Application of SNORT and Wireshark in Network Traffic Analysis

G Jain¹, Anubha²
¹,² Computer Science Department, Swami Vivekanand Subharti University, Meerut, UP, India
¹jaingarima2011@gmail.com

Abstract. Now a days, our life is totally dependent on internet which in turn leads to different kind of intrusion. In order to detect intrusion, detection tool is needed so as to detect any kind of intrusion without user involvement. Intrusion detection system is a process of analyzing intrusion so as to provide secured data transmission in networking. One of the most used tools in analyzing packets is Wireshark. Nevertheless, Wireshark is less effective in detecting the intrusion still it can be used to intercept and detect network encrypted traffic which will analyze the captured traffic. Wireshark helps in identifying number of attacks like DoS, DDOS etc. SNORT take all live packets from internet and captured the live packets with predefined rules and if matches didn’t find then directs alert messages to the user. In this method, router is used to access internet so as to get precise flow of data packets. It generates a log file which entails all the live captured packets. The log file “Wi-Fi” generated by SNORT tool is then exported to Wireshark to examine the captured network packets. The Wireshark tool creates each detail about the packets of the recorded log file. In this paper, the I/O graph outlined the flow of the packet which demonstrations the total traffic which is further measured in either bytes or packets per second. TCP errors and delta time graph are shown.

Keywords. SNORT, Wireshark, NMAP, data packets, network traffic, packet analysis, DoS, DDoS.

1. Introduction
Network protection is one in all the most important demanding situations that organizations are going through from time to time. There are plenty of tries via way of means of the black hat hackers to interrupt and compromise with the safety of Company’s community and a number of them are even successful. As using net increasing, those malicious sports are gaining reputation many of the black hats. Everyday big quantity of records is being generated and exceeded on and plenty of those records holds touchy records approximately the organization and its employee. Thus, securing community is one of the maximum vital challenge for an organization to survive. To make this simpler and green we use Intrusion Detection System it allows to acquire records approximately any malicious packet that passes throughout an organization's community.

1.1. Intrusion Detection System
Intrusion detection system (IDS) is a sort of safety machine for computer systems and laptop networks. Intrusion Detection specifically enables in detecting outer and internal assaults done via way of means of both consumer and hackers. An IDS machine collects facts from numerous reasserts and analyzes facts from numerous regions inside a laptop or a community to be aware of viable safety breaches, which encompass each intrusion (assaults from outdoor the organization) and misuse (assaults from in the
organization). IDS make use of vulnerability assessment (also known as scanning), to evaluate the safety of a laptop machine or community.

1.1.1 Prons of IDS
- Trace any changes made within the network.
- Audits system activity
- Normal and abnormal activities can be distinguished in the network

1.1.2 Cons of IDS.
- At times provides false alarms i.e., IDS might produce alert message even though packet is not malicious the packet wasn't malicious.
- Takes a lot time in time consuming
- Is not 100% harmless from attack.

1.2. SNORT
Snort as NIDS is an open-source network intrusion and sensing program (IDS / IPS). Snort is the mostly used as IDS / IPS technology in the world and brings collectively the benefits of protocols, signatures, and specifications based on exceptions. This tool is a IDPS (Intrusion Detection and Prevention System) which uses a sequence of rules/policies that aid to outline or describe malicious network activity and make use of those rules/policies to discover packets that didn’t match and creates alerts for users. User has written these rules/policies in a text file which is associated with snort.conf file where all the snort configurations are stated. To get SNORT running, few commands are these so that it can examine network behaviour.

1.3. WIRESHARK
The most widespread network protocol analyzer is Wireshark [2]. It has an efficient feature and runs on every platform comprising Windows, Linux, OS X, and UNIX. Network professionals, security experts, developers, and educators around the world use it regularly. It is an open source which is used by security experts, network professionals etc. on regular basis. Global team of protocol experts developed and maintained this tool. Wireshark previously used to be recognized as Ethereal. It is a free packet sniffer which has some of the aspects like analysis, network troubleshooting etc. This tool is used for viewing, capturing, and analysis of data packets. It has refined wireless protocol to aid administrators troubleshoot wireless networks. It can capture traffic from the air and decrypt it into that format which aids administrators to trace down those problems which causes poor performance, intermittent connectivity using appropriate driver support.

2. Literature Review
Author [1] executed a network intrusion system with the help of an anomaly tool by considering machine learning. This procedure logged the live network transmission using Wireshark and snort tool. Wireshark showed the I/O graph of network packets. The authors [2] presented a procedure which uses Wireshark to examine network protocols. The author has done examination to identify predictable network threats such as hidden FTP, port search etc. The authors also showed that packet inspection can discover an extensive type of protection vulnerabilities and attacks on networks. The authors [3] projected a framework to dodge DDOS attacks in cloud computing using Wireshark and Snort IDS/IPS. Moreover, authors simplified the facilities available on-demand in cloud storage to permit the customer to access such facilities via internet. DOS and DDOS are the most substantial attacks which yield benefits of cloud computing vulnerabilities. The authors presented an experimental design to stop DDOS attacks but consistency and expense factors were not measured. The authors [4] presented the network protocol analysis to accumulate data for examination and technical understanding of packets. A complete study was presented about network attacks in terms of security, network sniffer and protocol
analyzer. The authors [5] planned technique to assessment the efficiency and accuracy of the DDOS attack. The paper observed important factors that impact the effectiveness and detection abilities of snort and planned schemes for refining the IDS. The research has proven that better tools can use to strengthen snort’s handling effectiveness. Snort IDS are the attacking discovery device which the analysts around the globe intrigued. In [6-7] introduced the device that causes the organization head to make the SnortIDS rules and alarm by means of Graphical User Interfaces (GUI). The authors [8] clarified about Snort lab which assists the understudies with figuring out how to make the Snort-IDS rules. They gave 6 issues to the understudies by applying the Snort-IDS rules for each assaulting discovery. Likewise, In [9-12] authors examined subtleties of Snort-IDS rules to the planned and changed Snort-IDS rules for distinguishing and securing the assault in 3 sorts of site which are SQL infusion, XSS and order execution, individually.

3. Methodology
In the procedure, the final analyzed report of the captured live data packets is generated. The SNORT, an open-source tool will take live data packets from the internet. This tool will match the captured packets with predefined signatures and directs alert messages to the user if matches didn’t find. In the procedure, in order to access internet, WIFI is used so as to get precise flow of data packets. After initiating the capturing process, this tool generates a log file in its directory that stores each and every captured packet [13-14]. This log file entails data packets along with their alert messages. The log file generated by SNORT tool is then exported to Wireshark to examine the captured network packets. The Wireshark tool creates each detail about the packets of the recorded log file. Given figure 1 describes the framework of Wireshark and snort. After then figure.2 explains the flow of methodology.

![Figure 1. Framework of methodology using Snort and Wireshark](image-url)
4. Experimental Results
To configure SNORT, firstly visit www.snort.org.com and also install wincap to use snort tool in windows. SNORT configuration file is divided into 9 sections which are as follows:

- Set the network variables.
- Configure the decoder.
- Configure the base detection engine.
- Configure dynamic loaded libraries.
- Configure preprocessors.
- Configure output plugins.
- Customize your rule set.
- Customize preprocessor and decoder rule set

![Figure 2. Flowchart of methodology](image)

![Figure 3. Successful SNORT configuration](image)
In figure 3 configuration using SNORT is done successfully with a successful message.

![Configuration Success](image)

**Figure 4.** Live data packets captured by Snort with their alert messages

In figure 4 using snort data packets are captured with alert messages. By using “Ctrl+C”, the process of capturing packet will be stopped and can have a summary.

![Summary of Captured Data](image)

**Figure 5.** Summary of captured data packets by Snort- NIDS

In figure 5 the summary of captured data packets is observed using SNORT-NIDS.
5. Export to Wireshark

The recorded log file is exported to Wireshark for an in-depth evaluation of the captured packet. In these different protocols are studied. Whenever the file is retrieved, all the collected data can be seen. It displays the source address and destination address of the packet [15-16], the protocol and the packet information like length. The below figure specifies the network traffic analysis. In figure 6 and figure 7 analyzing of data packet is done.

![Image of Wireshark analysis](image1)

**Figure. 6. Analysis of data packets**

![Image of Wireshark analysis](image2)

**Figure. 7. Analysis of data packets**
A line pattern of the packets is shown on the I/O graph, as seen in figure 8. The x-axis is the time interval per second, and the y-axis is the packets captured in every 1 second. In figure 9, TCP errors and delta time graph are shown. Delta time graph are difference between two packets.

**Figure 8:** Wireshark I/O: ALL 950 PACKETS

**Figure 9:** Wireshark I/O: TCP Errors and Delta time graph
6. Conclusion
The main issue that each agencies or companies faces in this digital scenario is network security. Network monitoring has been a vital aspect of protecting attacks. IDS plays a vivacious role in network monitoring with the help of Wireshark and Snort tools. These tools can track intrusive digital data graphically on network processes. Efficiency and security is improved by IDS and IPS network management. In this paper, Network Intrusion Detection System properties of Snort which is used for intrusion detection by making use of predefined rules and alerting the user by directing alert messages. The SNORT tool creates log file that entails data packets along with their alert messages. The recorded log file is then exported to Wireshark so as to examine the captured data packets. This Wireshark tool generates each detail about the packets of the log file. It provides minute details about frames, internet protocols, Ethernet, protocol hierarchy etc. An I/O graph outlined the flow of the packet which demonstrates the total traffic which is further measured in either bytes or packets per second.

References

[1]. Rashmi Hebbar, Mohan K., “Packet analysis with Network Intrusion Detection System” International Journal of Science and Research (IJSR), vol. 4, Issue 2, February (2015).
[2]. V. Ndatinya, Z. Xiao, “Network Forensic Analysis using Wireshark”, International Journal of Sensor Networks, Vol. 10, No. 2. (2015).
[3]. M. Ahmad, K. Ullah, “Snort Implementation with Wireshark HelpingAvoiding DDOS Attack in the Cloud Computing”, International Journal of Computer Science and Information Security, Vol. 15, No. 1, January (2017).
[4]. Qing-Xiu Wu, “The Network Protocol Analysis Technique in Snort”, International Conference on Solid State Devices and Materials Science, (2012).
[5]. Saboor, M. Akhlaq, B. Aslam, “Experimental Evaluation of Snort against DDOS Attacks under different Hardware Configurations”, 2nd National Conference of Information Assurance, (2013).
[6]. Alia yahia, Eric Atwell, “Evaluation of Capabilities of Wireshark as Intrusion Detection System”, Journal of Global Research in Computer Science, Volume 9, No. 8, August 2018.
[7]. Xiaojin Hong, Changzhen Hu, Zhigang Wang, Guoqiang Wang and Ying Wan, “VisSRA: Visualizing Snort Rules and Alerts,” In Proc. Of Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp.441-444, 2012.
[8]. A. EL-Dia Riad, I. Elhenawy, A. Hassan and N. Awadallah, “Using Jquery with Snort to Visualize Intrusion,” IJCSI International Journal of Computer Science Issues, pp.486-491, 2012.
[9]. Jinsheng Xu, Jinhua Zhang, Triveni Gadipalli, Xiaohong Yuan and Huiming Yu, “Learning Snort Rule by Capturing Intrusions in Live Network Traffic Replay,” Proceedings of the 15th Colloquium for Information Systems Security Education (CISSE), pp.145-150, 2011.
[10]. Mohammad Dabbour, Izzat Alsmai di and Emad Alsukhni, “Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT,” International Journal of Security and its Applications, pp.7- 16, 2013.
[11]. Guozi, S.U.N., Jiang, W., Yu, G.U., Danni, R.E.N., Huakang, L.I.: DDoS attacks and flash event detection based on flow characteristics in SDN. In: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1–6 (2018).
[12]. https://snort.org/. Accessed 28 Dec 2019
[13]. Sakshi Singh, Suresh Kumar, “Capabilities of Wireshark as intrusion Detection System”, International Journal of Recent Technology and Engineering, vol. 8, Issue 5, January (2020).
[14]. Sakshi Singh, Suresh Kumar, “Qualitative Assessment of Digital Forensic Tools” Vidya bharati International Interdisciplinary Research Journal, vol. 10, Issue 1, March (2020).
[15]. Snort_manual.pdf
[16]. https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html