International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

Application of Network Forensics in Identification of Network Traffic

[1]Ajay Sehrawat, [2]Neha Shankar Das and [3]Praveen Mishra
[1]Software Engineer (IT), Regional Centre for Biotechnology,
[2]M.Tech, GGSIPU,
[3]Additional Director, ERNET India,

***Abstract* - With the development of the latest technology interventions in the field of networking, cyber- crimes are increasing at a gradual rate. It has led to increase in online crimes and attacks in which malicious packets are being sent to other hosts. Network Traffic Analysis comes under Network Forensics which is one of the classifications of Cyber Forensics that deals with capturing, recording, monitoring and analysis of network traffic. Keeping this in view, the paper describes the need of network forensics and its aspects. The paper proposes a model for network traffic analysis which is useful for detecting malicious packets received from intruders.**

Keywords: Network Forensics, Network Monitoring and Network Traffic Analysis

1.0. INTRODUCTION

Network attacks and cyber crimes are one of the most critical issues in today's era of ICT. These attacks are characterized by stealing authentic information by malicious hosts that continuously monitors websites Criminals make use of techniques like information hiding, network source trackback that can cause harm to security of system [**10**]. As these crimes cannot be removed completely only by improving technologies but it must cover legal issues and such malicious intruders must be punished.

The use of Network Traffic Analysis can also be seen in security domain. It includes management and monitoring of packets from source IP address to destination IP port number. It takes amount of packets sent in consideration to check flow of consistency in network. Network forensics is defined in [**11]** as "*capturing, monitoring and scrutiny of network events in order to determine the cause of security attacks and other problem incidents".* It can be said that Network Forensics is a branch of digital forensics which is studied to examine the network traffic so that attacks and malicious activities can be discovered. There is difference between computer forensics and digital forensics. Computer forensics deals with copying of files, removal and recovery of deleted files, buffer content access and system log analysis while Network forensics reduces risk of unwanted hosts and monitors track of packets sent on network.

The remaining paper is categorized as follows. Section II describes related work and research on network forensics and traffic analysis. Section III describes some techniques used in network forensics. It is followed by proposed model for the network traffic analysis. Section IV shows analysis of packets sent through different port numbers followed by conclusion and references.

2.0 LITERATURE REVIEW

The given table presents the review of studies conducted in the context of network forensics.

Table1: Review of studies conducted in context of network forensics

Authors	*Work on network forensics*
Amran et al [1]	This paper proposed a seven step model for the analysis of network flow of packets on Internet. The query is scanned in the model itself from corrupt query. It is then filtered using rephrases and techniques.
Ham et al [2]	This paper describes various challenges associated in network forensics like acquisition (gathering information about packets), content (what is hidden in them), storage (how much space does the packets take) and their admissibility.
Simon et al [3]	They proposed a two stage network forensics system. It captures large data packets and puts them on the server. Secondly, it analyzed each packet and saved its information for future uses.
Kim et al [4]	This paper identified the problems encountered while monitoring large network of packets. Correlation analysis is needed to monitor packets which make process intelligent.
M. Huang et al [5]	The paper describes the need to preserve all network information by addition of the information behavior coordinates and performing real time analysis. It also presents applications of data packets used in forensics.
Redmonet al [6]	It introduced a network security technique named as Honeypot, which uses deception technique. It is a trap that monitors packets accessed by hackers in real time environment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

Pilli et al [7]	They devised a generic framework for investigation of network forensics. Their model consists of 8 phases viz. preparation, detection, collection, preservation, examination, analysis, investigation and maintenance. Every phase is described precisely. Preparation phase deals with network sensors detection system that needs to be put on servers to stop unwanted attacks. Detection phase will generate alert in case of violation. Collection phase deals with changing of data on the network. Preservation phase maintains a copy of original data for back up support. It is followed by Analysis and Investigation phase.

3.0 PROPOSED MODEL

A network traffic analysis model has been proposed that employs use of machine learning techniques in its phases. It has a number of phases as stated below:-

Collection of data

Data means packets (large number of random packets sent on various servers). Now, these packets are being collected by using server devices like Firewall, Hypervisors. These are placed between main server and receiver so that it gets noticeable in case of any data attack.

Categorization of data

The data collected in the above step is now classified into different packets on the basis of their size and content of information. It involves techniques like deep packet inspection and port based learning. [8]

Clustering

Classified data is now clustered in order to separate them on the basis of common feature values. Clusters are defined on the basis of data mining algorithms like Naïve Bayes, KNN Algorithm. It will determine them in statistical manner. [9]

Detection

This phase will detect clusters that have been identified as harmful after going through clustering and classification phase. It will lead to creation of log files to ensure different clusters formed through machine learning. After the log file is created, it can be updated time to time.

Analysis

This phase presents report of packets that have been analyzed on the basis of clusters. It requires usage of Capsa tool that is discussed in the next section. It classifies and analyses packets on different ports.

Documentation

The report is made which contains information about clusters henceforth.

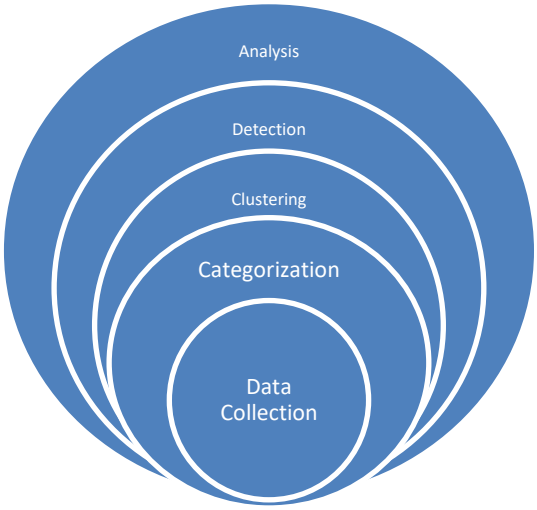

Fig1: Steps in proposed model

4.0 IMPLEMENTATION & SCENARIO

This section demonstrates classification of different network packets at different ports using real time network application Capsa Tool. ColasoftCapsa is a "real-time" portable network analysis application for both LAN and WLAN [12]. It is one of the tools used for monitoring of network traffic by identifying malicious hosts and estimate performance level of data in particular layer.

Figure 2 and 3 depicts distribution of network packets on different TCP ports and UDP ports. The malicious packets will be identified this tool and they are blocked automatically using senor device fitted in proposed model. There are various ports associated with identification of network like MAIL, TCP, UDP, POP3 and many more. The demonstration of packets via TCP and UDP is shown in figures. The traffic monitor window is shown in figure 4 that depicts identification and flow of packets via TCP layer. *The values shown in graphs are in bytes which denote receiving bytes as y axis and sending bytes as x axis respectively.*

The tool takes IP address or any website URL as input. It automatically detects malicious packets from address and starts its diagnosis. In Fig 4, flow of packets in TCP layer is diagnosed and network monitoring is done after 5 successful attempts. The tool gives a prompt message as it detects malicious packets. So, after 5 attempts, it lists IP and Mac addresses of valid packets by filtering malicious packets from it. In fig 2, it is seen that in last value 29450 packets have been sent but received bytes lies between 0-2236 which is less as compared to traffic. It leads to downfall in traffic flow due to bad packets in network. The graphs are taken after 3 attempts so that unevenness can be seen due to bad packets.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

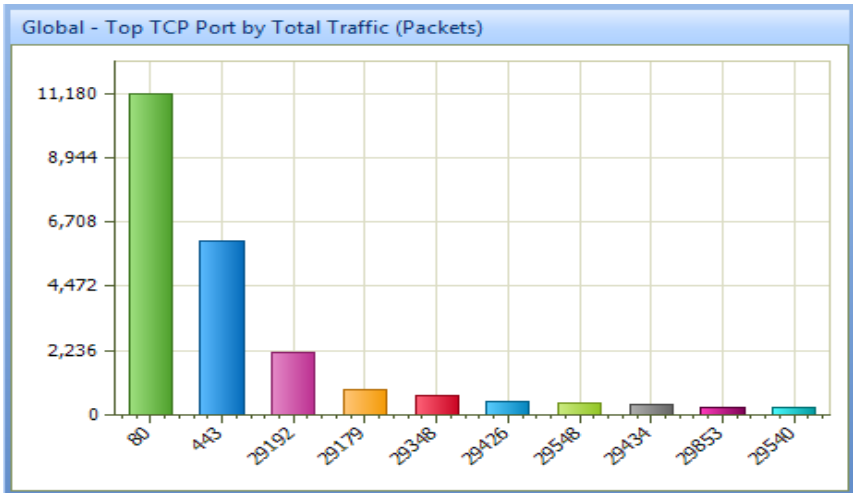

Fig 2: TCP ports distribution (x axis – sending bytes, y axis- receiving bytes)

Similarly, packets distribution can be seen at UDP layer as shown in fig 3.

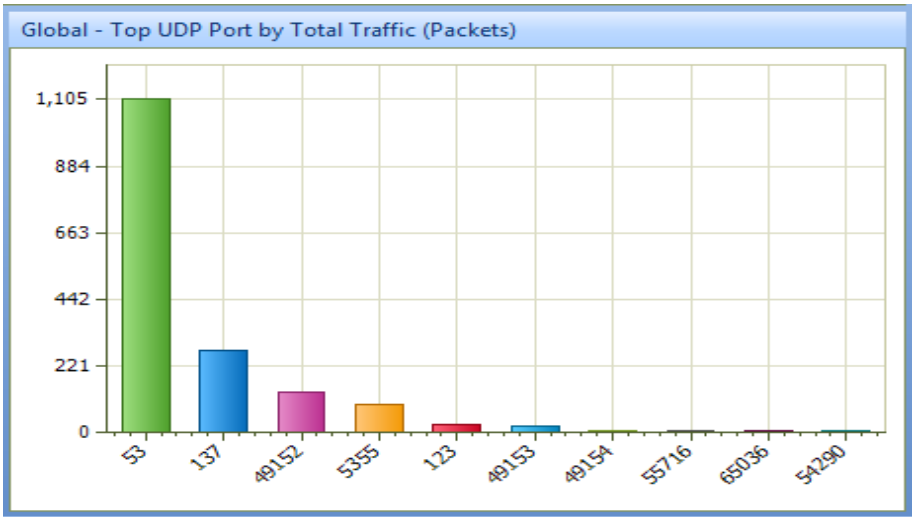

Fig3: UDP ports classification

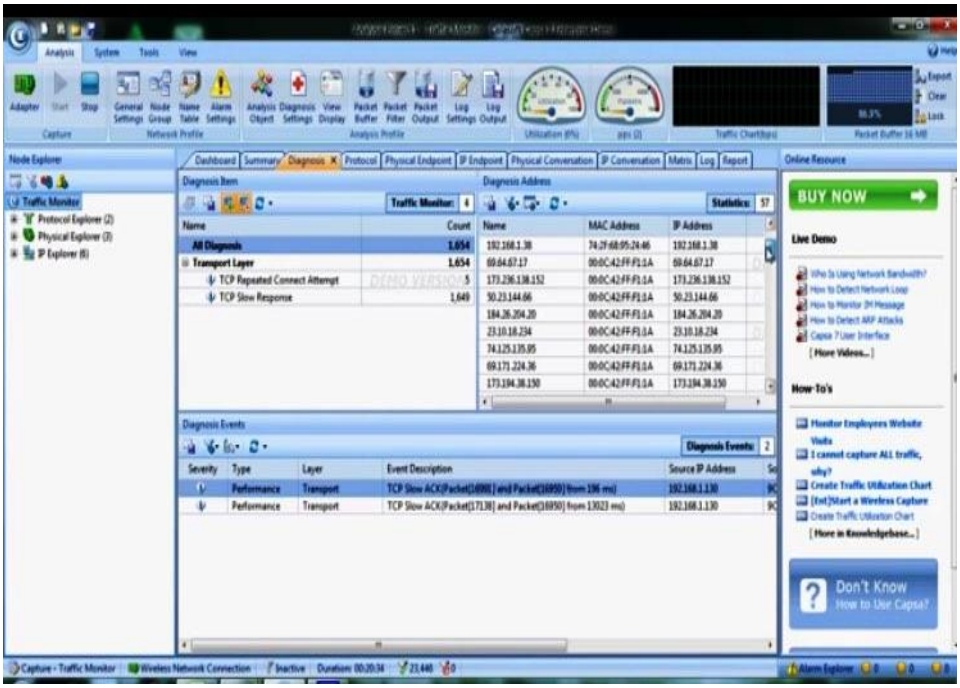

Fig4: Network performance in TCP layer

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

5.0 CONCLUSION

This paper describes proposed model of network traffic analysis by considering various factors and studies conducted in the context of digital forensics. Network traffic is divided into various clusters and their analysis is done in real time network application to detect malware packets. This paper also makes readers aware about the various network intrusion detection techniques that form the basis of the theory. The model can be extended in cloud based environment using virtualization and ontological based features.

REFERENCES

[1] Amran, A. R., &Saad, A. (2014, January). An evidential network forensics analysis model with adversarial capability and layering. In *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on* (pp. 1-9). IEEE.

[2] Davidoff, S., & Ham, J. (2012). *Network forensics: tracking hackers through cyberspace* (Vol. 2014). Upper Saddle River: Prentice hall.

[3] Garfinkel, S. (2002). Network forensics: Tapping the internet. *IEEE Internet Computing*, *6*, 60-66.

[4] Kim, J. S., Kim, M., & Noh, B. N. (2004, May). A fuzzy expert system for network forensics.In *International Conference on Computational Science and Its Applications* (pp. 175-182).Springer, Berlin, Heidelberg.

[5] Huang, M. Y., Jasper, R. J., & Wicks, T. M. (1999). A large scale distributed intrusion detection framework based on attack strategy analysis. *Computer Networks*, *31*(23-24), 2465-2475.

[6] Redmon, B. J. Maintaining forensic evidence for law enforcement agencies from a federation of decoy networks. *MitretekSystems, Fall 2002*.

[7] Pilli, E. S., Joshi, R. C., &Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *digital investigation*, *7*(1-2), 14-27.

[8] Zhang, L., & White, G. B. (2007, March). An approach to detect executable content for anomaly based network intrusion detection. In *Parallel and Distributed Processing Symposium, 2007.IPDPS 2007. IEEE International* (pp. 1-8). IEEE.

[9] Erman, J., Mahanti, A., &Arlitt, M. (2006, November). Qrp05-4: Internet traffic identification using machine learning. In *Global Telecommunications Conference, 2006.GLOBECOM'06. IEEE* (pp. 1-6). IEEE.

[10] Dixon, P. D. (2005). An overview of computer forensics. *IEEE Potentials*, *24*(5), 7-10.

[11] Ranum, M. (2008). Network flight recorder. *Inc. Intrusion Detection: Challenges and Myths*, 11-16, Jan 2008.

[12] ColasoftCapsa Download Link of Free Version http://www.colasoft.com/download/products/download_capsa.php?c=b