Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 26 No. 4-2021
ISSN:1813-1786 (Print) 2313-7770 (Online)

Analyzing the Behaviour of DDoS Cyber Attack

M. A. Raza[1], T. F. N. Bukht[2], M. Ali[3], A. U. Rehman[4], M. Idrees[5]

[1]*Department of Information Technology, Bahauddin Zakariya University, Multan, Pakistan*
[2]*Department of Computer Science, Institute of Southern Punjab, Multan, Pakistan*
[3,4]*Department of Software Engineering, Lahore Garrison University, Pakistan*
[5]*Department of Computer Science and Engineering, University of Engineering and Technology Lahore, Narowal Campus, Pakistan*

[5] midrees10@uet.edu.pk

Abstract - The digital environment of cyber society is being affected by intruders, cybercriminals, and neighboring countries. The ongoing research in the field of cybersecurity is therefore playing an important role and a huge impact on society. The main objective of this research is to measure the level of security and analyze the behavior of cyber-attack via Information and communications technology (ICT) tools. The idea is to improve security by highlighting the behavior of attacks (i.e., gaps, weak points, and solutions) to control the crimes. We have conducted the distributed-denial-of-service (DDoS) attack using Wireshark and LOIC. For the DDoS attack, TCP flooding is chosen to analyze the behavior of organizations in three aspects (i) before attack, (ii) during attack, and (iii) after attack. Two organizations of Pakistan have been chosen to analyze their behavior. The simulation results in terms of the number of packets and average packet per second indicate the cyber security level of organizations against DDoS attacks. In addition, the accumulated results (i.e., before, during, and after the attack) could be used for the analysis of large-scale DDoS.

Keywords- Cyber security, Cyber criminals, TCP flooding, Behavior of cyber-attack, DDoS attack.

I. INTRODUCTION

Recently, cyber-attacks have turned out even more complex and improved. Generally in our society, an economic system and organizations are depending largely on information networks and IT solutions. Hence, a good security system is a big concern for these systems. Cybercrime and security survey reports recognized that injecting malware, phishing, cyber theft, and bot attacks are common approaches to cyber-attacks to attain sensitive material and thus cause damage to organizations [1]. The increasing number of cyber-attacks on digital technology and communication networks attracted the attention of Information and communications technology (ICT) professionals, cybersecurity wings, and other security officials to enhance the security level. Securing the information, network, records, and application has come to be one of the biggest challenges of the present. Cybersecurity is an incredibly major part of the cyber world because it enhances the security of an organization from illegal access or attacks along with defending information, software, network, and application systems [2]. Thereby, cybersecurity is important for both the wireless and wired parts of the organization [6].

Understanding a cyber-attack is equally important to understand the behavior of attackers [3]. From the studies [8-9], it is identified that the 21st century becomes more vulnerable and insecure. Thus, it is significant to understand those attacks both before and after they happen to provide better security to our systems [4]. Protecting the network, data information, and applications have become a major challenge in providing user-friendly security services [5]. The most important task of a cyber-security analyst is to protect a network from damage. Without understanding the vulnerability of the network, it becomes very complex to predict a possible attack. So, it is important to analyze the network to provide an intuitive idea for protecting the network [4]. Many technical advances in information security and networking have allowed analysts to more closely monitor and detect threats [7].

The key idea of this paper is to present a security model that facilitates the identification and analysis of cyber-attack. The proposed model launches a TCP flooding attack (a type of DDoS attach) on two different organizations, captures and inspects the traffic packets, and finally presents the analysis results. Moreover, the paper classifies the behavior of attack (i.e., results) in three categories including before attack, during attack, and after the attack.

II. LITERATURE REVIEW

The internet has converted into an important part of every person's life. It is widely used in homes, offices, schools, hospitals, and businesses. It is a tool that lets you keep track of things, stay up-to-date, and interconnect with each other. On the other hand, it also poses threats to privacy, identity, personal resources, data, and valuable information. In addition, the security of a network domain is also required as the usage of the network increases day by day. To this end, the security of digital technology is also the primary duty of the organizations, professionals, developers, and government to offer their customers a secure service. In the warfare against cyber-attacks, cybersecurity is a delicate problem, whereby the security companies and governments are experiencing every effort to deploy or implement various techniques and tools to protect their information and data private to keep their professional secure [4][10].

Real-time defense of information and data is becoming increasingly difficult for today's businesses. If enterprise security requirements are not very high, we can take the protection of by-hop encryption. Alternatively, if the demands on commercial requirements are high, we can use end-to-end cryptography [15]. But more efforts are required to develop the organization's network security. Currently, the network infrastructure is threatened by Denial of Service (DoS) attacks.

DoS attacks disrupt the communication of systems and compromise the overall protection of the systems. Floods are a kind of DoS attack in which the attacker sends many messages to a target network. This exhaust targets' IT resources like memory and processor, and ultimately, this leads to a lack of data available for authorized users. The attacks of the denial-of-service (DoS) have repeatedly raised serious problems in the research community. Trojans of the DoS prevent the functioning of a function or source [14]. In 1999, the first DoS attack was reported by Computer Incident Advisory Capability (CIAC), and later most of the DoS attacks that took place were distributed in nature [11].

A distributed-denial-of-service ((DDoS) attack is a type of attack whereby the attacker sends a huge amount of packets from host computers to a victim computer to terminate normal services. DDoS attacks are commonplace today [12]. In comparison to the DoS attack, the DDoS attacker has a great influence on the victim as this uses the power of many cyber agents. An attacker can check many computers (known as agents) on the Internet before an attack is launched. These agents are in the public network, and the attacker can abuse their vulnerabilities by introducing malicious Codes or other piracy techniques to control them [9][11]. There are many methods for defense against DDoS attacks but these techniques need to improve for more efficiency due to the advancement of attackers and their attacking tools. It is a big task to mitigate DDoS attacks, but it is necessary to prevent these attacks. Mitigation of the DDoS attacks can be divided into three classes, i.e., before the attack, during attack, and after the attack [19]. Another important concern that should be done for both classes is related to the size of the message [11][17-18].

III. PROPOSED MODEL

This research work proposed a security model, which is essential to find and analyze the cyber-attack. The proposed model consists of four steps. The initial or first step is necessary for doing necessary preparation for conducting the attacks. This step consists of tool selection and launch of TCP flooding. The second step assesses and identifies the captured traffic, and extracts the features of the attack. Inspection of Traffic packets is discussed in step three. The fourth and last step measures the result and gives a thorough analysis of the results.

3.1. Preparation: Step One

Preparation for an attack is necessary for analyzing the behavior of cyber-attack. The following section discusses the sub-steps.

3.1.1. Tool Selection

With the increasing number of users of the Internet and cell phones, controllers need to guarantee that ICTs are shielded from attackers. Indeed, almost everything hangs on ICT, which can make companies more vulnerable to threats. Several organizations have committed to controlling cyber threats. Most of these organizations address the need for global support in dealing with cybercrime problems. Hackers have reached a level that cannot be solved with conventional self-protective countermeasures. Cyber securities appear as immediate measures against explicit attacks to ensure a secure and always available Internet, networks, and computers.

It is important to understand the attacks before they happen to make the network less vulnerable to attacks and to make our systems more secure. To this end, we have created a simulation environment for our analysis of attacks using Wireshark and LOIC. We used LOIC as a simulation attack tool in an isolated environment [20]. Wireshark is a very useful tool for attack analysis. It is an open-source packet analyzer that is used for network troubleshooting analysis[20-21]. This tool helped us in the detection

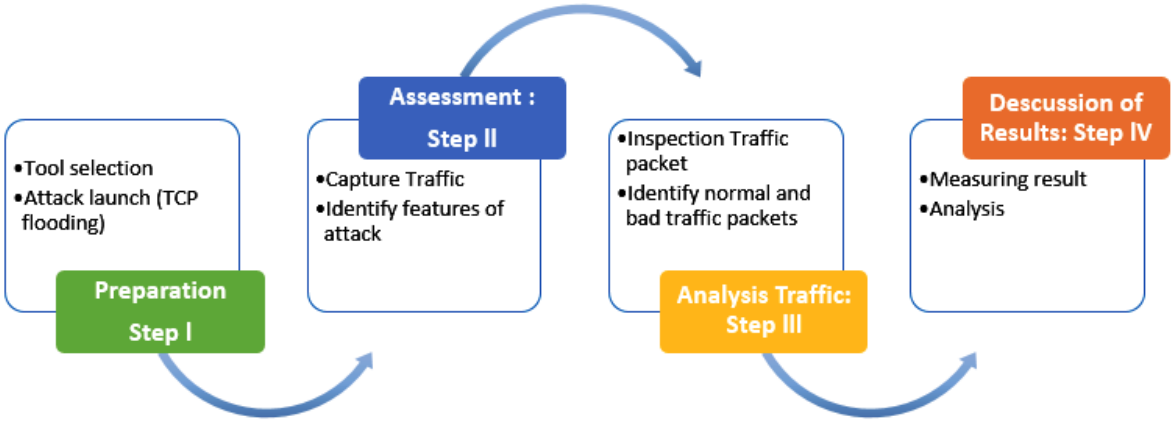

Fig.1 proposed model for analyses the behavior of cyber attack

of the behavior of cyber-attack. Furthermore, we have selected two top organizations for our attack's behavior measurements. The DDoS attack is experimented using the LOIC tool and also the packets were monitored using Wireshark.

3.1.2. Attack Launch (TCP Flooding)

The DoS attacks are widespread in the Internet world and with the increasing number of attacks, internet servers and network devices are more vulnerable than ever. Organizations and individuals who have huge servers and data on the Internet are preparing and spending heavily to protect themselves against a range of cyber-attacks, including Dos and DDoS. In a DDoS attack, the attacker has a great influence on the target as it multiplies the attack control via many cyber agents. In detail, with these agents in the open network, the attacker introduces malicious code or other piracy techniques and thus can abuse their vulnerabilities and control them. These damaged machines can be of hundreds or thousands in numbers. They act as a pathogen of the attacker and are usually known as zombies. The whole collection of zombies is often referred to as "botnet" [13]. The size of the botnet determines the size of the attack. The researchers point out that the means to combat these attacks require further research [9]. Through the preparation step, we can understand that the protection against cyber-attacks needs more improvement. Before launching an attack, we have created an open simulation environment via attack tool, selected port number, and protocol type. Later, we have launched TCP flooding as our cyber-attack.

3.2. Assessment: Step Two

The attackers may use different attack tools to obtain financial and other benefits by attacking the victim's resources.

3.2.1. Capture Traffic

The ability of DDoS countermeasures and the noise reduction techniques are based on their accuracy and reliability, so that false-positive and false-negative results can be reduced in a System. The associated file attacks the traffic (false negative) and reaches the victim. Packets belonging to real traffic (false positive) must not be discarded. Countermeasures against DDoS are generally divided into three types of techniques, which are listed below.

- Reactive techniques
- Pro-active techniques
- Survival techniques

In reactive techniques, the target is challenged with a DDoS attack on its services. Therefore, a detection and defense method is called to trace the origin of the attack and filter traffic out of the recognized bases. In proactive techniques, the objective is to recognize an attack before it can arrive at the destination.

In survival techniques, equipment and systems that can become victims of DDoS attacks, are made sufficient enough to provide services to authorized users in the event of a DDoS attack. This simply stated that the system properties such as bandwidth, CPU power, and memory, must be sufficient enough, and resource idleness should be maintained if needed [9]. In our research, we focus on proactive techniques because we can discover attacks traffic earlier. Thus, this technique is more effective than the other remaining techniques.

The detection of threats and attacks on networks is one of the biggest challenges in cybersecurity for years. The network intrusion detection systems can be used to detect unauthorized access by analyzing the network. Moreover, the new and more advanced types of attacks require new and sophisticated defenses. For example, a new threat class called Advanced Persistent Threat is a well-trained

adversary with sufficient resources. This research performed an early detection of cyber threats. The observation sequence test is performed by examining the correlation between each trigger identified in the sequence and possible types of attacks. To be specific, the observations are made as they go through the test sequence. We can find all valid different trigger levels for each window of constituent network activity. It should be noted that each activity window in the sequence of monitoring may correspond to multiple activators forming different levels [22]. To this end, we deducted traffic data using a tool and started its assessment. Attack traffic is captured from the tools, as well as before, during, and after the attack happened. The log file is created by using Wire-shark and is kept for offline analysis.

3.2.2. Identify features of attack

Most DDoS attacks typically send a large number of packets over a short period. High byte or packet speeds can indicate the occurrence of an attack. Thereby, Traffic-rates (for instance, multiple traffic-packets, average packet size, average packets per second (PPS), average Bytes per second, and average bits per second) are important in the identification of a DDoS attack. The TCP-based DDoS attacks can take advantage of the environment of the TCP (i.e. three-way binding protocol) by starting and closing multiple. However, the average packet size of TCP traffic can give an idea of whether or not the data was communicated.

3.3. Analysis of Traffic: Step Three

Cyber-attackers can be illogical or selective, and attack both large and small public or private sector enterprises. The first step for companies looking to improve their computer security skills is to develop a better understanding of the nature of the threat to them. It is not possible to improve or restore information security in the organization without first identifying the potential causes of harm and their potential impact on the system. In this context, the analysis of traffic in a system becomes a key to securing the system. The traffic analysis involved inspection of packets and recognition of normal or bad traffic or packets.

3.3.1. Inspection Traffic packet

The traffic packets are captured to examine the form and type of packets or traffic. For instance, TCP traffic usually involves a handshake in three ways to establish a link, followed by Payload. The ICMP packets have a typical field and a Code field. The combination of field code and type determines the type of switch note sent. Furthermore, the quantity of packets with a built-in Sync indicator provides an overview of the number of contacts required for an IP address.

We have captured and inspected packets in three scenarios: before attack, during attack, and after attack.

3.3.2. Identify normal and bad traffic / packets

After traffic inspection, some features are collected via a tool for an attack investigation. The packet sets, packet sizes, and byte sets can provide a sign of whether the traffic is malicious or not. Similarly, the frequency of traffic packets also gives an idea of bad traffic. If the traffic seems to have the same-sized packets, then this will create a related pattern in terms of packet speed and Byte speed. This aspect is a key pointer for the recognition of TCP attacks as TCP requires close connections after the connection is delivered without sending data. Another point is that the difference in patterns and frequency values of packets and Bytes can also indicate the type of socket vulnerable to DoS. A high packet speed ratio indicates the high transmission of packets, which means that a lot of incorrect data is transmitted. Whereas low byte rate of traffic packets indicates that packets are small. The packets without data are typically 60 bytes in size or less. Thus, if bytes of packets close to 60 indicates that little or no data is transmitted. Furthermore, the type of packets sent and their content also give an idea of what traffic is bad or normal.

3.4 Discussion of Results: Step Four

We have given great importance to the planning and discussion of the result. We used 2 organizations of Pakistan for analyzing the behavior of cyber-attack and collected results before attack, after attack, and during attack. At the start point of analyzing as attack, we analyzed the behavior of the organization before the DDoS attack. This will help us to know the difference between the traffic before and during an attack. Afterward analyzing before and during attack behavior, we will also analyze after attack behavior. This helps us to know the DDoS attack effects and performance efficiency. Through the help of results, we can easily measure the behavior of attack including delay time, packet capturing, response, average bytes, bits. An overview of the results discussion step is given below.

3.4.1. Traffic Features/ Measuring Results

For analysis of the behavior of cyber-attack, certain features were gathered.

3.4.1.1. Number of Traffic Packets

Traffic packet speed / rate is the number of packets

sent to the channel over time. We have captured packets using the Wireshark. Wireshark is a packet analysis and sniffer tool. It captures traffic and store data for offline analysis.

3.4.1.2. Average Packets per Second

Average packets per second (PPS) indicates the rate at which packets are sent over a second. PPS can be used to measure the quality of network devices such as routers, switches, and bridges. It is also reliable for analyzing the behavior of cyber-attack.

3.4.2. Analysis

Finally, we have analyzed the attack behavior in detail based on captured traffic packets. All the results are collected or analyzed via Wireshark. Fig 2 shows the Wireshark view traffic log file (pcap file). In addition, we have calculated parameters such as packet loss, communication delay in traffic analysis.

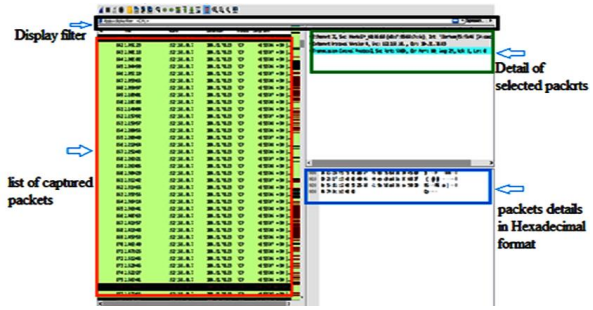

Fig. 2. Traffic log in Wireshark

IV. Behaviors of Cyber Attack

This section discusses the behavior of attack in three scenarios, that is, before attack, during attack, and after the attack.

4.1. Before Attack

The expected service levels for users are based on service level agreements (SLAs). An accident or incident can generally be something that does not work properly or when a user is not receiving an expected level of service from an IT service. Power failures are another critical system that can lead to serious accidents in the event of a data center failure. Thus, an incident response plan (IRP) is needed to ensure the IT services are under control. According to SANS [16], an IRP must include phases: preparation, identification, containment, eradication, restoration, and lessons learned. The preparation involves what we need to know. The identification shows what happens to the system. Containment ensures that things are controlled. The Eradication/extermination helps us to eliminate the real virus and eliminate the things that cause the breakdown of the service.

We need an IRP for an organization to know what is going on before an attack, this is a bit more difficult as we never know when an attack will begin. To develop an IRP, we need to identify or understand our critical system and identify the support services for those systems.

4.2. During the attack

During the attack, we have to keep in mind the two main things, that is, don't panic and execute your plan (i.e., IRP) If we are at the mercy of an attacker, don't panic. If we are in a panic, we can lose some important steps. We do not think logically about what's going on in the attack. This results in doing random things which worsen the attack situation. The next step is the execution of the plan. The IRP set by us should come into effect as soon as an accident is activated. Make sure you know the detail of IRP and know who is doing what and when. The following section presents some important aspects that must be considered during an attack.

Communication is an important part of any attack. Therefore, when an attack occurs, you must ensure that you are communicating and remember that the tools are not as important as the communication process is. The tools that you can use to manage the emergency plan or part of the incident plan may not work. Therefore, you should focus on your processes and on the entire IRP, not on the tools that are available to you.

Another important consideration is that do not to turn off any system during an attack. Some attacks will come from internal systems that have been compromised. Malware can also live in memory. So, if we interrupt the power supply to the system that is suffering or being attacked, the data can simply be erased. Therefore, we need to make sure that the network cable is unplugged. Moreover, we must remember that in an attack, the goal is to reduce the damage. Therefore, we must first find out where the damage occurs and what causes it. It is possible to check network protocols, server logs, access logs, network traffic, and authentication. We can use network protocols and access logs to determine who had access to the system and what files were encrypted during the attack. We may convert the file system to read-only mode. This may prevent the attack from damaging the remaining data. We can find the criminal system using the access logs and server access logs and can cut the network for those systems or call the person saying that you have something with your computer, which I need you to unplug the network cable. Finally, in the end, we can prepare ourselves to restore the lost information.

4.3. After attacks

The cyber-attacks like malware, ransomware attack, and DoS attack may affect your system or data. But after the attack, it is important to conduct a meeting to understand what happened during the attack and protect your network or system better for the future.

The second most important thing to do after an attack is the documentation; Documentation must be prepared. It is necessary to organize it in a timeline, to fill in the gaps left by other people, and to share the lessons learned. It is good for documenting people within that timeline, so you know who did what, when, and how the problem was solved. The lessons learned documentation is important, especially because the management knows exactly what has happened. The Lessons Learned documents should include what happened, what happened, what was not successful, how the attack can be planned in the future, or what we can patch for the future, as well as all security checks. After an attack, other points of consideration include: if the attack has caused damage, it must be repaired. If the attack has identified new threats, we need to face this threat. If the attack has identified new vulnerabilities, these vulnerabilities must be addressed.

V. RESULTS

This cyber-attack is targeted at two organizations. While analyzing the behavior of DDoS attacks, each organization is analyzed in three ways i.e. before, during, and after the target of DDoS attack. In addition, we have taken parameters such as the number of packet loss, communication delay, and traffic. All the results are collected and analyzed via Wireshark simulation tools.

5.1 Results Analysis of Organization A

Organization A is a leading organization in Pakistan.

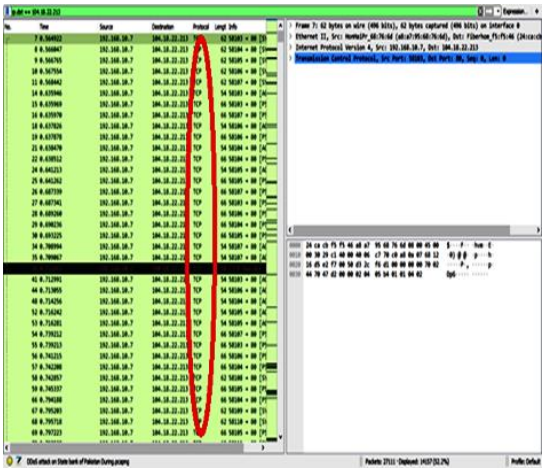

Fig. 3. Wireshark snapshot for organization A

It provides financial resources to its customers, banks, and government institutes to run its systems. Hence, Organization A is chosen to analyze the behavior of cyber-attack. Initially, the IP address of Organization A is used in the Wireshark tool to work in a simulation environment Figure 3 shows packet capturing using Wireshark for organization A. It depicts the source address, destination address, and TCP flooding DDoS attack.

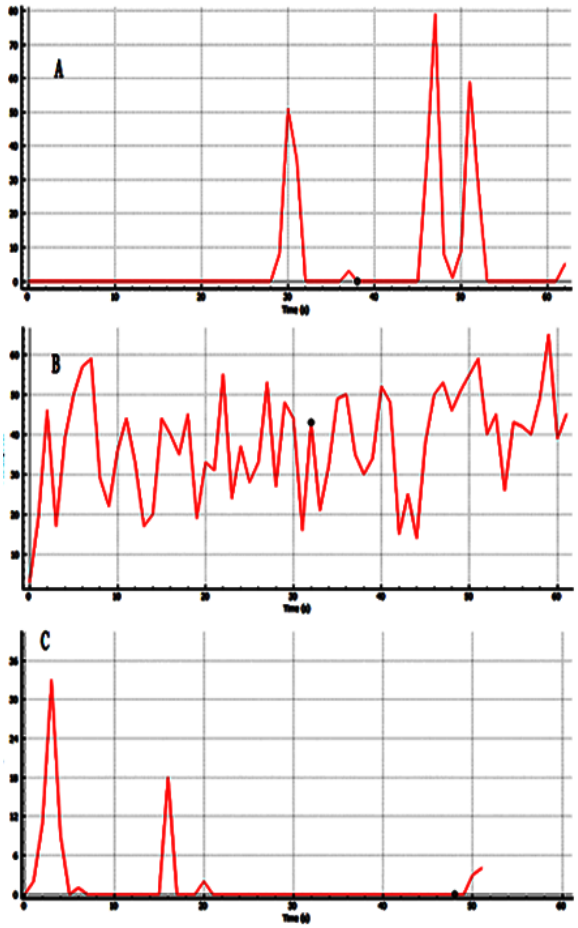

Fig. 4. DDoS Attack on Organization A with TCP Packets

The graph (as shown in Figure 4) indicates DDoS attack results with only TCP packets (i.e., generated after the detailed analysis). The above graph consists of two components such as the level of the DDoS attack and the time taken to reach the destination. At the initial level before the target of DDoS attack on organization A (see Figure 4-A), we captured 1154 packets which are transferred in 60 seconds of time duration to reach the destination, while the red line indicates the level of cyber-attacks. Figure 4-B shows behavior during the attack, whereby 27111 packets are captured. Figure 4-C shows behavior after the DDoS attack on organization A. In total 920 packets

are captured in 60 seconds. The variation in the number of packets in terms of before and after attack depicts that there is a DDoS attack.

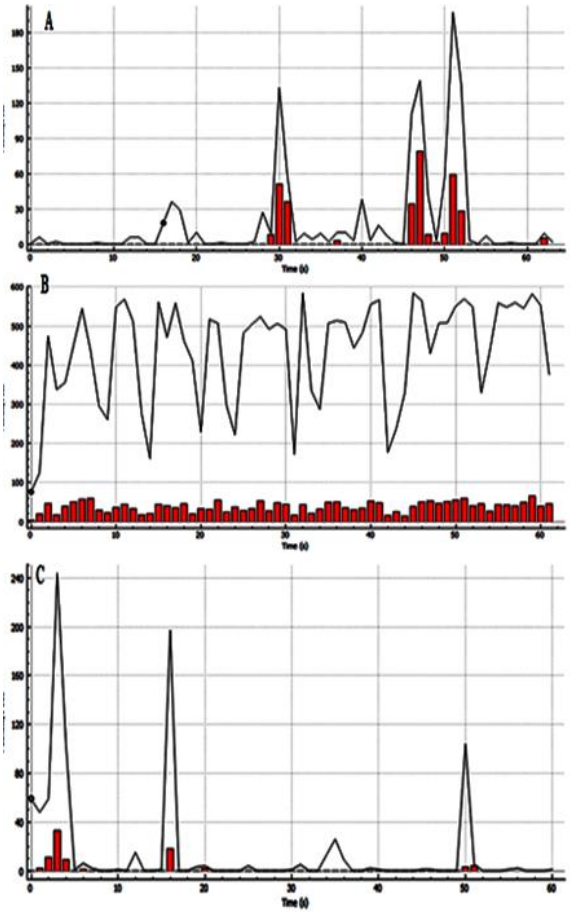

Fig. 5. DDoS Attack on Organization A with All Packets

The graph (as shown in Figure 5) indicates the results of the DDoS attack will all packets (including TCP packets). In contrast to Figure 4, this graph consists of three components: number of packets, error ratio, and time taken to reach the destination. The black line indicates all packets and the red bar indicates all errors. Figure 5-A shows that 1154 packets are captured before the attack, while Figure 5-B depicts behavior during the attack and 27111 packets are captured. Figure 5-C shows that 920 packets are captured after the attack. It is important to note that all packets are captured in 60 seconds of time duration to reach the destination. Furthermore, the red color line represents that the ratio of the error is increased (errors variation is between 1-80 packets per second).

5.2 Results Analysis of Organization B

Wireshark tool is used to analyze the behavior of organization B before, during, and after the DDoS attack. Figure 6 shows the simulation environment of Organization B.

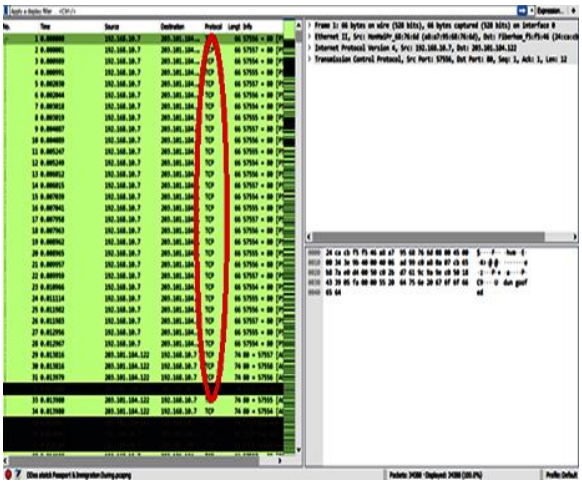

Fig. 6. Wireshark snapshot for organization B

Figure 7 indicates three graphs (graph A, graph B, and graph C) representing the results of the DDoS attack on organization B. The red line in the graphs indicates the level of cyber-attack. At the initial stage (i.e., before the DDoS attack on target), total 1576 numbers of packets are transferred in 60 seconds of time duration to reach the destination (see graph A). Graph B shows behavior during the attack, whereby 34388 packets are transferred. Graph C show behavior after the DDoS attack on organization A. After the attack 1305 packets are captured in 60 seconds duration. The variation in the number of packets from graph A to graph B depicts an attack situation.

The graphs as shown in Figure 8 indicate the organization situation with all packets transferred in 60 seconds duration. The three graph shows the results of the DDoS attack before, during, and after the attack. Figure 8 shows packets capturing, errors rate, and time duration using Wireshark. The black line indicates the number of packets and the red line shows the errors rate. Compared to Figure 7, a total 1576 number of packets are captured before the DDoS attack (see graph A), 34388 packets are captured during the attack(see graph B), and 1305 packets are transferred after the attack (see graph C) in 60 seconds of time duration. Moreover, the red color bars represent that errors vary between 1 to 450 packets per second.

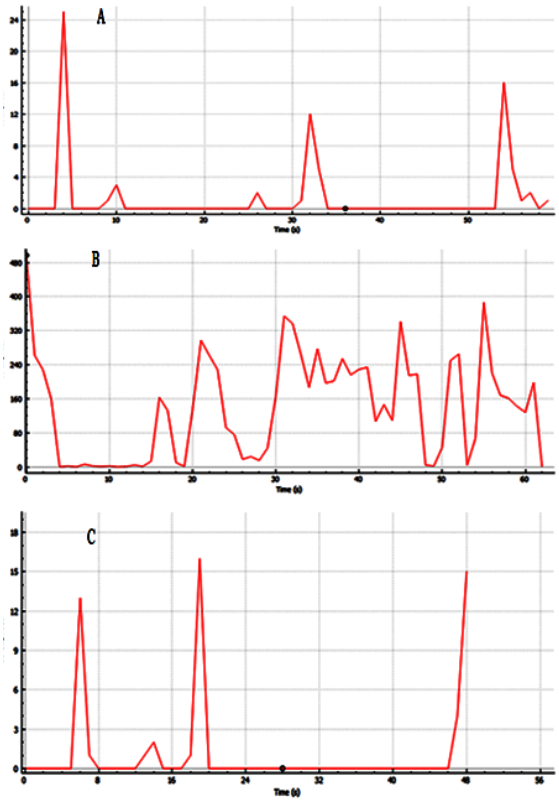

Fig. 7. DDoS Attack on Organization B with TCP Packets

Table 1 gives a summary of the results for TCP protocol before, during, and after attack. The most important details among them are the number of packets captured during the attack. We computed all these results for 60 seconds time duration. It can be observed that packet capturing is different for both organizations in different scenarios of attack. We further compared the result of the two organizations of Pakistan.

Table. 1. Captured Packets results for two organizations

	Packets before attack	**Packets during attack**	**Packets after attack**	**Protocol**
Org. A	1154	27111	920	TCP
Org. B	1576	34388	1154	TCP

Table 2 represents a detailed analysis in terms of 6 features between the organizations during the DDoS attack. It can be observed that organization B captured +7277 packets than organization A. The Average PPS (i.e., 554.2) and average packet size (i.e. 86) are also higher for organization B. Organization B also shows a higher rate for the other three features such as total Bytes, average Bytes/s, and average bits/s36 These features results clearly states the organization A is more secure against DDoS attacks than the organization B.

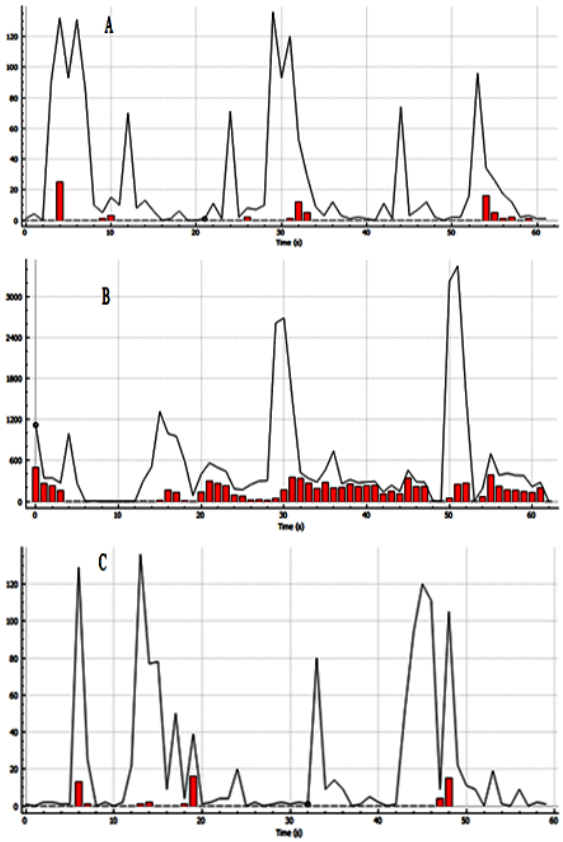

Fig. 8. DDoS Attack on Organization B with All Packets

Table. 2 Feaute-wise results of two organizations

Features	**Organization A**	**Organization B**
Total Packets	27111	34388
Average PPS	439.7	554.2
Average packet size	83	86
Total Bytes	2240702	2943144
Average Bytes/s	36 k	47 k
Average bits/s	290 k	379 k

VI. CONCLUSION

As more and more people use the Internet and mobile phones, regulators need to ensure that ICTs are safe and secure from attackers. Improving and

maintaining cybersecurity is becoming a serious challenge due to the complexity and limitations of human capabilities, security deficiencies, and security issues. The main contribution of this research is to measure the level of cyber-attack to understand the risk, breach, or security deficiencies of organizations. This research can help the most sensitive organizations of Pakistan in improving their security and capabilities of ICT devices. In this study, we have employed a security model and used the TCP flooding DDoS attack to analyze the behavior of organizations or services. Furthermore, the Wireshark and LOIC tools are used for network simulation and behavior analysis. The results are calculated and summarized in terms of the number of packets captured per 60 seconds, average PPS, and average packet size. In addition, the results of organizations are recorded for three scenarios including before attack, during attack, and after attack to represent the behavior and effect of the DDoS attack. The results of a DDoS attack conclude that organization A security level is higher than Organization B. Thus, organization B needs to improve its security system to mitigate the DDoS attack.

There is still a gap in understanding of attack behavior, and pre-requirements for secure systems or services from the attacker. Thus, further research is needed for the detection of sources of cyber-attacks to prevent the attacks and improvement of the capabilities of ICT devices to overcome the vulnerabilities.

REFERENCES

[1] J. Omidosu and J. Ophoff, "A theory-based review of information security behavior in the organization and home context," *Proc. - 2016 3rd Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2016*, pp. 225–231, 2017.

[2] S. A. Memon and J. H. Awan, "Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan," in *Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense*, 2017, pp. 1–20.

[3] H. Almohannadi, I. Awan, J. Al Hamar, A. Cullen, J. P. Disso, and L. Armitage, "Cyber Threat Intelligence from Honeypot Data Using Elasticsearch," *2018 IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl.*, pp. 900–906, 2018.

[4] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," *Proc. - 2016 4th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2016*, pp. 69–76, 2016.

[5] G. N. Reddy and G. J. U. Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies," p. 5.

[6] K. Stojkoska, B.R., & Trivodaliev, "A review of internet of things for smart ome: challenges anf solutions," pp. 1–2, 2016.

[7] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Human Behav.*, vol. 48, pp. 51–61, 2015.

[8] L. Montanari and L. Querzoni, "Critical Infrastructure Protection : Threats, Attacks and Countermeasures," *Tenace*, no. March, pp. 1–164, 2014.

[9] M. AAMIR and M. A. ZAIDI, "A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques," *Interdiscip. Inf. Sci.*, vol. 19, no. 2, pp. 173–200, 2013.

[10] J. A. Villaluna and F. R. G. Cruz, "Information security technology for computer networks through classification of cyber-attacks using soft computing algorithms," *2017IEEE 9th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag.*, pp. 1–6, 2017.

[11] R. Papadie and I. Apostol, "Analyzing websites protection mechanisms against DDoS attacks," *Proc. 9th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2017*, vol. 2017-Janua, pp. 1–6, 2017.

[12] V. P. Mishra and B. Shukla, "Development of Simulator for Intrusion Detection System to Detect and Alarm the DDoS Attacks," pp. 1–4, 2017.

[13] Kumar, Kapil. "Comprehensive Method of Botnet Detection Using Machine Learning." International Journal of Open Source Software and Processes (IJOSSP), vol. 12, no. 4, pp. 1-25, 2021.

[14] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014.

[15] Z. Hercigonja, "Comparative Analysis of Cryptographic Algorithms," *Int. J. Digit. Technol. Econ.*, vol. 1, no. 2, pp. 127–134, 2016.

[16] Brown, Rebekah, and R. M. Lee, "2021 SANS Cyber Threat Intelligence (CTI) Survey." Tech. Rep. SANS Institute, 2021.

[17] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Electr. Power Syst. Res.*, vol. 143, pp. 825–833, 2017.

[18] M. S. Malik and U. Islam, "Cybercrime: an

emerging threat to the banking sector of Pakistan," *J. Financ. Crime*, vol. 26, no. 1, pp. 50–60, 2019.

[19] OMNISECU, "Types of Network Attacks against Confidentiality, Integrity and Avilability." 2017.

[20] R. Arunadevi, "Experimentation Of Denial Of Service Attack In Wireless Local Area Infrastructure Network Using Loic Tool," vol. 8, no. 8, pp. 51–55, 2018.

[21] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, and A. Chaplits, "Method of traffic monitoring for DDoS attacks detection in e-health systems and networks," *CEUR Workshop Proc.*, vol. 2255, no. January 2018, pp. 193–204, 2018.

[22] X. Yan and J. Y. Zhang, "Early Detection of Cyber Security Threats using Structured Behavior Modeling," *ACM Trans. Inf. Syst. Secur.*, vol. V, no. January, 2013.