RESEARCH REVIEW JOURNALS
Volume-02
Issue-08
August-2017

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com

To Study About the Content Analysis and Network Setup for Basic Understanding of Network Communication

[1]Devajit Mahanta and [2]Dr. Ashish Chaturvedi

[1]Research Scholar, Kalinga University, Raipur, Chhattishgarh
[2]Associate Professor, Kalinga University, Raipur, Chhattishgarh

ARTICLE DETAILS

Article History
Received: 22 July 2017
Accepted: 09 August 2017
Published Online: 28 August 2017

Keywords
Computer Networks, Social Networking, Security, Applications, Information..

ABSTRACT

Some risks, such as viruses, worms, root kits, etc., have been found to cause no apparent change in the flow pattern on networks and can be recognized by matching the signatures via packet inspection. They are thus beyond the scope of this project, and for this project work, their capture is not included. It should be remembered, however, that these are effective weapons from which miscreants cause other forms of attacks, such as DoS, scanning, port flooding, etc., causing changes in flow patterns. Communication between the application and the IP is provided by TCP. It establishes a 3-way handshake link, transfers information, and then disconnects it with a 4-way handshake. The device does not send data after sending the FIN flag. The port remains open in listening mode until the ACK against the FIN flag is received. If the port is not open during link initialization, the device will send RST instead of sending ACK. During link termination, attackers may use the half-open technique vulnerability or send RST instead of ACK while the connection is being formed. In order to identify open ports, TCP scans are very common, which can subsequently be exploited to cause cyber attacks. By breaking the TCP connection into a client-to-attacker connection and an attacker-to-server connection, man-in-the-middle attacks can be enabled. In TCP links, data loss or data delivery out of order due to network congestion contributes to retransmission. In the case of anomalous cases, large numbers of malformed packets, duplicate packets and retransmissions are found.

1. INTRODUCTION

In all aspects of our lives, computer networks have collapsed, such as social networking sites, banking, shopping, industry, education, travel, science, etc. Computer networks are different systems that host a large number of software and web services for computers. One vast network of interconnected computers worldwide is the Internet. By using a variety of protocols, these devices communicate via packet transfers. Intelligent packet routing is a dynamic operation within a network. Filtering, routing to neighbouring routers or subnets and transformations are performed by routers. Network traffic includes the flow of packets between two endpoints.

In view of the legal issues associated with the capturing of live data, global scalability and smart routing, it is not possible to get a full view of the network flow with the current technology restrictions and resources available. The network packets, however, are collected using different methods and the study of the network packet flow is used to analyze communication patterns on a computer network. Network data is deduced from contact patterns.

Network flow data offers information on network activity, configuration of the network and policy enforcement. For management, accounting, network planning, monitoring activities, investigations, troubleshooting of various network problems, security, etc., computer network understanding is essential. Different studies are conducted to meet these aspects, and researchers create a connection between different parameters of the network flow. The methodology and scope of analysis of network packets differs on the basis of the intent. Protection, since it is a public domain, is a big problem with the network. Sniffing, snooping, eavesdropping, botnets, Distributed Denial of Service (DDoS) attacks, SQL injection and many other kinds of security threats are vulnerable to the cyber world. Stalking and intimidation, identification fraud and theft, technological discovery, standard lead development investigation, anti-pedophile investigation, disciplinary proceedings, company policy breaches, identity checking, alias vetting, development of subject character, discovery of accomplices, violations of probation, other court order violations, cr cr.

Monitoring of the traffic across network and correct examination of the content flow will identify any malicious activities from security threat point of view in the cyber world. The area of research for the present study is the control of the network from a safety perspective. All network issues stem from the stage of the packet. We need to go to the packet level to better understand network problems and the related security concerns. It is important to consider the theoretical connection between the patterns of packet flow and the security issues resulting from them. For data analysis, various methodologies and techniques are used, including statistics, profiling, behavior-based approach, sampling, visualisation and computational infrastructures. Network packet capture can be achieved using different methods. Each instrument has its own applicability and limitations that need to be checked before deciding on the study methodology.

The framework for the conduct of the study has been developed based on the above. In order to provide an overview of different protocols that make communication possible, the network traffic is first analyzed. In a network, the usual patterns of packet flow are studied. To identify co-relationships between them, variables such as protocol types, packet size, flow rate, etc are studied. Using third party software, experiments are carried out and the known typical attack scenarios are simulated. During cyber attack situations, the changes in packet flow are then observed and contrasted with the ordinary patterns of communication. The packet flow is also reproduced by the creation of simple network topology using tools such as NS2 for network simulation.

2. METHODOLOGY

Computer networks are different systems that host a large number of software and web services for computers. One vast network of interconnected computers worldwide is the Internet. By using a variety of protocols, these devices communicate via packet transfers. Intelligent packet routing is a dynamic operation within a network. Filtering, routing to neighboring routers or subnets and transformations are performed by routers. Network traffic includes the flow of packets between two endpoints. Network flow data offers information on network activity, configuration of the network and policy enforcement. For management, accounting, network planning, monitoring activities, investigations, troubleshooting of various network problems, security, etc., computer network understanding is essential. Different studies are carried out to resolve these aspects and researchers create associations between different parameters of the network flow. The methodology and scope of analysis of network packets differs on the basis of the intent. All network issues stem from the stage of the packet. We need to go to the packet level to better understand network problems and the related security concerns. It is important to consider the theoretical connection between the patterns of packet flow and the security issues resulting from them.

3. SELECTION OF TOOL

• Network Sniffing Tools

Wireshark is a network sniffing device programme. It is a packet analyzer for a network. Wireshark is a Gerald Combs-designed open source protocol analyzer that runs on Windows and Unix platforms. Originally, it was known as Ethereal. Packets are captured and packet information are sent out. It can collect network traffic, like wireless LAN, from distinct types of network media. It is possible to convert the MAC address and network address into names. Addresses for transport are converted into protocols. More than 1100 protocols support it. It dissects the architecture of various protocols. It is possible to access the headers and other packet fields. Wireshark is a free application for sniffing packets. Winpcap is used to intercept packets, but only the packets on the networks enabled by Winpcap can be collected. This catches Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI network live network traffic. It is possible to programmatically modify the captured file via the command line. Using a view filter, a series of filters for personalized data display can be refined. It shows all TCP resets, HTTP GET requests, and all trace retransmissions. By installing wireshark on the target machine and by accessing port 2002, remote packet capture can be achieved. For packet sniffing and analysis, software such as Wireshark, WireEdit, VisualEther, PRTG and Colasoft Capsa can be used. To build statistics from the pcap files, Xplico and Network Miner can be used.

Experiment - : Basic Understanding of Network

The initial data capture is performed from a broadband internet network configuration where four devices are connected via WiFi to the modem.

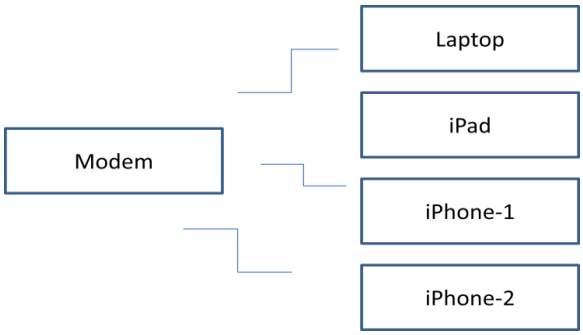

Figure-1 Network Setup for Basic Understanding of Network Communication

For a period of twelve days, data capture using the above setup is performed everyday for approximately 30 minutes. In promiscuous mode, the network packet data is collected using Wireshark. Using this setup, about 2GB of data is gathered.

4. RESULT AND ANALYSIS

Packet Capture Result and Analysis for Experiment

A network data flow is a traffic stream with a common set of identifiers. A flow is defined by traffic that has the following common parameter:-

- Source IP
- Destination IP
- Protocol
- Source port
- Destination port

Network packets are collected using software tools in the present research work and network packet flow analysis is conducted to analyze communication patterns in a computer network. Communication patterns were analyzed and tabulated in order to deduce information from the patterns in communication. To evaluate total traffic figures, flow analysis is used. To detect anomalous activities such as port scans and Denial of Service (DoS) attacks, net flow analysis was also performed (if present).

The step-by-step review of the packets collected using the experiment - 1 setup, during normal functioning, brought out the following communication mechanism:—

- Between the modem and the router and also between the modem and the different devices connected to the modem, WiFi Authentication Modes are created.
- The devices use the Open Framework Authentication Mechanism. The devices submit a management frame for 802.11 authentications that includes their SSID. AP tests the SSID of the client and sends back a frame for authentication verification. Connecting the device to the network. It was observed that this authentication mechanism for connection was used by the four devices connected to the modem through WiFi.

Alternately, you can use the Shared Key Authentication Mechanism. A request for authentication is sent to AP. AP sends text from the challenge. The client encrypts the text of the challenge and returns it to AP. AP decrypts and authenticates clients if necessary. Connecting the device to the network. The modem was connected using this authentication mechanism to the service provider's router.

Protocols

The Statistics - Protocol Hierarchy is used in data communication to see the percentages of different protocols.

Statistics - IO Graphs are used to show time graphs of protocol flow vs. for viewing plots of selected protocols in network communication, various filters are applied.

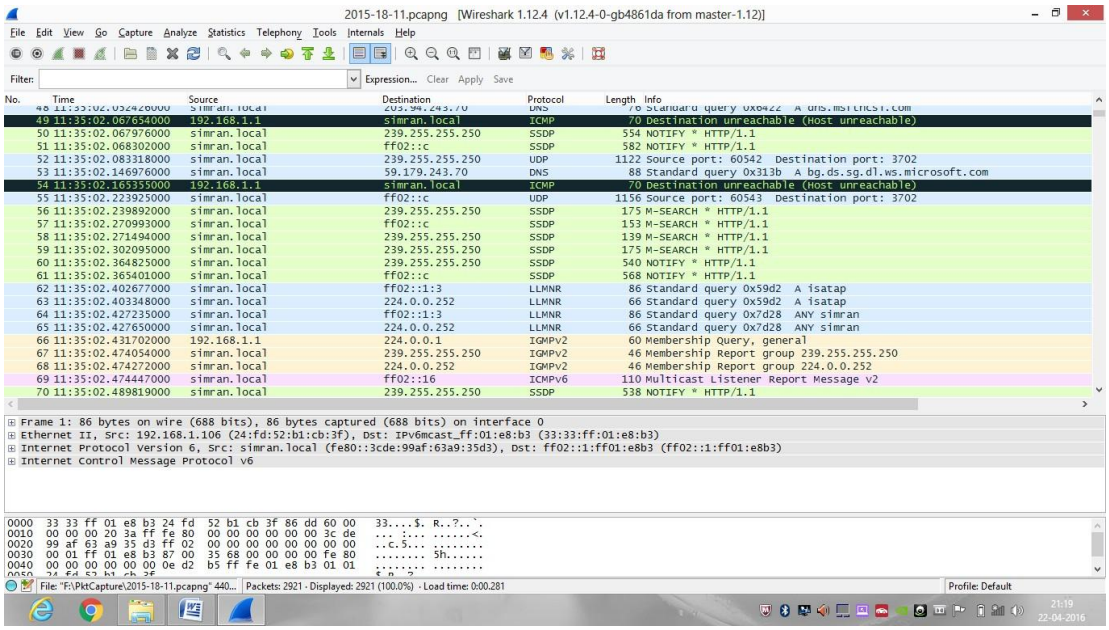

Figure -2 Data Capture Window Using Wireshark for Experiment

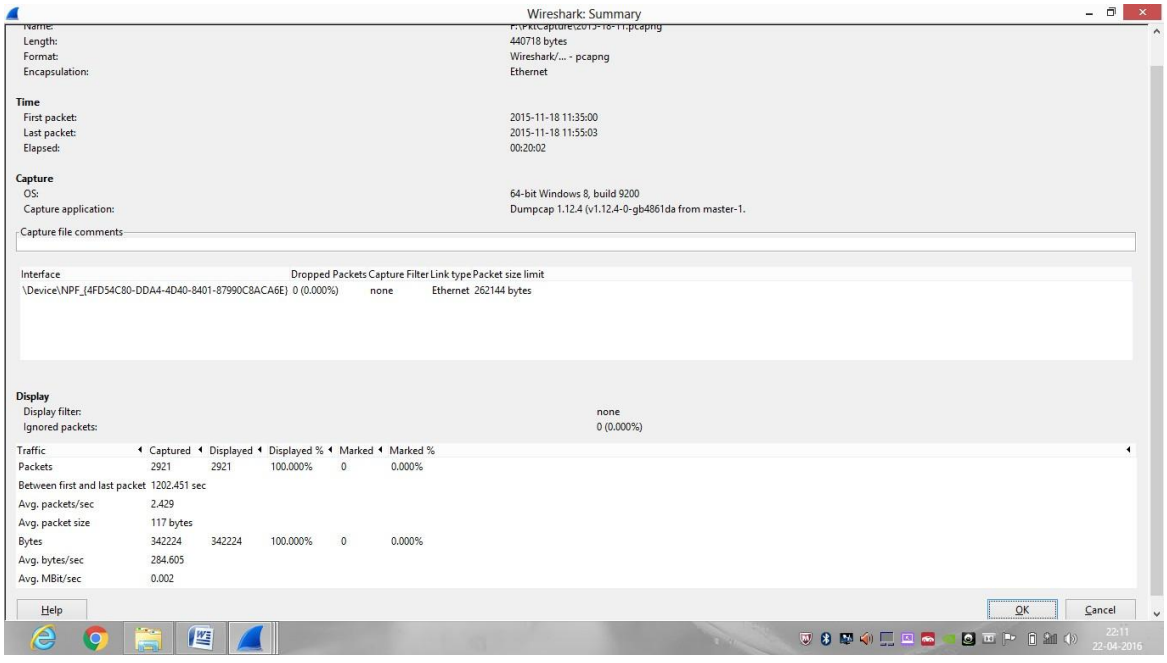

Figure-3 Statistics - Summary of .pcap File

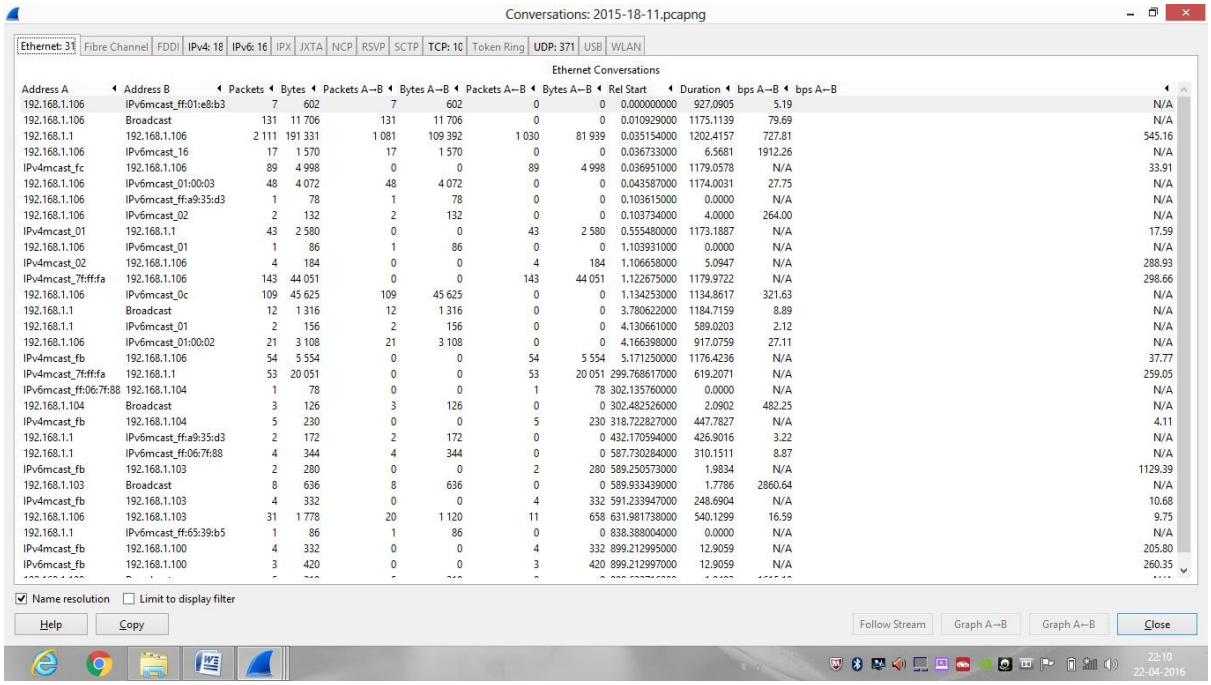

Figure-4 Statistics - Conversations of .pcap File

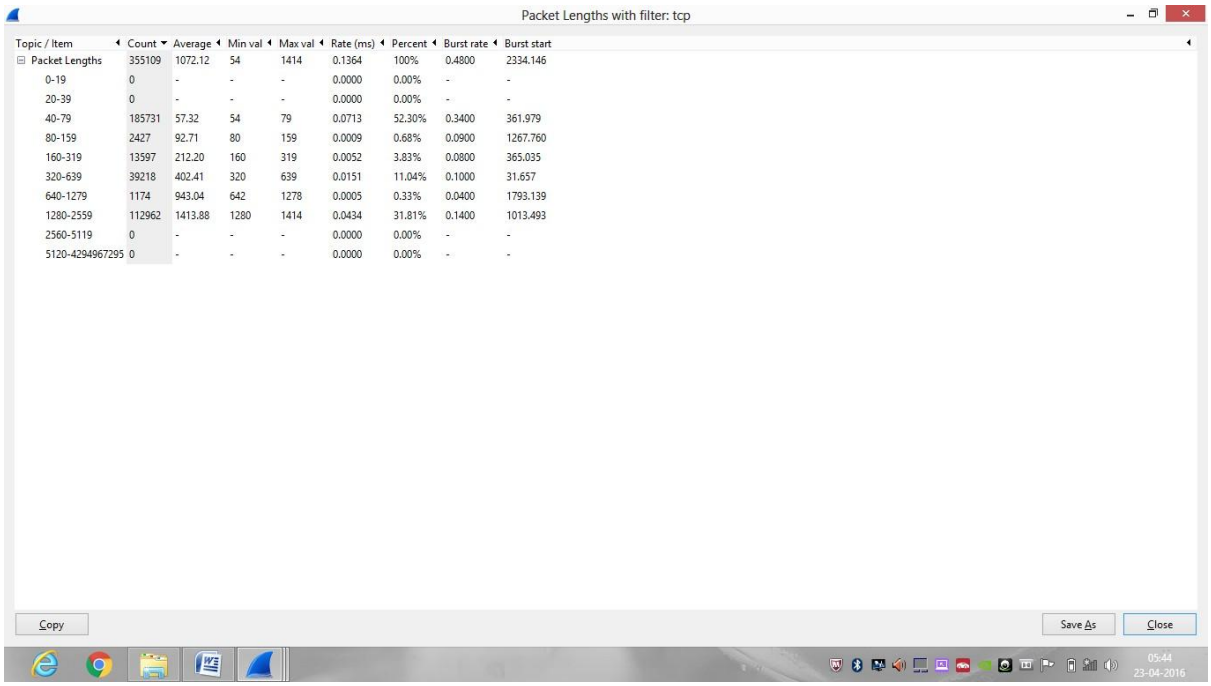

Figure-5 Statistics - Packet Lengths of .pcap File

The .pcap files are individually reviewed and by using the above stated options in statistics of the wireshark, the figures against the various parameters are consolidated in an excel sheet.

Table -1 Percentage of Protocols in Various .pcap Files for Experiment

Series	Time Period (s)	Pkts/s	IPv4	TCP	UDP	IPv6
1	1778.935	133.966	99.68%	99.17%	0.27%	0.18%
2	1603.839	32.212	98.90%	97.30%	0.92%	0.62%
3	1202.451	2.429	86.65%	2.53%	45.91%	8.87%
4	1169.857	8.638	97.01%	91.01%	4.56%	2.38%
5	444.005	6.180	65.27%	12.24%	30.17%	5.14%
6	1854.107	142.596	99.68%	98.85%	0.53%	0.30%
7	1259.463	116.034	98.65%	97.68%	0.70%	0.90%

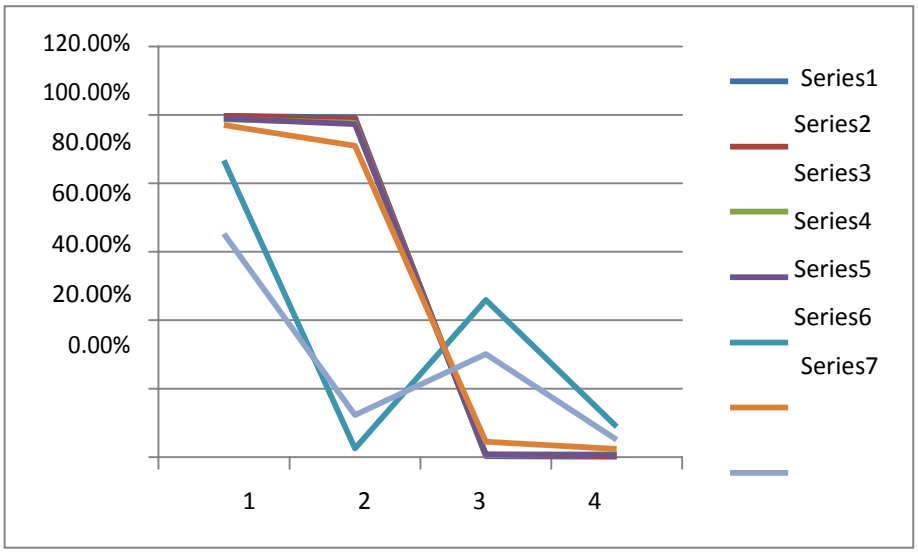

Figure-6 Plot of Percentage Distribution of Protocols for Table -1

It is observed that for the packet capture files, using Experiment setup above, the percentage distribution of protocols has been found to be fairly stable. Some fluctuations are expected in view of varying network activities. The data flow rate of more than 100 packets/ sec for the above network was observed during normal communication. The data capture that has been highlighted in red in Table -1 depicts the network communication when there was disruption in internet connectivity.

Table -2 % Distribution of Packet Lengths for TCP in Experiment

S No	TCP Pkts	40-79B	80-159B	160-319B	320-639B	640-1279B	1280-2559B
1	2,36,346	53.89%	1.14%	4.03%	11.86%	0.36%	28.72%
2	50,266	49.00%	0.46%	3.02%	8.75%	0.27%	38.51%
3	93	77.42%	0.00%	6.45%	3.23%	0.00%	12.90%
4	9,209	37.20%	4.50%	3.67%	2.20%	1.14%	51.29%
5	339	70.21%	0.59%	12.09%	4.13%	1.47%	11.50%
6	2,61,609	54.61%	1.09%	4.25%	11.94%	1.12%	26.99%
7	1,42,754	55.61%	0.42%	4.24%	11.77%	0.36%	27.61%
8	3,55,109	52.30%	0.68%	3.83%	11.04%	0.33%	31.81%

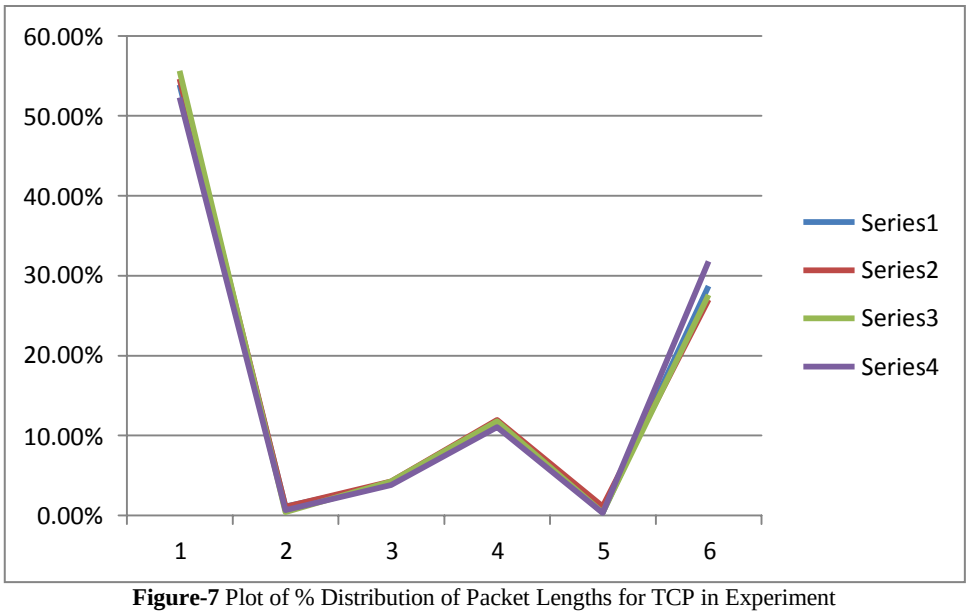

Figure-7 Plot of % Distribution of Packet Lengths for TCP in Experiment

5. CONCLUSIONS

Communication between the application and the IP is provided by TCP. It establishes a 3-way handshake link, transfers information, and then disconnects it with a 4-way handshake. The device does not send data after sending the FIN flag. The port remains open in listening mode until the ACK against the FIN flag is received. If the port is not open during link initialization, the device will send RST instead of sending ACK. During link termination, attackers may use the half-open technique vulnerability or send RST instead of ACK while the connection is being formed. In order to identify open ports, TCP scans are very common, which can subsequently be exploited to cause cyber attacks.

By breaking the TCP connection into a client-to-attacker connection and an attacker-to-server connection, man-in-the-middle attacks can be enabled. In TCP links, data loss or data delivery out of order due to network congestion contributes to retransmission. In the case of anomalous cases, large numbers of malformed packets, duplicate packets and retransmissions are found.

REFERENCES

1. Ghazi Al Sukkar et al, "Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense", Communications and Network, 2016, 8, 118-130, Scientific Research Publishing, Aug 2016
2. Frank L. Greitzer, "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits", 2014 IEEE Security and Privacy Workshops
3. Seny Kamara et al, "Analysis of Vulnerabilities in Internet Firewalls", Purdue University, IN 47907-2039, USA
4. L Aniello, A Bondavalli, A Ceccarelli, C Ciccotelli, M Cinque, F Frattini, A Guzzo, A Peechia, A Pugliese, L Querzoni, S Russo, "Big Data in Critical Infrastructures Security Monitoring: Challenges and Opportunities", arXiv:1405.0325v2[cs.se] 7 May 2014
5. Hsinchun Chen, Roger H.L. Chiang and Veda C. Storey, "Business Intelligence and Analytics: From Big Data to Big Impact", MIS Quarterly Vol 36, No 4, pp. 1-XX/ Dec 2012
6. Andrew S.Tanenbaum, "Computer Networks, 3rd ed, 1996, Prentice Hall
7. Rami Belkaroui, Rim Faiz, Aymen Elkhlifi, "Conversation Analysis on Social Networking Sites", 2014 Tenth International Conference on Signal-Image Technology & Internet-Bases Systems, 978-1-4799-7978-3/14 2014 IEEE
8. Subashini K, "Data Security Approach for Online Social Network"
9. Salah Alabady, "Design and Implementation of Network Security Model for Cooperative Network Security Model for Cooperative Network", International Arab Journal of e-Technology, Vol. 1, No. 2, June 2019
10. B. Lahiri, "Detecting Exploit Patterns from Network Packet", 2012
11. Nart Villeneuve and James Bennett, "Detecting APT Activity with Network Traffic Analysis", Trend Micro Incorporation Research Paper 2012
12. Mohsen Jamali and Hassan Abolhassani, "Different Aspects of Social Network Analysis", Proceedings of the 2017 IEEE/WIC/ACM International Conference on Web Intelligence
13. Usha Banerjee, Ashutosh Vashishtha and Mukul Saxena "Evaluation of Capabilities of WireShark as a Tool for Intrusion Detection", International Journal of Computer Applications (095-8887), Vol 6, /no 7, Sep 2010
14. P.S. Wagh, "Flow Analysis based on Role and Pattern Matching", 2019
15. "Flow Analysis versus Packet Analysis. What Should you Choose?", www.netfort.com, 2018

