive attack, i.e. Man in the Middle (MITM). Wireshark collects and analyzes the MITM behaviors in his experiment. From the results, the characteristics of the MITM attack were established. He also addressed preventive measures and stressed the importance of abnormality awareness.

# **III. Wireshark as Intrusion Detection System**

Since Wireshark is not an intrusion detection tool but the user with expert knowledge can detect intrusions on the network. Wireshark consists of some expert features which can help the user to detect any intrusion [13] and suspicious activities on the network. Here is a list of some advanced features of Wireshark:

# A. Display filter

Wireshark has two types of filters: filter capture and display filter. A capture filter cannot be modified. Display filters are used according to certain requirements to display packets in Wireshark. Display filters enable us to focus on the packets in which we are interested in while hiding uninteresting ones at the moment. Packets are displayedbased on protocol, field presence, field values, and field comparison.

# B. I/O graph

Wireshark has the function of an I/O graph that summarizes the flow of the packet. Wireshark I / O Graphs display the total traffic in the capture file, usually measured in bytes or packets per second.

## C. Network conversation window

Contact between two separate endpoints is a connection on the network. The contact window comprises four columns together with names, packet counters and byte counters: the start time of the chat, the length of the conversation inseconds, and the average bits in each direction.

# **D.** Coloring rules

It is possible to apply the coloring rules that reflect an infringement. The coloring rules require a word, a list (based on the view filter format), a foreground color and a background color.

# E. Expert information

Expert knowledge is a compilation of exceptions in the Wireshark capture log. The general idea behind the following "Expert Info" is to have a more "uncommon" or simply notable perception of network activity. The quantity of expert knowledge depends largely on the protocol used.

# **IV. Research Methodology**

To identify intrusions on the grid, the system must have a detection engine that can detect intrusions. But Wireshark lacks this feature. We have designed a general architecture of manual attack detection using Wireshark



## Figure 1. General Architecture of Manual Attack

## **Detection using Wireshark**

According to this architecture, data packets from the internet or private network are captured by Wireshark. After capturing, data packets are saved in a .pcap file in the system. A dictionary will be created which consists of all the attack patterns that can be identified by the Wireshark. Attack patterns will be mapped manually with the saved file of captured packets to detect attacks. Once the mapping process will complete, the list of manually detected attacks is created as the output.

In this architecture, the mapping process will be done manually. Wireshark is not able to detect attacks automatically because it does not contain any detection engine, so we are developing a mapping process in which a manually created dictionary of attack patterns will be compared with the data packets captured by Wireshark. After comparison, a list of attacks will be created which are identified in the mapping process

# **V. DICTIONARY OF ATTACK PATTERN**

To implement the defined model and detect intrusions manually, a dictionary of attack patterns has to be maintained. Here is a list or various attack patterns that can help in detecting intrusions on the network.

#### A. Attack – DDOS (Distributed Denial of Service)

When a large number of data packets with the same source address and destination address are captured then it can be considered as a DDOS attack [14]. The data packets captured by the Wireshark will have the unknown protocol and the length of each packet will be the same. All these features indicate that it is a DDOS attack. When the DDOS attack takes place, a large number or similar packets are captured within a short period.

	• - 1 - 7 - 7 - 7 - 4 - 7	TAX TAXAB		
	Access in case			10 June 1
	and in case of the second	The second second	The second	
	and the second sec		2010 000 000	
	Contract in the second		Marchine and Long	
	A BOLLER BALLER	and and a second	PRI 1076-1075-10-2	
	The second second second		day fuels- multi filter-	
	Carlo and an other states of the states of t		MI 1000 Not. 19 1	
	and the second s		and the second sec	
	the second second		and the local side of	
			<ol> <li>MC 1405 2010, 101 (1</li> </ol>	
	the state of the s		and the local states and the	
	A DECEMBER OF A DECEMBER OF		Bio Carlo Tana Lini - F	
	- Contraction of the second		BALANCE ALL ALL ALL ALL ALL ALL ALL ALL ALL AL	
			and their store with a	
	- 10 Brown Brown - 10 Jan 4	100 (00 H L L L L L L L L L L L L L L L L L L	480 5 815 5 441, 7 5 8	
	and the second s		and the best times	
			AND DATE AND THE R	
			And the second sec	
	the second second second		The state was a set of	
	the far manual time to be a lot		Man Andre Samer and a	
			MO 1000 1000 1010	
	and the second s			
		and the second sec		
	the second second second	and the second s	and the local side of	
	the second the later of		and the local size of	
	the second the second		METERS BUILT AND A	
	CONTRACTOR OF THE R.		and heart from the lat	
	The second se		Martin fam. 17 P	
	- In the second second		and the second sec	
	the local data and the local data	10 mm	and have been also a	
	in the local design of	Merson and	Zineer.	
HER KIN THE DATE AND ADDRESS OF A DATE AND A	And services in such	NAMES OF TAXABLE	1.00	
and him the star and the set free and the	And Allow States in the	And and the state		
	STATE STATE LINES TOTAL	which wants from our	5. F	

Figure 2. Screenshot of DDOS attack

## B. Attack – MITM

When the source MAC address of the captured data packetschanges from normal address to unusual address then the MITM attack takes place. The ARP packets are sent back and forth, but in packet 56, the intruder sends another ARPpacket with a separate MAC address from the router, delivering the data to the attacker and then the router. So hence MITM attack [15].

a			*****	monarian (Weephark 3.12	4 1v1 13.4-0-ge-40010a H	tion stration	1.1.11
E4x . 1	de the Dr	Caller Andres Settlers	Talophory Lasts personals	Abelar			
		1 H H H H H I A 4	a a A a a a		1 15 16 1 22		
-			¥ 84	manager. Clear Apply Sa	- Ration and		
-	Sara .	Service.	Brooks SANC	Destination	Event MARK	Property	Langth July
	43 0.000043	373.38.0.387	100112001801401	TAL 235 893 847 11	27443.31107188	TEF.	88.43492-
	42.010355.00	122-230-20-02	CENERGELERINGLER	172-58.0.507		1.000	ESA BLANKS
	A8.41.451887	ATELER. 0. 800	COMPANY OF A COMPA	CREATERING	CTARMERS INTERN.	1001	#3. 94 arves
	KI G. OULGER	13.11.00.01	CONTRACTOR - 100 - 100		- BETS_EBINE(#BI)	CHECK.	134 EXample
	44 0.011200	475.18.0.0.007	4411,001001FB	A PURK AND AN	CONTRACTOR OF CAR.	1966	73.00 81464
	43.0.005588	82-251-20-45	CREAK BEIGHTER	172.58.0.597	04112-0120-00	Cont.	00% 05 arvite
	48 0.006578	BPR/BROWSERP	BARKLER BRITE	4.8.4.4.9.29.48	A THUR ALLOY DE	0.00	80 84 ATMS
	41.0.000188	CRACK AND DR. MR.	CONTRACTOR OF CAR.	1.	BRANCH BRANK	EWIL .	800.58 ares
	48.0.000214	APPLER BUSIES	CONTRACTOR OF AN OTHER OF AN	17,151,00,00	CONTRACTOR OF A DECISION OF A DECISIONO OF A	08/5	75 55 ands
	** 0.004005	CARCENEL ROLLAR	CHINGOL BAUBALBS	C. 8.781.881.91.887		1.6840	111. EL 24464
	99-6-DE2835	472.18.0.107	CONTRACTOR OF A CONTRACT OF A CONTRACT. CONTRACT OF A CONT	120103-20085	COLUMN 81 (07-38	0.00	76 EX.amia
	ALCO, DELETE	4.8. 8.9.8. 80.48	CONTRACTOR OF CAR	3.878-58.81.887	0411,00104.00	1411	ERR DAMAGE
	12.0.000211	172.18.0.587	404 T. T. LOUIS T. D. B. 1 W 10	13.1.1.1.1.20.101	LEVINGRA DATEST	1001	77.54.8144
	33 0. 200359	17-117-20.41	COLUMN STORY (ST	377.38.0.287	2011.00.24.70	Date:	111 District
	5414-579.500	PARTING LOLAST COLUMN	Interestant and a set of a set	B0011240156070	00000.00000000000000000000000000000000	180	60 who for
-	NS. III, DODGS J	5e11_c0:34:F0	0411,40:54:70	These and the part of the case	manufactor. before and	489	43 373.14
-	35.0.000011	personal and the second second	parafrates, left bet can	0011 00:100 FB	math.exits.fr	440	60.177.15
	57 8,904785	A DOLLAR DOLLAR	and Statistics of the second	100 C 10	mana 1 8 1 9 2 4 1 8 7 1 9 2 1 9 9	#77P	860 687.71
	14.0.000188	-FA- 8.2%, W3- 8.8.7	manhatics_affine	473.34.4.247	8411, 491114 (FD	46.0	784 (129-1
	11.0.000078	372.58.0.557	BATTLADIBE FOR	24.329.89.348	maulatt-,bf:01:se	TCF	44.41491-
	And in A PARTS	378.38.0.807	0011.00.00.00.00	A4.1.25.89.247	man have a state of the later		1005 067-70
	41-0.079392	74.323.93.347	NEW TAXES, MALES INC.	372.56.0.507	0011-00-10-70	ATTE	85 WTTP/3
	42-0.000051	177.18.0.107	##\$\$_\$@\$\$41F0	24.1225.00.247	man het to . Ad 193 tes	71.0	66.43683-
-			and here the restreet				
		HHERHE	HHEHEH :	**			

### Figure . 3. Screenshot of Man -in -the- Middle attack

#### C. Attack – ARP Cache Poisoning Attack

In the figure, in packet number 57, the destination IP is .147, the MAC ID shows up as Hewlett-Packard i.e. it is an HP computer. But if we look at an earlier packet that is supposed to be sent to the router like packet 40 it's also being sent to IP .147 but the MAC address is for Cisco router. This shows that it is an ARP Cache Poisoning attack. Therefore, in short when two packets with the same source address, same destination address but different destination MAC addresses are captured then the attack is ARP Cache Packet Poisoning attack [15].





## D. Attack – Exploitation (Malicious Sites)

In the figure, packet 6 has a "302 moved" response. This response is unusual and can be a malicious site. The location of the packet in packet detail pane is also not readable. In follow TCP stream of the same packet, script command consists of gibberish data and after scrolling down the follow TCP stream, iframe attack is taking place. In this scenario, it is an attack that is sent to the user.

										aurora pca	P M	[Wireshark 1.12.4: (v1.12.4-0-gb4861da from master-1.12)]	
24. 1	Lau	Yes	-	Capture	down	. 54	ideh To	-	Inch	jonamata 1545			
			A	Sin S	1 26 1	314	4.		5 4	-	4 94	Q.Q.E.   # M 19 %   23	
Eiter	C									w Equation	L . C	Ocar Apply Save Authort and	
	1 2 3 4 5 7 8 4 1 5 7 8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	term 0,0000 0,0000 0,000000	10000 224 B 204 S 204 S 205 S 20	Small State	64.100 64.100 64.100 64.100 64.100 64.100 64.100 64.100 64.101 64.103 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.104 64.105 64	206 303 206 200 200 304 300 (1532) 304 (1532) 304 (1532) 304 (1532) 304 (1532) 304 (1532) 304 (1532) 304 (1532) 305 (1532) 30 (1532) 305 (1532) (1532) (15	t bitta) sec Cr 192 Fr Par Gretas Gretas Gretas (1) 2 (mo	vituation 92.168 92.169 92.168 92.169 92.168 92.169 92.168	.100.2 (#0). 100.2 (#0). 100.2 (#0). 100.2 (#0). 100.2 (#0). 100.2 (#0). 100.2 (#0).2 (#0).2 100.2 (#0).2 (#0).2 (#0).2 (#0).2 (#0).2 (#1)	Pro 20 Tri 20 Tri	528.0 0.33	d Longin, Mar. 40 L	24

Figure. 5. Screenshot of malicious packet



Figure. 6. Screenshot of TCP Stream of malicious packet

	Follow TCP Stream (tcp.stream eq 0)	,
tream Conte	nt	
0a391c1c e0f22296 10180f26 84b2d042 033a2022 .var RX .for (1 RXb +	0.300.00.00.00.00.00.00.00.00.00.00.00.0	
.var vul .var Ng: .for (1	wGWsvUonxrQzpqgBXPrZNSKRGee = location.search.substring(1); xAXnnXrILOBMwVnKoqnbp = '; oj:lexb.length;1++) {	
vuwGws vu	onxrqzpqgBxPrZNSkRGee.charcodeat(1%vuwGwsvuonxrqzpqgBxPrZNSkRGee.length));	
window	<pre>nmx(l2bodwwineQuests) file(nmx(l2bodwineQuest)); mxr(2programmerzuskRede, charCodeat(1%vuneGuestNonxr(2programmerzuskRede, length)); ["eval".replace(/[A-z]/g."")](NqxAxnnx1ILOEMwvnkoqnbp); ;</pre>	
<pre>vuwGwsvU</pre>	nnxrq2pqgbXFr2MSkRGee.charCddetdClawWGBsVUonxrq2pqgbXFr2MSkRGee.length)); ["eval".replace(/[A-z]/g,"")](NqxAxnnxiILoBMwVnKoqnbp); s	
<pre>c/script: c/head&gt; chody&gt; cspan 10/ mfowrve onload= c/body&gt;</pre>	<pre>nmxrqzpqgxXrrzMskRGee.charCodext(%x/wGssVUonxrqzpqgbxrrzMskRGee.length)); ["eval".replace(/[A-z]/g,"")](wqxxxnnxilcomwvnkoqnbp); &gt; Conversion-conve</pre>	
<pre>vuwGwsvU</pre>	<pre>onsrd2piggBXPr2MSkRGe.charCddxLdCfXVWGGSVUonxrd2piggBXPr2MSkRGe.length)); ["eval".replace(/[A-Z]/g."")](NqXAXINXiLLOBMWVNKoqhbp); s Ververcopro2UoUxAffIbszyFINYD100ASHKKtod1KSFFFFFFFFKGGE[1902cffebme.srce#/ euvinementsfffbaneckeffKszuctuvgmuzCAMAfjEctIbr0vPrctcffbattMarSyx1.giff eGDYJWMfsrdrvXIYApnuPoCMjRrSZuktbVgmuZCAWsKjEctIbr0JPFctcflbsttMRrSyx1.giff </pre>	
<pre>// index // inde</pre>	<pre>onvrdphgBXPrzMskkGe.charCddAtdCtwiwGesVuonvrdphgBXPrzMskkGee.length)); ["eval".replace(/[A-Z]/g."")](NqXAXNNXILLOBMWVNKoqNbp); s VhyvretounozUGUXAfIDszveIIIVN)]0]AccHkktGdlKSUFUEstKGGES[IV&gt;&gt;iframe_src=#/ gdvJsWfSodVxIVAnuPocHjRFZUKLDVgMuZCXMAK[ttclbPuJPPctcflhsttMRrSyx].gif eGDVJWHfsrdrvXipAnuPocHjRFZUKLDVgmuZCXWKKjtEclbPuJPPctcflhsttMRrSyx].gif HsgGgif, Hsge/x-xbitmap, HsgG/Jpeg, Hsge/Jpeg, appl(ation/x-shockwave- http://sl65100.22/jf0foffstuiti.ame</pre>	
<pre>// index // inde</pre>	<pre>nonrdppggbXPrzMskRGee.charCddext(%x/wGGsVUonrdppggbXPrzMskRGee.length)); ["eval".replace(/[A-Z]/g,"")](wqxxxnxilcomwvrkoqnbp); &gt; NonrdppgbXPrzMskGee.charCddext(%x/wGGsVUonrdppgbXPrzMskRGee.length)); &gt; NonrdppgbXPrzMsKGee.charCddext(%x/wGGsVUonrkoqnbp); &gt; NonrdppgbXPrzMsKGee.charCddext(%x/wGGsVUonrkoqnbpycc/chindsvec/html; &gt; T/ SSRGGTNEfaoNekEqaMyAUALUMYW(event)" /&gt; /bothfsrdrvXIYApnuPoCMjRrSZUKtbVgwuZCXwxKjtEclbPuJPPctcflhsttMRrSyxl;gff fmage/gff, image/xsthtmap, image/jpeg, image/jpeg, application/x-shockwave- http://192.166.100.202/info?rfwEujcJmpP</pre>	
<pre>vuwGwsvU</pre>	<pre>onsrd2pigBXPr2MSkGee.charCddAtC(1xvWoGsVUonxrd2pigBXPr2MSkRGee.length)); ["eval".replace(/[A-Z]/g."")](MqXAXINX1LODMWVIKOqNDD); &gt; ovkyrstouprozuouxaf1DszyHINYDJ0jASCH042q0]EureutictorConflictiv_Sciframe_srce_/ isigfarEaoNekEqamyANALLNYK(event)" /&gt;</pre>	

Figure. 7. Screenshot of iframe attack

At the follow TCP stream of packet 25, window command shell and attacker is getting admin privileges to the user's files like there is a password.txt. This is also an exploit

4								autori	apcap	[Wires	hark 1	12.4	(11	2.4-0	gb48	61da	from	mast	ber-1.1	2)]	
Ele	Edd Yew	Gell	Cipture	druhy:	e Station	ics Telep	tony Ico	its pitemats	Hele												
		1	-	x	-		071	1	Q	Q Q	<b>1</b>		1	34	33						
Fitter.								e Erp	ression	Clear	Apph	6 5	ave 1	haktipl							
No.	Time		leurce .			Desti	nation		Protect	ol Len	gth h	de .									
	19 0.000	0146	192.16	8.100	206	192	168.100	0.202	TCP.		60 1	1031	-80 (	ACK1	Sequ	597 1	Ack=1	11579	. wine	61609	Lenso
	20 0.000	1110	192,16	8.100	206	192	168.100	202	TCF		60	TCP	wind	OW UP	date	] 101	11-80	D [AC	K] Se	0-597	ACK-11
	21 0.45	5107	192.16	8.100.	206	192	168.100	0.202	HTTP		475 0	DET .	/1nfo	WTVE	GDY3	WINTER	cdcva	SYAD	INUPOC	HIRPS	ZUKEDVO
	22 0.19	9959	192.16	8.100.	202	192	168.100	0.206	TCP		60.1	80-11	1 160	ACK]	Seq-	11529	) ACI	-101	8 win	-6451	8 Lenno
	23 0.00	1166	192.16	8.100	202	192	168.100	0.206	HTTP		201 +	ITTP.	/1.1	200 0	ж (	GIFES	94)				
	24 0.163	1592	192.16	8.100	206	197	168.100	3, 202	TCP		60 1	1011	-80 [	ACK]	Seq-	1018	Ack.	1167	6 orth	+6408	Tillen+0
	25 2.75	53R1	192.16	1.100	206	192	164.100	0,202	207		62 1	1032	-4321	1.5 1	() 50	Q=0 %	W10-0	64240	Len-	0 NSS	-1460 5
-	Contraction of the	JUN I	1000020	11100	202	192	ALCONG. OF	0.205	- ICA	_	0410	1144	11000	and a	1. AU	a de marce	aunun	ALK	distanting the	101004	A REAL PROPERTY.
	ernet Pr nuttst ource Pr bestinat Stream TCP Seguence schrowle teader Lo 0000 rindow S	orticion Colorti on Colorti ion Prindex ment i numbi dgmenn ength 0.0000 12e vi	01 vers trol 0 1032 (1 prt: 4 1] er: 0 t number 28 by 0010 alue: 0	1001 4 1032) 121 (4 (re ri 0 rt 1 4240	() SPCI () SPC	sequen	ce numbe	96 (192.10 1032), 041 17)	100. Port	206); 4321	Dst: (4321	197.	168. Gegi	100/2	02 (1	19271	68.1	60.2	02)		
	calculat hecksum ingent po options:	ted w : 0x7 ointer (8 b)	indow : Idb [vi r: 0 rtes).	Haxia	64240) ton dt	sabled] ment si	ze, no-c	operation	(NOP),	NO-05	erati	ion i	(NOP)	, s.40	к ре	raite	ed				

Figure. 8. Screenshot of exploitation -1



Figure. 9. Screenshot of exploitation -2

# **E. Port Scanning:**

To check the open ports in the network, first of all, check the conversation window and see which protocol's data packets are received the most. In the figure, the most packets are of TCP. Select any TCP packet and check the destination port from packet detail pane. Write a filter command of that port indisplay filter and it shows all the packets with the same destination port. The figure shows that the server is trying to reach out to the intruder, but the attacker rejects the link ending with the TCP handshake. So it seems like the DNS port is already accessible.



Figure . 10 Screenshot of Port Scanning

## F. Attack - Packet sniffing (Username and Password)

In order to sniff password and username [17], Right-click on the suspect packet and open the next packet to navigate the follow TCP stream. The follow TCP stream shows the username and password.

Dearn Content		
····· ·······		
User Access Verification		
Username:	-	
Password: ciscol2345		
R1>eennaabb11ee		
Password: danscourses		
R1#	I	
Rl#sshhooww lipp rroouuttee		
Codes: C - connected, S - static, R - RIP, M - mobil D = LGGMP, EX - ELGGMP extremal, O - OSPF, IA N1 - OSPF NSSA external type 1, N2 - OSPF vSS E1 - OSPF external type 1, R2 - OSPF external is a - IS-IS inter area, " - candidate default, 0 - OOG, P - periodic downloaded static route	e, B - BGP - OSPF inter area A external type 2 type 2 el-1, L2 - IS-IS level-2 U - per-user static rout	e
Gateway of last resort is not set		
c 192,168,0.0/24 is directly connected. FastEther	net0/1	
R14		

Figure . 11 Screenshot of Packet Sniffing

# **VI. Result and Discussion**

Wireshark captures live data packets from the network and the packets are saved in .pcap format file. The file is then mapped with the attack patterns saved in the attack pattern dictionary. If the same packet pattern is found in the saved packet file as defined in the attack pattern dictionary then we can say that the following attack takes place on the home networked computer system. After mapping the dictionary and the captured data packet file, a list of attacks is identified in our home network.

S No.	Attack Name	Detection
1	DDOS Attack	Not Detected
2	MITM Attack	Not Detected
3	ARP Cache Poisoning Attack	Not Detected
4	IFrame Attack	Not Detected
5	Exploitation 1-malicious Site	Detected
6	Exploitation 2-Unauthorized	Not Detected
	Attack	
7	Port Scanning	<b>Open Port Detected</b>
8	Sniff Username and Password	Detected

#### Table I: List of Manually Detected Attacks on Lab Network

## **VII. CONCLUSION**

Wireshark is a very important tool that has several advanced features like display filters, I/O graphs, color coding, expert information, etc. that can be used to detect various types of attacks on the networked computer systems. The paper introduced a model of a manual attack detection process using Wireshark. The defined model consists of an attack pattern dictionary in which a list of attack patterns are introduced. In the defined model, Wireshark captured live data packets from the network that are manually mapped with the attack pattern dictionary. Wireshark can identify a number of attacks like DDOS attack, Man-in-the-Middle attack, ARP cache poisoning attack etc. The model is usedfor the identification of various attacks on the network. This experiment showed that the Wireshark can not only be used as a packet analyzer, troubleshooting tool but also as an intrusion detection tool. A user with expert knowledge ofdata packets, protocols, etc. can detect intrusion usingWireshark.

## REFERENCES

[1]. Alia yahia, Eric Atwell, "Evaluation of Capabilities of Wireshark as Intrusion Detection System", Journal of Global Research in Computer Science, Volume 9, No. 8, August2018.

[2]. Santosh Kumar, "Detect/Analyze Scanning Traffic using Wireshark", PenTest Magazine, June 2013.

[3]. Vivens Ndatinya, Zhifeng Xiao, Ke Meng, "Network Forensic Analysis using Wireshark", International Journal of Sensor Networks, vol. 10, Issue No. 2, 2015.

[4]. Sameena Naaz, Firdoos Ahmad Badroo, "Investigating DHCP and DNS Protocols using Wireshark", IOSR Journalof Computer Engineering, vol. 18, Issue No. 3, May- June 2016.

[5]. Wolf- Bastian Pottner, Lars Wolf, "IEEE 802.15.4 Packet Analysis with Wireshark and Off- Shelf Hardware", Institute of Operating System and Computer Networks.

[6]. Mohsin Khan, Saleh Alshomrani, Shahzad Qamar, "Investigation of DHCP Packets using Wireshark", International Journal of Computer Application, vol. 63, Issue No. 4, Feb 2013.

[7]. Usha Banerjee, Ashutosh Vashishtha, Mukul Saxena, "Evaluation of Capabilities of Wireshark as a tool for Intrusion Detection System" International Journal of Computer Application, vol. 6, Issue No. 7, September 2010 [8]. Rashmi Hebbar, Mohan K., "Packet Analysis with Network Intrusion Detection System" International Journal of Science and Research, vol. 4, Issue 2, Feb. 2015.

[9]. S. Pavithirakini, D.D.M.M. Bandra, C.N. Gunawardhana, "Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS attacks" International Journal of Scientific and Research Publications, vol. 6, Issue 4, April 2016.

[10]. Ming- Hsing Chiu, Kuo- Pao Yang, R. Meyer, T. Kidder, "Analysis of a Man-in-the-Middle Experiment with Wireshark", http://worldcompproceedings.com/proc/p2011/ SAM4991.p df

[11]. Sandeep Choudhary, Nanhay Singh "Safety Measures and Auto Detection against SQL Injection Attacks", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2,December, 2019 pp. 2827 – 2833

[12]. K Sinha, S Choudhary, S Paul, P Paul "Security of Multimedia in Cloud using Secret Shared Key", International Conference on Computing, Power and Communication Technologies, 2018, pp. 908-912

[13]. Haroon Iqbal, Sameena Naaz, "Wireshark as a tool for detection of various LAN attacks", International Journal ofComputer Science and Engineering, vol. 7, issue 5, May 2019

[14]. <u>https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5\_635</u>

[15]. C. Calvert, Taghi M. Khoshgoftaar, Maryam M. Najafabadi, C. Kemp, "A Procedure of Collecting and Labeling MITM attack Traffic", International Journal of Relaibility, Quality and Safety Engineering, 2017, vol. 24, No. 01.

[16]. H Awang Mangut, Ameer Al- Nemrat Chafika Benzaid, Abdel- Rehman "ARP Cache Poisoning Mitigation and Forensics Investigation", IEEE, August 2015.

[17]. Pallavi Asrodia, Hemlata Patel, "Analysis of various Packet Sniffing tools for Network Monitoring and Analysis", International Journal of Electrical, Electronics and Computer Engineering, ISSN No.: 2277-2626.