



<http://www.ijssit.com>

FRAMEWORK EXAMINING IMPLEMENTATION OF SNORT AS A NETWORK INTRUSION DETECTION SYSTEM AND PREVENTION SYSTEM

^{1*}John Marete

Mount Kenya University, Kenya

jmarete@mku.ac.ke

Abstract

Any network is subject to any kind of attacks, intrusion detection systems (IDSs) is a mechanism that provides advanced security mechanism to both computer machine, systems and the entire network. The key responsibility for IDSs is detect any anomalies, suspicious, or violation of set network policy and rules so that it can alert network

Introduction

Snort[1] is a free and open source intrusion detection system(IDS) by Marty Roesch in 1998. Martin Roesch released Snort. A Snort works as a packet sniffer which is one of the network security tools used today. Implementation of this security monitoring tools in a network basically is to keep track of network traffic and scan any violation of network rules and policies. It also checks on any anomalies, potential attacks, virus, worms etc. when implemented in any network it assists network administrators to easily identify any type of attacks, compromised systems, wrong machine configurations, traffic leaks etc.

Basically snort can be configured in network devices like hubs or in host based IDS to monitor flow of traffic to and from network machines. By the use of a PHP web based console you can place

administrator any malicious activities in the network. Various network monitoring tools are in use firewalls, snort etc. The use of Snort which is an open source and popular can enhance set rules (signatures).

Keywords: IDS, HIDS, NIDS, Network analysis

snort scanner in a certain console monitor for your network to track various activities. Snort can be implemented in IDS as well as in IPS by the use of inline mode tying Linux iptables and or BSD firewall application.

Five Components of Snort

1. A Packet Decoder- this is snort device component that collects data packets from different network interfaces and prepares the packets to be pre-processed within the network.
2. Pre-processors component is after Decoder is used to arrange and modify traffic packets before being analysed by the detection engine in the architecture. It detects some basic network anomalies by

de-fragmenting traffic packets using HTTP and URL.

3. Detection Engine comes after packets have been checked by pre-processor they are passed to Detection engine. Then the Detection engine takes that data packets and checks through set of rules and policies. If the database rules match with the data in the packet, they are sent to the alert processor. Once the Snort data packets processed in Detection engine, and if data matches a rule, an alert is triggered.
4. Logging and Alerting System part comes after the detection of any intrusion by the detection engine, the activity is logged for the perusal of the network engineers or an alert is generated and transmitted to centralized main id.

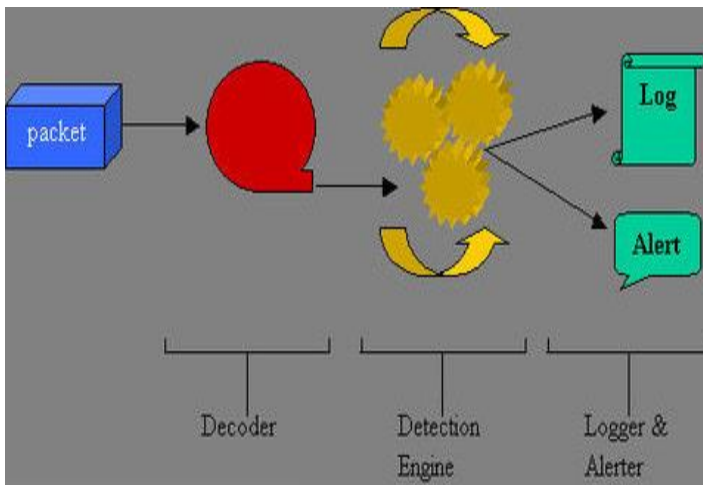


Fig1 snort components

Benefits of snort

1. It is an open source network system which is free.
2. Widely deployed IDS/IPS technology and combines the benefits of signature, protocol, and anomaly-based inspection.

3. Performs protocol analysis and content searching/matching.
4. Snort ids can be used to detect a variety of attacks and probes
5. Snort is an open source project, available for anyone to use for free
6. Evaluates and fine tune access control rules on firewalls and routers.

Snort Disadvantages Lawton (2002)

- During the time of capturing all network packets, it can produce large log/alert files it can also be difficult to cull through bulk of information.
- Network-based IDS is the problem of collecting and analyzing the potentially vast amount of log/alert files.
- Contains analysis Console that shows intrusion logs where network administrators will attempt to reduce exposure to vulnerabilities by segmenting their networks.
- Snorts Generates Traffic - Above the normal level of network traffic on the segment, the monitored workstations are sending information back to the central management system.

6. Lastly another problem with Snort is vulnerability to huge amount of alerts, unknown attacks, and no ways to identify the importance of alerts.

Challenges with snort

1. Misuse detection – avoid known intrusions
2. Rules database is larger and larger
3. It continues to grow

4. Snort spends 80% work time to do string match
5. Anomaly detection – identify new attacks
6. Probability of detection is low

How the Snort works with Network packets

1. Is it possible to get data traffic from snort IDS
2. Snort receives a number of data packets that from one destination only
3. Number of packets that Snort receives from all senders
4. The time between two received packets

Types of snort

SnoGE

Snort type that unified reporting tools, it processes your unified data packets and represents them as place-marks on the Google Earth application. SnoGE operate in following modes, Real-time, refresh, and one-time mode.

Pulled_Pork

Snort IDS software tool written in Perl program for managing Snort rule sets. It consists the following features:

1. Automatic rules for downloads
2. MD5 verification prior to downloading new set rules
3. Full handling of Shared Object rules snort
4. Generation of snort rules for stub files
5. Modification of rule set state

PE Sig

PE Sig is a snort tool written in Ruby that generates various signatures for portable executable files in various applications.

Dumb Pig

Snort IDS tool is used to detect automated bad-grammar for snort rules as IDS. It works by parsing various rules in a file and reports on incorrect usage, badly formatted entries, and any alerts to possible network performance issues.

Snort security

Snorts ids allows user to separate the network access control from the operating system, it safeguards the network against any threats, attacks and intrusions. Therefore the snort can be evaluated using the following: Manufacturers snort details

This details shows the application/usage of the snort eg installations, configuration etc.

Snort design

This defines the architectures of running the snort that contains the firewall that facilitates the detection and security issues.

Snort database/information

This defines the logs of snort towards the attempted penetration from outsides defined by the set standards, rules and policies of the device.

Testing snort intrusion penetrations.

Test the attempted intrusion this can be done by scanning the basic penetration access points by the hackers to the networks. A plan should be set in order to allow effective testing to take place.

Testing snort basis principles:

One should test the basic rules governing the implementation of the snort in wireless sensor network basically check on the:

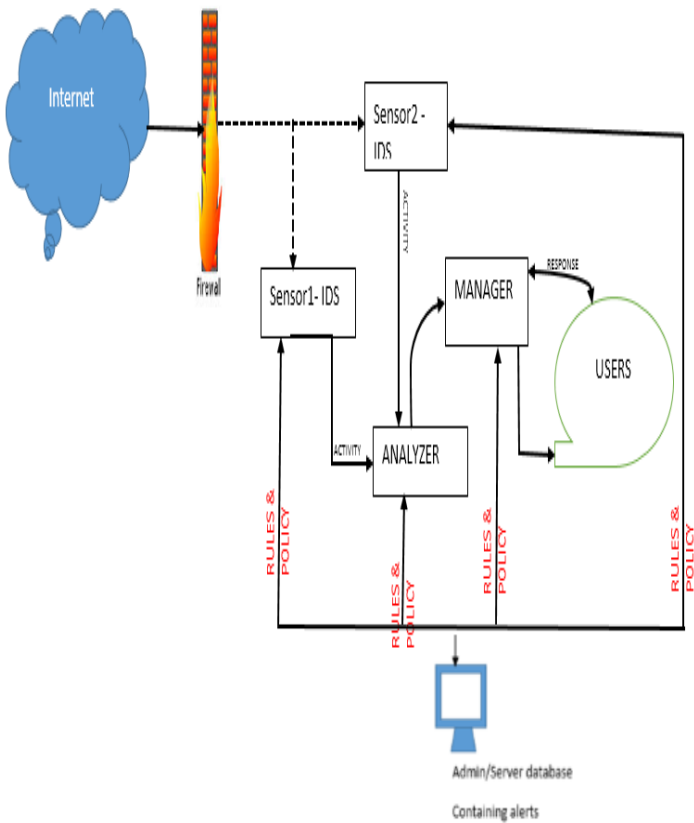
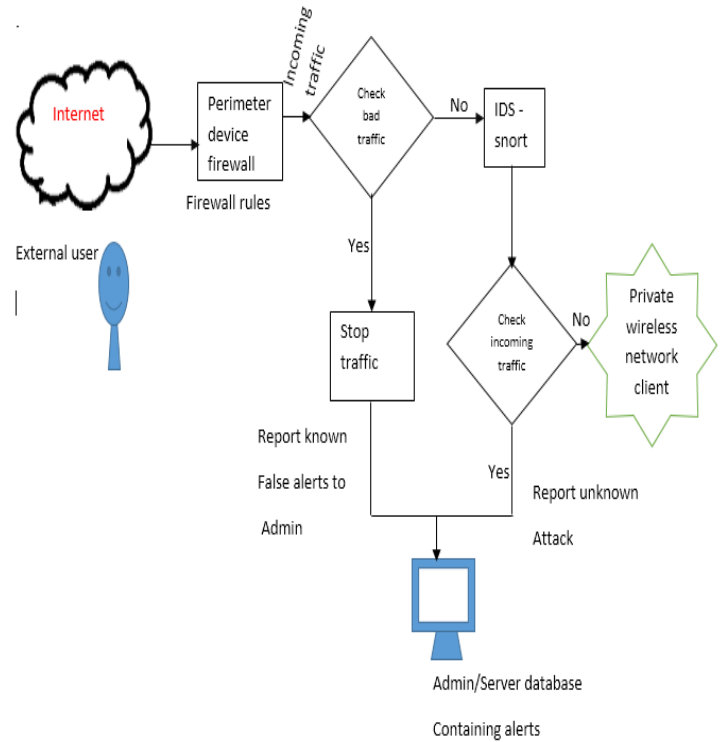
Snort security issues

- i. Confidentiality of the data packets
- ii. Access control within the network

- iii. Incoming and outgoing transmission of data packets.
- iv. Availability of services etc.
- v. Functionality of the snort.
- vi. Check for services available.
- vii. Check intruder's activity from public network that are incoming to private network.

Snort intrusion verification:

This is done to defect any leakage into the system with the purpose of determine and giving assurance that there are no single entry point of leakage into the network from external network. This also helps to determine the attempted logos. Therefore, the snort should be able to detect the attempted attack.



Result Analysis and evaluation

The focus in this framework is to examine the operation of a snort in a wireless sensor network to detect network intrusion using WIDS. Sufficient results will be gotten from how the snort is designed, installed and configured in the Wireless Network that secures the network from any attack or intrusions. The snort frameworks implementation, dataset used and the testing should facilitate sufficient results to be realised in WIDS situated in the snort server that contains different rules and policies.

NETWORK INTRUSION DETECTION SYSTEM SNORT CONSOLE											
Latest Events											
	<Sensor>	<SnID>	<Signature>	<timestamp>	<srcIP>	<Sport>	<Dest.Ip>	Dport	Sbyte	Obyte	<Attack Type>
Examine Events											
Server Management	Snortids	104691	SnortAlert1	2013-09-07 17:20:36	192.168.120.100	113	192.168.150.10	52	688	560	Backdoor
Client Management	Snortids	104691	SnortAlert2	2013-09-09 10:05:22	192.168.0.128	324	192.168.150.10	53	720	30	DOS
Report	Snortids	104691	SnortAlert3	2013-09-09 15:55:07	173.168.150.1	993	192.168.150.10	80	823	30	HTTP
Management	Snortids	104691	SnortAlert4	2013-09-10 08:05:22	10.1.1.66	80	192.168.150.10	79	142	23	Finger protocol
Account	Snortids	104691	SnortAlert5	2013-09-11 13:18:36	192.168.20.100	139	192.168.150.10	139	1003	790	DDOS
Management	Snortids	104691	SnortAlert6	2013-09-11 17:01:50	62.10.0.100	80	192.168.150.10	21	62	60	Trojan spyware
Logtime	Snortids	104691	SnortAlert7	2013-09-12 07:35:11	192.168.15.10	All	192.168.150.10	All	235	235	No alarm
Administrator	Snortids	104691	SnortAlert8	2013-09-13 18:15:02	173.168.150.1	22	192.168.150.10	445	10	0	TCP
Account											
Client User											
Type of attack											

The report shows that various types of attack are realised after the installation of firewall, snort and other security devices helps in detecting these attacks.







Experiment one

Aims to examine if snort enforces filters on incoming and outgoing spoofing and spying traffic. Backdoor

Backdoor being executable program that can be used to spy and spoof the target host. Once you install it. It provides a hidden means by passing normal authentication that obtains remote access. The software disguises itself to be ICQ installation program that failed during installation. After completed installation it will open a port and allow attackers or intruders to gain network access. The backdoor consists of two parts for the client and server. The server connects to the client as executable files which the user installs without much suspecting any problem. Once it is installed, then it opens client ports and initiates an attack.

Results Analysis

From the alert. Ids file it shows a RPC (Remote Procedure Call) an attack based on buffer overflow exploit which is classified as Misc activity and label it as priority which is rank as low level attack according to WIDS snort rule based listing. The host executing the attacks host with IP Address 192.168.120.100 targeting host with IP Address 192.168.0.128 which in this case is mail server. The port being used is port 52 where the snort cannot filter. The port 53 is now open where backdoor attack uses to explore network services classified as attempted administrator privileges gain with Priority which high. This implies the attacker have administrative privileges meaning access of network services if fully accessible. The protocol use in this case is TCP. When administrator has this report then it be ease to filter all traffic using TCP port 52 by enforcing the rule on Snort.

SNORT CONSOLE EXAMINING EVENTS ON INTRUSION DETECTION								
operation	Date Time	from	Name	To	Name	Protocol	Detection	details
 	2013-09-07 17:20:36	192.168.120.100	complab	192.168.150.10	1125-56	TCP	[Snort:backdoor-netbus-pro 2.0 connection request]	Details
 	2013-09-07 17:22:00	192.168.120.10	complab	192.168.150.10	1125-56	TCP	[Snort:backdoor-subseven 22]	Details
 	2013-09-07 17:56:30	192.168.120.12	complab	192.168.150.10	1125-56	TCP	DOS	Details

Experiment2

Aim: This experiment examines if snort enforces configured rules and policies towards incoming and outgoing traffic.

The DOS attack test the death of ping attack

The aim of using death of ping attack is to test snort has ability in detecting the traffic both from internal network and public network. The tool aimed at installed servers by sending infinite data packets. The target central servers should response to all ping packets sent to the internal network. Configured snort should stop this death ping immediately as soon it appears. The command used ping < IP target host> -t -l 65500. This command will send packet at 125 kbs. The target host test is mail server with ip address 192.168.0.128 as shown below:-



Figure 6: Death ping

Results Analysis

The report shows that traffic date, time, timestamp, packet NETBIOS Unicode data share accesses classified as generic protocol commands on decode priority, SMB, DOS etc. Analyzes of the report shows alert events had heavy traffic both coming from internal and external towards a given address 192.168.150.10 port 53 which is used for NETBIOS. The NETBIOS services are used to allow communication within internal LAN. This report provides information about the

status of hosts in the private network. The traffic is detected through the port 53. The other intrusion includes the HTTP, Finger protocol, Trojan horse.

REFERENCES

[1] Baker, A. R., Beale, J., Caswell, B., & Poor, M. (2004). *Snort 2.1 Intrusion Detection Second Edition*. Rockland, MA: Syngress Publishing, Inc.

[2] Brian Caswell, Jay Beale, Andrew Baker, "Snort IDS and IPS Toolkit" 2007 | pages: 769 | ISBN: 1597490997 | PDF | 8,4mb

[3] Carl, E. S. J. M., 2004. *Intrusion Detection & Prevention*. ISBN: 0072229543 ed. s.l.:s.n.

[4] Caruso, L. G. G. M. F., 2007. *SPP-NIDS, A sea of processors platform for Network Intrusion Detection System*. IEEE/IFIP International Workshop on Rapid System Prototyping, Issue 18, pp. 1-12.

[5] Deris, A. M., 2011. *Pitcher Flow: Unified Integration for Intrusion Prevention System*. Singapore, IACSIT press

- [6] *Generation over Anomalous Internet Episodes. IEEE Transactions on Dependable Computing 4(1):41-55.*
- [7] Gauda, M and Liu, A. (2005). *A model of Stateful Firewalls and its Properties. Proceedings of the 2005 International Conference on Dependable Systems and Networks(DSN'05)*
- [8] Hwang, K., Cai, M., Chen, Y. Qin, M. (2007). *Hybrid Intrusion Detection with Weighted Signature*
- [9] Joseph, S and Rod, A (2003). *Intrusion detection: methods and systems. Part II. Information Management and Computer Security 11(5):222-229.*
- [10] John, W. C., 2008. *Qualitative Inquiry and Research Design: Choosing Among Five*
- [11] Kobayashi, Y. B. a. H., 2003. *Intrusion detection systems: Technology and Development. IEEE Computer Society Press. Nihon University and Beihang University, IEEE Computer Society Press..*
- [12] Mahendra Pratap Singh Team: *Whitehat People 2004) Intrusion Detection System/Intrusion Prevention System (Snort)*
- [13] Mohammad (2012) *International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012*
- [14] Nalneesh Gaur 2001, *Snort: Planning IDS for your enterprise*
- [15] Newman, D, Snyder, J, Thayer, R. (2002, February 24). *Crying wolf: False alarms hide attacks Retrieved March 15, 2008, from http://www.networkworld.com/techinsider/2002/06_24security1.html*
- [16] Rafeeq Ur Rehman (2007) *Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID*
- [17] R. Sommer, V. Paxson, "Enhancing Byte-Level Network Intrusion Detection Signatures with Context," *ACM conf. on Computer and Communication Security, 2003, pp. 262--271. citeseer.ist.psu.edu/sommer03enhancing.html*

[18] Sailesh Kumar Snort: Light weight intrusion detection for networks," In Proc.13th Systems Administration Conference (LISA), USENIX Association, November 2003 pp229-238.

www.snort.org/

[19] Sailesh & Kumar (2003) Intrusion detection systems using snort IDS