ATTACKS ANALYSIS OF TCP AND UDP OF UNSW-NB15 DATASET

ASGHAR ALI SHAH¹, YASER DANIAL KHAN², MUHAMMAD ADEEL ASHRAF²

¹Department of Computer Sciences, Bahria University Lahore Campus

²Department of Computer Sciences, University of Management and Technology, Lahore, Pakistan
sgharali.bulc@bahria.edu.pk

Abstract: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the most important protocols in complete protocol architecture. There are many types of attacks that can block the communication or reduce the performance of a protocol. This study provides a detail analysis of TCP and UDP attacks and their application layer protocols. The authors will also suggest that where the security administrator should focus for providing best security. The old datasets such as KDD99 and NSLKDD has many limitations. This study uses UNSW-NB15 dataset which has recently been generated.

Keywords: TCP, UDP, UNSW-NB15 dataset, Analysis

1. Introduction. A device can never communicate over the internet without protocol architecture. Complete protocol architecture has all the necessary protocol for communication. There are layers in protocol architecture and each layer many protocols. A protocol is used to make a communication both possible and efficient. Transport layer is used to provide process to process communication and many other services such as segmentation and reassembly, port addressing, flow control, error control, congestion control and many more services. There are two main protocols used in transport layer and perform all the functions of transport layer. These protocols are TCP and UDP [1].

TCP is a secure protocol. It performs three way hand shake. It provides a reliable communication to the upper layer. It has a good system of acknowledgement. Despite its many benefits this protocol is complex and slow. On the other hand if we talk about UDP which is not reliable but simple and fast. UDP is a best effort delivery protocol.

It is very clear that attacks are everywhere and anytime in internet. Attacks are always on services provided on the internet. Attacks can be associated to any protocol. This study mainly focuses on the attacks on TCP and UDP which are mostly used protocols. Researchers have worked a lot on KDD99 and NSLKDD dataset. NSLKDD dataset is the improved version of KDD99 [2]. These are older datasets and do not give us satisfactory results [3]. UNSW-NB15 [4] is a complex and recently generated dataset. It is a comprehensive dataset. It is for Network Intrusion Detection System (NIDS) [5]. It has nine types of attacks. This study will analyze all these attacks for TCP and UDP. This study will also analyze attacks for application layer protocols associated with UDP and TCP.

2. Attack Types. UNSW-NB15 dataset has nine types of attacks [3, 5]. This section will discuss these all nine types of attack and then will analyze it for different types of protocols. The older dataset analysis with 4 to 5 types of attacks are also discussed in [6].

- **Denial of services:** It is an intrusion. It disrupts the resources to make it unavailable to users on the internet. It keeps the device extremely busy that even the authorized user will have no access.
- **Exploits:** The attacker has previous knowledge of the system or network and exploits the vulnerability.
- **Reconnaissance:** It is an attack which gets information of the system to get a control of the system.
- **Worm:** It replicates itself with authentic users' information and get into the system. Spread itself and get access of the system.
- **Fuzzers:** This attack tries to acquire about security loopholes. It input a huge random data to crash the system.
- **Analysis:** This intrusion gets into a system through a web application through an open port.
- **Backdoors:** This type of attack bypasses the security mechanism of a system and gets access to system or data.
- **Shellcode:** The attacker sends a small piece of code. It run in shell and get a control of a system.
- **Generic:** This is an attack on all kind of block ciphers.

3. Analysis of Protocols and attacks. UDP and TCP are both important protocols. There are many attacks on it. Table I shows that the total attacks on TCP is 58184 and UDP is 223750. UDP got high number of attacks then TCP.

TABLE I. COMPARISON OF ALL ENTRIES AND ALL ATTACKS

P r o t o c o l s	All Entries related to TCP and UDP	
	All Entries	All Attacks
T C P	1495074	990435
U D P	58184	223750

Figure 1 show the relationship of TCP and UDP. If we look at figure 1 it show clearly that the TCP has more entries than UDP but attacks rate of UDP is higher than TCP. It seems that TCP is a secure protocol because it has less attacks.

Figure-1: Comparison of All Entries and ALL Attacks

This section will discuss TCP in detail. Table 2 has 9 types of attacks. These nine types of attacks are discussed in attack types. Table 2 indicate entries of all these nine attacks. If we look at the table the most accruing attack is Exploit and the less accruing attack is worms.

TABLE 2. DIFFERENT TYPES OF ATTACKS ON TCP

TCP Attack Types	Entries for each type of Attacks
Exploits	27443
Reconnaissance	6965
DoS	3336
Generic	3118
Analysis	622
Worms	153
Shellcode	750
Backdoor	323
Fuzzers	15473

Diagrammatic representation of all types of attacks are displayed in Figure 2. In this figure it is clearly shown that Exploit attack has occurred the most and Worms attack has occurred the least.

Figure-2: Comparison of all TCP Attacks

Table 3 shows us all types of attacks occurred in UDP. UDP case is different from TCP. It can be clearly seen that generic attack has occurred the most. Analysis attack has not happened at all.

TABLE 3. DIFFERENT TYPES OF ATTACKS ON UDP

UDP Attack Types	Entries for each type of Attacks
Exploits	874
Reconnaissance	4890
DoS	527
Generic	210600

UDP Attack Types	Entries for each type of Attacks
Analysis	0
Worms	21
Shellcode	761
Backdoor	34
Fuzzers	6043

Table 3 has diagrammatically shown in figure 3. It can be clearly seen in the figure that generic attack is a big threat for UDP.

Figure-3:. Comparison of all UDP Attacks

The numbers of all types of attacks for TCP and UDP is written in the table 4. Exploit and Fuzzers have high entries while Generic has very high entries in UDP.

TABLE 4. COMPARISON OF ALL TCP AND UDP FOR EACH TYPE OF ATTACK

Types of Attacks	Comparison of TCP and UDP	
	TCP	UDP
Exploits	27 44 3	8 7 4
Reconnaissance	69 65	4 8 9 0
DoS	33 36	5 2 7
Generic	31 18	2 1 0

Types of Attacks	Comparison of TCP and UDP	
	TCP	UDP
		600
Analyses	622	0
Worms	153	21
Shellcode	750	761
Backdoor	323	34
Fuzzers	15473	6043

Figure-4:. Comparison of UDP and TCP Attacks

The application layer applications and associated transport layer protocol and its associated attacks are written in table 5.

TABLE 5. APPLICATIONS AND THEIR ATTACKS

Applications	No. of Application layer attacks for TCP and UDP
--------------	--

	T C P	U D P
DNS	65	210566
DHCP	0	172
HTTP	18847	0
FTP	4905	0
POP3	1529	0
SMTP	4989	0
SSH	19	0
SSL	142	0
Radius	0	30
SNMP	0	112

Figure-5:. Applications and their Attacks

Classifiers of Intrusion Detection System still have many drawbacks [7]. Therefore it is not good to only rely on IDS. IDS can never give complete security [8]. The attackers perform malicious activities and disorder the system management [9]. The network administrator must think about alternative ways.

All those applications that communicate over a network must use a port number. It means that at transport layer they use TCP or UDP. Transport layer provides port addresses to the application layer. It means that the assigned port address is an opening to the system. The attackers try to find a weak point in the system or network [10, 11]. If we secure TCP and UDP which means securing transport layer and securing transport layer means securing applications and systems. Table IV and V illustrate all the attacks related to TCP and UDP. It also illustrates the attacks related to applications. This study tells you that what the focus area is for hackers. Most of the applications will use either TCP or UDP but there are some applications which use both TCP and UDP. The entries are on both sides for those applications which use both TCP and UDP. Entries are on one side for those applications which use one of them. For TCP protocols the high number of attacks are received for HTTP and on the UDP side there are high number of records on DNS. It is not only important to secure the system and network but the network administrator should protect each protocol by identifying the intruders. A good analysis of the attacks is very important for security implementers.

4. Conclusion. This study focuses on the latest dataset and analyzes it for different attacks related to transport layer protocols and application layer protocols. Potential threats for UDP, TCP and application layer protocols are specified. It is suggested that a potential threat should be identified and then the preventing maintenance should be provided. UDP has a high no. of Generic Attacks while TCP has a high no. of Exploits and Fuzzers attacks. HTTP using TCP has a high no. of attacks while DNS using UDP has a high no. of attacks.

REFERENCES

- [1] "Kumar, S., Rai, S., (2012), Survey on Transport Layer Protocols: TCP & UDP, International Journal of Computer Applications, 46, 7, 0975-8887
- [2] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on (pp. 1-6). IEEE.
- [3] Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective*, 25(1-3), 18-31.
- [4] UNSW-NB15 Dataset for Network Intrusion Detection System. Retrieved from <https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys>, 2018-03-12
- [5] Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *Military Communications and Information Systems Conference (MilCIS), 2015* (pp. 1-6). IEEE.
- [6] "Shah, Asghar Ali; Khiyal, Malik Sikander Hayat; Awan, Muhammad Daud; (2015)", Analysis of Machine learning Technique for Intrusion Detection System: A Review, *International Journal of Computer Applications*, 119, 3, 0975-8887.
- [7] Salem, M., & Buehler, U. (2012). Mining techniques in network security to enhance intrusion detection systems. *arXiv preprint arXiv:1212.2414*.
- [8] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, 378, 484-497.
- [9] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279.
- [10] Eom, J. H., Kim, N. U., Kim, S. H., & Chung, T. M. (2012, June). Cyber military strategy for cyberspace superiority in cyber warfare. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 295-299). IEEE.
- [11] Vatis, M. A. (2001). Cyber attacks during the war on terrorism: A predictive analysis. Dartmouth Coll Hanover Nh Inst For Security.