International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876
Impact Factor: RJIF 5.44
www.newengineeringjournal.in
Volume 3; Issue 3; September 2017; Page No. 42-45

Enhancing snort IDS performance using TWIDS for collecting network logs dataset

[*1] Hajar Esmaeil As-Suhbani, [2] Dr. SD Khamitkar
[1] Research Scholar, School of Computational Sciences, SRTM University, Nanded, Maharashtra, India
[2] Associate Professor, School of Computational Sciences, SRTM University, Nanded, Maharashtra, India

Abstract
In recent years, computer networking technology has been utilized by entire mankind across the globe. Snort is an open source software and one of the most successful lightweight network IDS with log analyzer. Snort is mainly compatible with Unix-like operating system such as Linux, but we need to configure it with windows operating system. Snort developers stopped developing any new software on the Windows platform, and this prevents the Windows users to use Snort efficiently. TWIDS is an application which has the ability to process enormous malicious IP addresses in the dataset, by using Snort related protective resources. In addition, it can enhance the network security on Windows operating systems by checking and dropping packets effectively. Therefore, it provides a high network security that can insure the effective using for network gateway. In this paper, Snort is configured as a firewall along with TWIDS software on windows 7 platform, to monitor, allow and/or block connections, and collect log dataset of users' activities.

Keywords: rules, monitoring, blocking, snort, TWIDS

1. Introduction
With the advent of internet technology, day-to-day work has been shifted over internet and thus network security has become a global focus in the world. Although the deployment of firewall technology is the first important milestone toward securing networks, the effectiveness of firewall security may be limited or compromised by a poor management of firewall policy rules. Snort [1] is considered as the best open source IDS, which was created in 1998 by Source Fire. The essential work of Snort is sniffing and checking network data packets content that matches known attacks and it can be used to record a large number of users' activities for collecting dataset [2]. Snort rules can combine the benefits of protocol, signature and anomaly inspection methods. However, most security tools such as Snort are mainly compatible with Unix-like operating systems [3] and it provides a high security to network if configured on Linux platform. In addition, Snort IDS can be configured with Windows as a firewall [4]. When Snort is configured with windows platform, the result is very strong intrusion detection [3]. Snort organization stopped developing any new software on the Windows platform, which prevent the Windows users to use the Snort software efficiently [5].
TWIDS [6] is security software for Windows operating systems, which based on the windows NDIS filter drivers. It filters and drops packets effectively based on the Snort rule set and can process a large number of malicious IP addresses in the dataset. Thus, it provides a security solution that can help to eliminate the investments for network gateway and can be used by common users for limiting the malware traffic [5]. Using Snort IDS with TWIDS software as a control system on windows platform to monitor all traffic, we can record all the actions in the network, and terminating any connections according to rules list. In this paper, the main objective is to implement Snort as a firewall along with TWIDS in windows 7 platform to ensure that all logs of monitoring and detection are addressed and collected as a log dataset.

2. Snort on windows
Mainly, Snort was developed for open source Unix- like operating systems such as Linux and it provides a good security services to network when configured with Linux platform. However, installing Snort for average windows users is a little more difficult than for average Linux users. Many home users may not be able to use Snort directly, because a pre technical knowledge is needed to install Snort software and to modify its packages and configuration files before installation on Windows platform. For various reasons, many system administrators have been switched to Windows operating systems. The lack of available security tools on these operating systems can be frustrating to the system administrators. For this reason, some Snort functionality has been ported to Windows [4]. When Snort configured in windows platform, the result is very strong intrusion detection system.
From Snort organization website, the user can create an account, and all the requirements such as updates and rules can be downloaded from there [7]. After downloading the execution file (.exe), run the installer. After installing Snort in the computer within the network (gateway), we must configure it to work properly and monitoring network traffic to determine which packet is to be allowed or which one is to be blocked. Before running Snort, the config. File must be configured. It is the main file in Snort operation; the Snort preprocessors and detection engine will read this file. It is located in etc. folder in Snort path, and contains sample Snort configuration. Create a custom configuration, by modifying all

the steps in Snort config. File.

Essentially, Snort depends on rules [7], when the connection is established, Snort sniffs and decodes packets by using detection engine and preprocesses, it will compare packet contents against all rules list, then allow/drop or other action will be taken. By using user account, download Snort rules folders [4]. A new rule contains all requirements and specifications for the operation must be accomplished. To use Snort as a firewall, new rules have been created in the local. Rules file which is located in the rule folder. These rules are used to monitor websites accessing and the traffic between network nodes and external network and to allow/block accessing to a specific website. Some of the customized rules are listed in Table 1.

Table 1: Sample of Snort Rules

Website	Rule	Action
Any	Alert icmp any any -> any any (msg:"ICMP Testing Rule"; sid: 1000001 ;)	Alert
Any	Alert tcp any any -> any 80 (msg:"TCP Testing Rule"; sid: 1000002 ;)	Alert
Google	log tcp any any -> any 80 (content:"www.google.com"; \ msg:" tell you GOOOGLE SERACH ENGINE IS WORKING NOW"; sid:1000004; rev:1)	Log
Facebook	drop tcp any any -> any any (content:"www.facebook.com" ;\ msg:" tell you"someone visit FACEBOOK at this time"; sid:1000007; rev:4; resp: reset_source;)	Drop
Twitter	drop tcp any any -> any any (content:"www.twitter.com" ;\ msg:" tell you"someone visit TWITTER at this time"; sid:1000009; rev:6; resp: reset_source;)	Drop
YouTube	Drop ip any any -> any any (content:"www.youtube.com";\ msg:" tell you"someone visit YOUTUBE at this time""; sid: 100000010; rev: 7 ;)	Drop
Any	Drop tcp any any - any 23 (msg: "Telnet attempt"; sid: 10000011; rev: 8; resp: reset_source ;)	Drop
Any	Drop tcp any any - any 22 (msg: "SSH attempt"; sid: 10000012; rev: 9; resp: reset_source ;)	Drop

3. Snort network topology

The network topology is as shown in figure 1. Snort is downloaded and installed on a windows 7 computer which is considered as the network gateway. The default gateway is connected to all computers through a network. Because Snort computer is connected through the internet, it is necessary to set IP addresses for all computers in the network. The network ID is 192.168.137.0/32 and the IP address rang is (192.168.137.1 to 192.168.137.255). The default gateway address for the Snort PC and IP address for other PCs within the network address range is shown in Table 2. When one of the PCs trays to connect to the internet and that website is defined as allowed in Snort rules, the gateway would allow this connection and get alert in Snort log files. However, if that connection is defined in the rule list as UN allowed, it will be blocked from accessing that website and get alert in Snort log files.

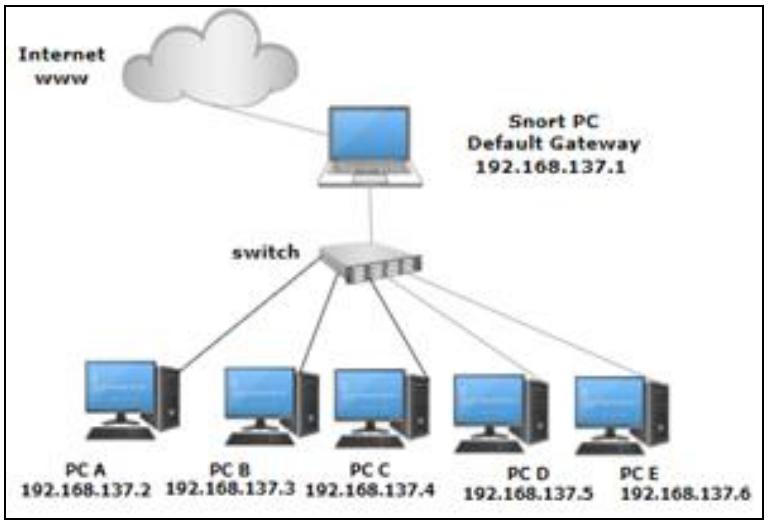

Fig 1: Snort IDS Network Topology

Table 2: IP Addresses for Snort Network Topology

PC	IP address	Subnet Mask	Gateway
A	192.168.137.2	255.255.255.0	192.168.137.1
B	192.168.137.3	255.255.255.0	192.168.137.1
C	192.168.137.4	255.255.255.0	192.168.137.1
D	192.168.137.5	255.255.255.0	192.168.137.1
E	192.168.137.6	255.255.255.0	192.168.137.1

4. Twids software

Snort cannot drop packet on Windows platform, because it needs the WinPcap package to carry out packet filtering on the Windows platform [4]. This causes Snort to lose the protective effect on Windows. Therefore, TWIDS (a filter driver) was designed to overcome this problem. TWIDS operates at the (IMD) layer. It installs the filter driver on the network interface card (NIC) drivers. After application installation, the

TWIDS filter driver is displayed in the properties of the network connection [5]. Figure 2 shows the filter driver on the Windows NIC drivers. TWIDS can drop packets on the Windows platform. It can minimize disturbance by packets from internet and prevent a PC from becoming a victim or/and attacker. TWIDS 1.6 can use Snort rules to filter packets. To get Snort rules to filter packets by TWIDS, the batch file is executed and gets Snort rule list on C:\TWIDS\merge-Snort.bat. The batch files C:\TWIDS\merge-Snort.bat merges Snort rule list to TWIDS engine [6].

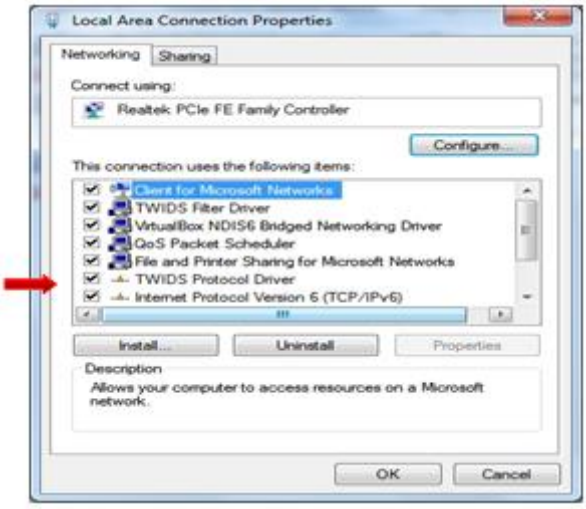

Fig 2: TWIDS filter driver on the Windows NIC drivers

5. Collecting Network Log Dataset

The methodology for generating firewall logs involves devising out our dataset from our deployed firewall. Snort supports a simple rule language, which matches against network packets [4]. TWIDS can receive and utilize all Snort rule sets. TWIDS can detect and protect PCs by Snort rulesets. It monitors packet contents, and generating alerts or log messages in real time [5]. The TCP/IP software on the computer will receive the packets from the driver software and copy them to the process address space. Port numbers are contained in the transport protocol header of the packets, and they can be interpreted by the sender and receiver. In the proposed approach, the logs records dataset is generated using Snort and TWIDS, which have been used to collect the information and activities of 5 people in period of one week. Initially with 13 firewall policy rules, once Snort it is installed in the gateway PC it will automatically captures the network packets passing over the network. It performs the actions and generates alert message files according to the information stored in the rule set as tcpdump. If any malicious activities found then the packet is blocked otherwise it can be allowed. The TWIDS batch file is executed to get Snort rules and provides packet information. Figure 3 illustrates how TWIDS provides packet information triggered by Snort rule set.

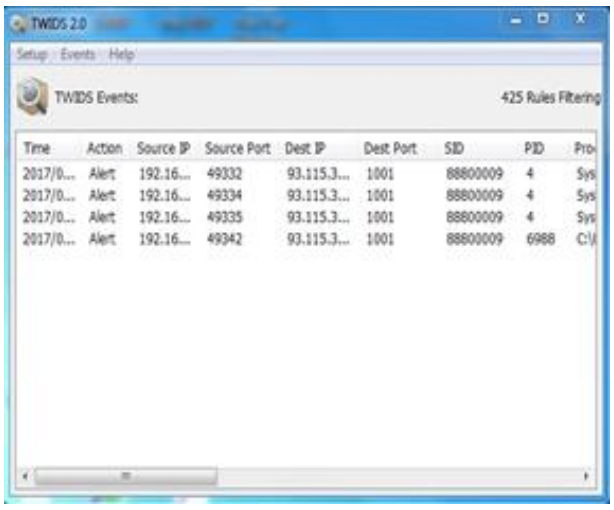

Fig 3: Sample of TWIDS Events

TWIDS provides process name, process id, alert message, source and destination IP addresses and ports, etc. The alert messages are stored as log records in the TWIDS Log folder in plain text and Excel formats. The main fields in the TWIDS events Log file are the date, time, action, source and destination IP Addresses, source and destination ports.

6. Conclusions

Snort supports a simple rule language, which matches against network packets. TWIDS can receive and utilize all Snort rule sets. It can detect and protect PCs by Snort rule sets, monitors packet contents, and generating alerts messages in real time. In this paper, a Firewall has been implemented using Snort and TWIDS and configured with windows environment, which was used to record logs data set of user activities.

7. References

1. Snort. An open source network intrusion detection system. http://www.Snort.org/.
2. Saboori E, Parsazad S, Sanatkhani Y. Automatic firewall rules generator for anomaly detection systems with Apriori algorithm. 3rd International Conference on Advanced Computer Theory and Engineering ICACTE, 2010, 57-60.
3. Zhou AT, Blustein J, Heywood NZ. Improving Intrusion Detection Systems through Heuristic Evaluation. IEEE Journal, computer security, 2004; 6(4).
4. Moath Alsafasfeha, Abdel Ilah Alshbatatb. Configuring Snort as a Firewall on Windows 7 Environment, Journal of Ubiquitous Systems & Pervasive Networks, 2011.
5. Chen, Kuo, Yu-Wen Chen. Security Software based on Windows NDIS Filter Drivers. Computer Software and Applications Conference Workshops COMPSACW, 2013 IEEE 37th Annual.
6. TWIDS : http://twids.cute.edu.tw/en
7. Rafeeq Rahmman. Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort Apache, MySQL, PHP and Acid. 1st Ed. Prentice Hall, 2009.