Configuring Snort as a Firewall on Windows 7 Environment

Moath Hashim Alsafasfeh[a], Abdel Ilah Noor Alshbatat[b]

[a]National university of Malaysia UKM, Selengor, Malaysia.
[b]Tafila Technical University, Electrical Engineering Department,Tafila, Jordan, 66110.

Abstract

Nowadays, computer networks play an important role in our daily live, and the widely use of computer networks are for accessing the internet. The network administrator has a full ability to control all access types to network, and tasked to allow or discard some of the connections. By using Snort Intrusion Detection System (IDS), the network administrator can monitor network access from the sender to the receiver. Snort is one of the IDS, and it is difficult to configure it with closed source operating systems for the purpose of accessing and terminating connections. Moreover, it needs more requirements to work with windows operating system. Snort is compatible with open source operating systems such as Linux but there is a need to configure it with closed source operating systems such as windows operating system. In this paper, Snort is configured with windows 7 operating system so that it will work as a firewall to monitor and terminate connections. This configuration is successfully achieved by identifying new rules in snort package. Using snort IDS, network administrator is able to monitor, allow, and block any accessing to the web with the ability to get alerts containing information related to the connection such as IP address and port numbers. Moreover, a Graphical User Interface (GUI) has been developed to allow end user to configure new snort rules with a user friendly interface depending on snort user requirements. The results indicate that the Snort can be configured with Windows 7 by creating new snort rules to monitor network traffic and terminate connection between two entities. In addition, they show how a GUI allows snort user to create new rules based on him/her requirements.

Keywords: *Intrusion Detection System, Intrusion Prevention System, Snort, Monitoring, and Blocking.*

1. Introduction

Snort is an open source network intrusion prevention and detection system developed by Source fire. It combines the benefits of signature, protocol, and anomaly-based inspection methods and uses as a control system to monitor all network traffic and prevent network from any attack. Snort is compatible with open source operating systems and provides a good security services to network if configured with Linux open source operating systems [2]. When we configure snort IDS with windows operating system, the result is a very strong intrusion detection system with highly secured networks [3]. Using snort IDS as a control system with windows to monitor all traffic, the administrator can be informed by reporting all actions in the network, and terminating any connections from the network to other entities that try to attack the network. The challenge herein is not only to be able to actively monitor all the activity but also to be able to react quickly to different events. The main objective aimed in this paper is to implement Snort in a windows-based environment to ensure that all aspects of monitoring and detection are addressed satisfactorily.

2. Methodology

In the following subsections, configuring snort IDS with windows operating system is going to be explained based on what is shown in figure 1. Before installing Snort, we need to verify that the system has a number of software packages installed. These packages are: Windows Packet Capture, Libnet, Data Acquisition, and Barnyard. Those programs allow snort IDS to work with closed source as a detection system to monitor network traffic.

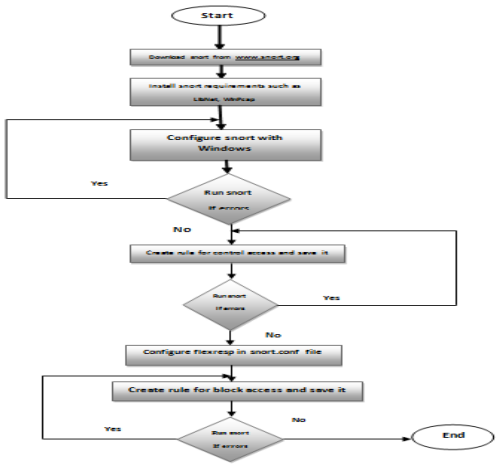

Fig. 1. Methodology Flow Chart

After downloading and installing all requirements for snort IDS to work with windows operating System, snort IDS can be

used as a detection system to monitor all packets that are sent or received. The Snort engine is distributed both as source code and as binaries for popular Linux distributions and windows. It's important to note that the Snort engine and Snort rules are distributed separately.

By creating an account in snort IDS organization, all requirements can be downloaded as well as all rules and updates that are used for developing snort engine [1]. From snort website, choose download snort , in the new window you can note that there are many latest releases, choose binaries section because of using windows operating system [1], then choose snort execution file (.exe). When start downloading, make sure to choose IPv6 because it is widely used at this time and in the future.

2.1. Snort Configuration

After installing snort on windows operating system, it must be configured to work correctly and capture packets. Monitoring network traffic to determine which attack is to be prevented or which one is not allowed to access my network to be terminated. Snort depends on rules [1], when the connection is created, snort decode packets and by using preprocesses and detection engine, it will compare packet contents with rule contents, if it is matched then the drop or other action will be occurred as shown in Figure 2. By using user account, download snort rule then choose all rules folders and download it.

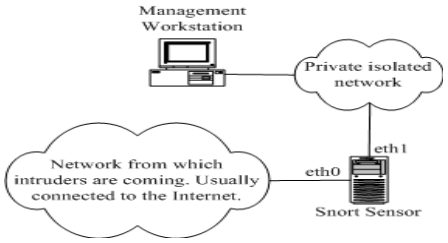

Fig. 2 Snort Operation

2.2. Configuring the snort.conf File

Snort.conf file is the main file in snort operation and must be configured before running snort; this file will be read by the detection engine and preprocessors. Snort.conf file located in etc folder in snort path. Snort.conf file contains sample snort configuration. To create a custom configuration, follow the following steps:

i. Set the network variables.
ii. Configure the decoder.
iii. Configure the base detection engine.
iv. Configure dynamic loaded libraries.
v. Configure preprocessors.
vi. Configure output plug-in.
vii. Customize your rule set.
viii. Customize preprocessor and decoder rule set.
ix. Customize shared object rule set.

2.3. Running Snort as Firewall

Firewall is a device or set of devices used to control access to network based on a set of rules. Snort is open system which works as a firewall to control access. Using snort, a new rule contains all specifications and requirements for the operation must be done. To make snort as a firewall, you have to create new rules. The first one is used to monitor websites accessing and tell network administrator about the whole connections between network nodes and external network. The second one is to block accessing to a specific website.

2.3.1 Configuring Snort for Monitoring Access

Snort based on a set of rules, these rules contain a set of operations that allow network administrator to monitor all network traffics. To create a new rule that has the authority to monitor all accesses form our network to external networks, you must write all primary contents of rule header and rule options.

Making snort as a monitoring system that is telling the network administrator who is visiting websites such as YouTube, Facebook or Google. The first step is determining content of rule header. In this case the rule header is:

Alert ip 192.168.1.2 any -> any any

From the above rule; the action is alert, because it is used to tell network administrator who is accessing the network. IP protocol is used to check the link layer which determine the packet type and check IP addresses of the two entities. IP address is 192.168.1.2; this address for the local machine and can differ from machine to another machine. To skip this point you can put any keyword instead of IP address and select any port. The direction is from local machine in my network to other computer or server. The destination part is any because the destination can have any IP address or port number.

After determining the rule header, the rule options must be determined. The rule options are control access to websites and tell network administrator who is accessing a specific website such as YouTube and which IP address is accessing to YouTube and the access time. The rule is shown in Figure 3.

```
alert tcp any any -> any any ( content:"www.facebook.com" ;\
 msg:"moath tell you"someone visit FACEBOOK at this time""; sid:10000009; rev:1;)
alert ip any any -> any any ( content:"www.youtube.com";\
 msg:"moath tell you"someone visit YOUTUBE at this time""; sid:1000004; rev:2;)
alert IP any any -> any 80 ( content:"www.google.com"; \
msg:" moath tell you GOOOGLE SERACH ENGINE IS WORKING NOW"; SID:222999; REV:3;)
```

Fig. 3 Snort Rules for Monitoring Access

After creating the rule, it must be configured with snort, because snort depends on rules contents in performing some actions by comparing packet content with rules. To configure new rule with snort, it must be saved in rule folder with .rules extension, new rule file saved as (moath.rules). After that, the path of new rule file must be written in snort.conf file in the site specific rules and save configuration rule as shown below:

```
# site specific rules
include $RULE_PATH\moath.rules
```

As running snort in IDS mode, there were no errors detected. If some errors have appeared, a message that will appear in command prompt and snort.conf file must be checked for correction.

2.3.2 Configuring Snort for Blocking Access

The first step in configuring Snort for blocking access is to configure it with active response. Active response is a race between Snort and the endpoints in network communication [4]. Active response is a supplementary tool, deployed in

addition to other security technologies. It should not be relied upon solely to protect systems or services that are known to be vulnerable. The process of transmitting active response packets will block the rest of the system. To activate active response, flexresp2 will be used.

The flexresp2 detection plugin for Snort allows users to configure rules that will attempt to terminate connection actively [5]. The process of active response consists of two steps: First step is to create some Snort rules that use the resp keyword [1]. Write new rule in the same rule file (moath.rules). Determine rule header with alert action, IP protocol, IP address 192.168.1.2, direction, any IP address and port for destination.

The main part in this rule is to add *resp* keyword with a suitable modifier as follows:

- reset_dest : send TCP reset packets to the destination of an attack.
- reset_source : send TCP reset packets to the source of an attack. This is best way used with attack-response rules.
- reset_both: send TCP reset packets to both source and destination of an attack (the destination resets are sent first).
- icmp_net: send an ICMP network unreachable packet to the attack source.
- icmp_host : send an ICMP host unreachable packet to the attack source.
- icmp_port: send an ICMP port unreachable packet to the attack source.
- icmp_all: send all of the above to the attack source.

After determining the resp modifier, write resp part at the end of the rule. The best modifier is reset_source because the termination process will be start from sender to destination. The final structure of rules is shown in Figure 4.

```
alert tcp any any -> any any ( content:"www.ammonnews.net"; msg:"not allowed access to ammonnew.net please call moath"; priority:1; sid:10000088; rev:3; resp: reset_source;)
alert ip any any -> any any ( content:"www.yahoo.com"; msg:"not allowed access to yahoo.com please call MOATH KBJ"; priority:1; sid:10000089; rev:4; resp: reset_both;)
```

Fig. 4 Snort Rules for Blocking Access

After creating rules to block access, it must be configured in snort configuration file. Flesresponce2 is configured in snort.conf file by defining network interface and define number of brute-force TCP resets. Flesresponse2 is configured in snort.conf file as shown below:

config flexresp2_interface: 3
config response:attempts 20

The network interface is 3 because of the use of wireless network, and the number of attempts is 20. Since 20 is the maximum number of attempts; running snort in IDS mode with all previous configurations should work correctly without any errors. If any error occurred, the command prompt would tell the error type and its location.

2.3.3 Snort IDS Network Topology

The network topology contains a set of devices connected with snort IDS device. In other word, snort IDS is downloaded and installed on a computer that connected to all computers through a network. Since Snort IDS computer is connected through the internet, there is a need to set IP addresses for all devices in the network. The network ID is 192.168.1.0\24 and the IP address rang is (192.168.1.1 to 192.168.1.255). As an example, set the default gateway address for the snort devices as shown in figure 5, and set IP address for other devices within the network address range as shown in Table 1. In the case that there is one of the devices tried to connect to the internet, the snort IDS computer would allow this connection, but would get alert in snort log files if that website is defined in snort rules, or if that connection is not allowed; it will be blocked from accessing the requested website as it is defined in snort rules as shown in Figure 5.

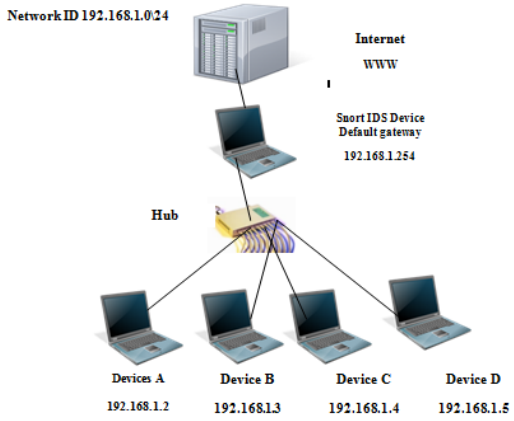

Fig. 5 Snort IDS Network Topology

Table. 1 IP Addresses for Snort Network Topology

Device	IP address	Subnet Mask	Gateway
A	192.168.1.2	255.255.255.0	198.168.1.254
B	192.168.1.3	255.255.255.0	198.168.1.254
C	192.168.1.4	255.255.255.0	198.168.1.254
D	192.168.1.5	255.255.255.0	198.168.1.254

The blocking access is done when the administrator is accessing the website, but when one of the client try to access the website, snort will get alert but it doesn't block access since snort device working in passive mode. In other word, In-line mode is required with this network, and the In-line snort mode is not compatible with Windows operating system. Snort IDS computer will work as a network administrator, it will check for all connections and get alert for each access. All snort IDS computer functions based on snort rules, and can create new rule for new functions based on network administrator requirements.

alert tcp 192.168.1.2 any -> any 80
(content:"www.google.com"; msg: "NOT ALLOWED"; sid:1000008; rev:1; priority:1; resp: reset_source;).

2.3.4 GUI for Snort IDS Rules

A Graphical User Interface allows snort IDS user to create new rules by a simple method and directly without difficulties. The GUI is designed to create new rules and save it automatically in the rules path for the snort program (save new rule in *moath.rule* file), so no changes need for snort configuration

file, because the *moath rule* file is configured with snort and its path set in the configuration file.

Snort rule contains two main parts: rule header and rule options. Snort rule parts depend on each other to perform rule function without errors if it is created correctly.

Figure 6 shows the GUI that allows snort user to create his\her rule. The first part is determining rule header by specifying rule action such as alert, pass and drop. Choosing protocol depends on rule functions that may be one of these protocols TCP, IP, UDP or ICMP. After determining rule action and it's protocol, connection entities (source and destination) must be determined by defining IP address and port number for each. IP address can be any address or specific address such as 19.168.1.2, and the port number can be any number or specific number depending on rule function such as 80 if the rule deals with HTTP protocol. Connection direction can be determined based on rule function which may be from source to destination, between them or form destination to source. After determining rule header in correct form, the user can determine rule options.

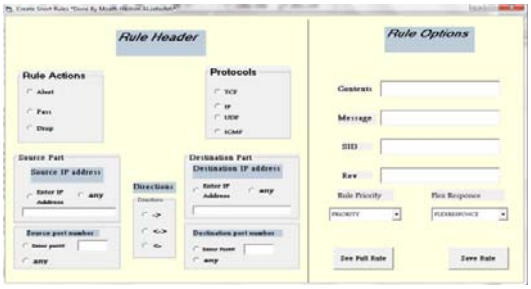

Fig. 6 GUI for Snort Rules

Rule options in Figure 6 have six options: these options are popular in all snort rules except Flexresp. They are added to the GUI since one of the objectives of this paper is to terminate connection between source and destination. First option is the content; it is specific for the website that rules option will applied on it. Second option is the message that will appear in command prompt when the content of packet matched with rule options. SID is a security ID that is given to the rule with value greater than 1000000 as shown in Figure 3. Rev is a specific number to identify rule in snort organization for update purposes. It takes values (1, 2, 3…) as shown in Figure 3. Priority option takes integer value, maybe 1 or 2. To get high priority of rule greater than other rule; flexresponce allows snort user to block website access by using three types : reset destination, reset source or reset both source and destination.

3. Results

New rules have been created to allow snort to monitor access and get alert for system administration. Alert file contains all data that describes the connection between two entities, IP address for two entities (sender and destination) and the access time. The rules below were written in snort environment to monitor access to websites. As running snort in IDS mode and some users access to websites such as Facebook, YouTube and Google, the detection engine in snort has checked packet contents with rule options and when matching is found, the snort engine will send alert to network administrator with message tell him\her who is accessing the website.

From Figure 7, when snort detection engine runs and user access to google.com, snort sends alert to network administrator telling him who is accessing the website by specifying the IP address of the sender (192.168.1.3) and destination address (74.14.203.99) and which ports are used (by sender 1937 and by destination 80) and time of connection at 05/12-20:05:30.712395.

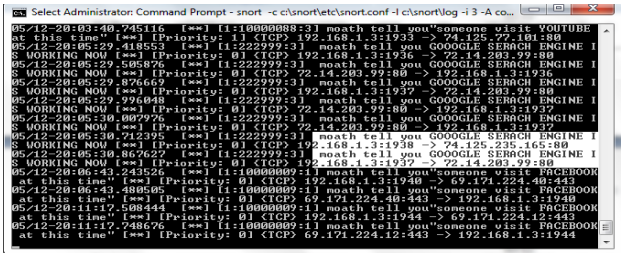

Fig. 7 Snorts Get Alert for Google Website

Depending on Table 2, all information shown is related to the connection between user and three websites: YouTube, Facebook and Google. Note that the destination port is 80 and the source port is differing between connections since it takes port number for each connection and can use many port numbers in snort rule by define port number such as 8080 instead of *any* keyword. So it differs from session to another for the same website, because the port number for destination is defined *any* in snort rule.

Table 2 Snort Alerts for Monitor Access

Website	Source address	Destination address	Source port	Destination port	Access date and time	Connection Statues
YouTube	192.168.1.3	74.125.127.93	1928	80	05/12 20:03:38.721770	allowed
Facebook	192.168.1.3	69.63.189.26	1896	80	05/12 20:03:00.212437	allowed
Google	2001:0:4137:9e76:3cf4:11aa:f5e9:f5c7	2404:6800:800b::68	1938	80	05/12-20:05:30.712395	allowed
YouTube	192.168.1.3	74.125.235.171	1927	443	05/12 20:03:21.772	allowed
Facebook	192.168.1.3	69.63.189.26	1924	443	05/12 18:10:53.188345	allowed

New rules have been created to allow snort to terminate connection between two entities and send alert to the system administrator. Alert file contains all data that describes the connection between two entities depending on IP addresses for the two entities (sender and destination) and the access time. As an example, the connection between user machine and any of these two websites: Yahoo.com and ammonnews.net will be terminated and an alert will be sent to network administrator contains all information of connection as shown in Figure 8.

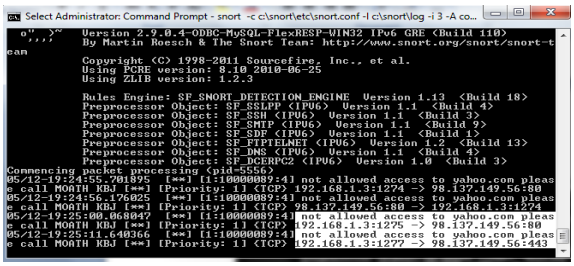

Fig. 8 Snort Alert for Block Access to www.yahoo.com

Depending on Table 3, all information showed the related connection between user and two websites Yahoo and Ammonnews. Note that the destination port number is 80 and the source port number is defined as *any* in snort rule. It is obvious that the connection status is blocked.

Table 3 Snort Alerts for Blocking Access

Website	Source Address	Destination Address	Source Port	Destination Port	Access Date and Time	Connection Statues
Yahoo	192.168.1.3	98.137.149.56	1275	80	03/16 22:07:38.232538	block
Ammonnews	192.168.1.3	74.86.156.8	1759	80	05/12 19:30:53.188345	block
Yahoo	192.168.1.3	98.137.149.56	1277	443	05/12 19:43:53.134544	Block
Ammonnews	192.168.1.3	74.86.165.8	1761	1433	05/12 19:33:53.188367	block
Ammonnews	192.168.1.3	74.86.165.8	1769	8081	05/12 19:51:53.18955	block

4. Conclusion

Snort is the best alternative system to ensure network security. It considered as the heart of Intrusion Detection System. In this paper, Intrusion Detection System with snort has been implemented and configured with windows-based environment. However, snort is a strong Intrusion Detection System; the problem is that snort system is not familiar with Windows Operating System. The results show that it is possible to configure snort IDS with Windows and it can be configured as a firewall. Moreover, Graphical User Interface is created in this paper to allow snort user to create new rules. As stated above, GUI contains two parts in which the user can select rule header information and determine rule options to create specific functions such as controlling the access or terminating the connections between two entities.

5. References

[1]. Rafeeq Rahmman. 2009. *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort Apache, MySQL, PHP and Acid*. 1st Ed. Prentice Hall.

[2]. Zhou, K. Chu, J. Che, X. Lin, L. and Hu, L. 2008. Improvement on Rules Matching Algorithm on Snort Based on Dynamic Adjustments. JilIin University.

[3]. Zhou, A, T. Blustein, J. and Heywood, N, Z. 2004. Improving Intrusion Detection Systems Through Heuristic Evaluation. *IEEE Journal, computer security*. Vol 6. No 4.

[4]. Muthuregunathan, R. Siddharth, S. Srivathsan, R, and Rajesh, SR. 2009. Efficient Snort Rule Generation Using Evolutionary Computing for Network Intrusion Detection. *IEEE Journal. Vol. 6 No. 9*

[5]. Frey, M. 2005. Securing your System with Snort. [Online], Available:http://www.redhat.com/magazine/013nov05/features/snort/ [Accessed 30 march 2011].