

**FRAMEWORK FOR EXAMINING INTRUSION
DETECTION IN WIRELESS NETWORK**

BY

JOHN MBAABU MARETE

KCA/11/02984

**A RESEARCH PROJECT SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD
OF MASTER OF SCIENCE IN DATA COMMUNICATION AT
KCA UNIVERSITY**

NOVEMBER 2013

DECLARATION

I declare that the work in this Research project has not been previously published or submitted elsewhere for award of a degree. I also declare that this my own original work and contains no material written of published by other people except where due reference is made and author duly acknowledged.

NAME: JOHN MBAABU MARETE

REGNO: MSc. 11/02984

SIGN _____

DATE 2ND NOV. 2013

I do hereby confirm that I have examined the master's Research project of **JOHN MBAABU MARETE** AND have certified that all revisions that the Research project panel and examiners recommended have been adequately addressed.

PROF. PATRICK OGAO SIGNATURE _____ DATE _____

Research Supervisor

ABSTRACT

In today's technology many institutions and business communities have embrace computer network connections to facilitate communication and sharing of available resources as means of exchanging electronic information locally and externally with other network. Wireless devices in a network are used to detect any intrusion and director types used for checking effect of attack (**Carl, 2004**). Network security devices/software like snort, firewall etc. are installed as the first step of securing networks after the implementation of any network. Snort IDS is a security tool and an intrusion detection system, capable of performing network real-time data traffic analysis and also data packet logs on IP networks (**Caruso, 2007**). Snort IDS software uses defined rules and policies to check each packet reaching to its network interface card in any connection.

Despite the usage of this software in security the network there are a lot of intrusion and attack into private networks even with the implementation security tools. Organizations, institutions and other network implementers therefore are not certain that their networks are truly protected due to external attacks and intrusions subject to them. Implementation of firewall and snort software will help to monitor, detect, observe and examine and report any intrusion and attack to the network either known or unknown attacks. To achieve this, a framework implementation of Wireless Network in Intrusion Detection system (WIDS) within network perimeter to examine SNORT operation in detecting any attack and intrusion is used. The technology which can be implemented here is WIDS used for detecting inappropriate, incorrect, or anomalies activity on a network. WIDS are suitable for any types of organization for protecting the networks and associated devices systems.

The main objective for this research writing is to examine snort operations using intrusion detection systems (IDS). **Judy (2002)**, IDS identifies any attacks and protects the system against attack, threats, misuse and Denial of Service in computer network. The framework developed will examine the IDS software operations to monitor any anomalies within the network. To achieve this objective, IDS will be implemented on a network to examine its operations to determine their shortcomings in protecting the network.

TABLE OF CONTENT

DECLARATION.....	i
ABSTRACT	ii
DEDICATION	vi
LIST OF FIGURES	vii
LIST OF TABLES	viii
LIST OF ACRONYMS	ix
CHAPTER ONE.....	1
1.1 INTRODUCTION	1
1.2 Background.....	2
1.3 Problem Statement.....	2
1.3.1 Justification.....	3
1.4 Aim of the study	4
1.4.1 General objectives.	4
1.4.2 Specific Objectives	4
1.5 Scope of the Project.....	4
1.6 Significance of the Project.....	4
1.7 Project Limitation.....	5
1.8 Assumption.....	5
CHAPTER TWO.....	7
LITERATURE REVIEW	7
2.0 SNORT	7
2.1 Snort Requirement.....	9
2.1.1 The functional requirements	9
2.1.2 Non-functional requirements	9
2.1.3 Snort Advantages in wireless network	9
2.1.4 Required Software	9
2.1.5 IDSs approaches for event analysis	12
2.3 Snort Architecture	13
2.3.1 Five Components of Snort.....	14
2.4 Snort data flow	15
2.5 Discussion.....	15
2.5.1 Benefits of snort.....	15
2.5.2 Snort Disadvantages Lawton (2002)	16
2.5.3 Challenges with snort	16

2.5.4 How the Snort works with Network packets	16
2.6 SNORT	17
2.6.1 Output modes and destinations of snort.....	17
2.7 Snort rules /protocols/ characteristics/ services/ controls	18
2.7.1 Snort configuration rules	18
2.7.2 Snort protocols.....	19
2.7.2.1 Protocol Stack levels	19
2.7.3 Characteristics	20
2.7.4 Network service.....	20
2.7.5 Snort controls.....	21
2.8 Types of snort.....	21
2.8.1 SnoGE.....	21
2.8.2 Pulled Pork	21
2.8.3 PE Sig	21
2.8.4 DumbPig.....	21
2.9 FIREWALL	22
2.9.1 How firewall works	23
2.9.2 Benefits of Firewall	24
2.9.3 Limitation of Firewall.....	24
2.9.4 Firewalls in Network Security	25
2.9.5 Shortcomings of Intrusion Detection.....	25
CHAPTER THREE	26
METHODOLOGY	26
3.0 Introduction	26
3.1 Problem identification	26
3.2 Snort security evaluation	26
3.2.1 Snort security	27
3.2.2 Snort design	27
3.2.3 Snort database/information.....	27
3.2.4 Testing snort intrusion penetrations.	27
3.2.3 Testing snort basis principles:	27
3.2.4 Snort intrusion verification:.....	28
3.3 WIDS Simulation design and configuration models.	28
3.3.1 Implementation phase.....	28
3.3.2 Discussion.....	29
3.4 Validity and reliability.....	29
3.5 Result Analysis and evaluation.....	30

CHAPTER FOUR	31
4.0 IMPLEMENTATION AND CONFIGURATION	31
4.1 Introduction	31
4.2 Framework Design, Development and Implementation	31
4.2.1 Discussion.....	32
4.2.2 Algorithm for Examining intrusion detection using IDSs	32
4.2.3 Role of NIDS in Combating Attack.....	33
4.3.1 Types of Router	34
4.3.2 Types of Switches	35
4.3.3 Sensors.....	35
4.3.4 Master sensor.....	35
4.3.5 Discussion.....	36
CHAPTER FIVE	37
TESTING AND EVALUATION	37
5.1 Introduction	37
5.2 Methods of attack and facilities.....	37
5.3 Framework Validation.....	37
5.3.1 Snort intrusion detection classification rules.....	37
5.4 .0 Discussion of results.....	38
5.4 .1 Experiment one.....	38
5.4 Backdoor.....	39
5.4.1 Results Analysis	39
5.4.2 Experiment 2	40
5.4.2 Results Analysis	40
CHAPTER SIX	42
CONCLUSION AND RECOMMENDATIONS	42
6.1 Introduction	42
6.2 Findings.....	43
6.3 Conclusion.....	43
6.4 Recommendations	44
6.5 Future Work.....	44
6.6 References	45

DEDICATION

Much gratitude goes to my lovely and supportive wife who ensured assistance throughout the entire proposal writing process, to my mum for her finances and support and lastly the deep affections from my son Junior. Finally, much of praises to the Almighty God for His strength in me, ability, provision of finances and care all through my studies.

LIST OF FIGURES

Figure 1: Placement of snort sensors

Figure 2: Classification of Intrusion Detection System

Figure 3: HIDS with agent's console

Figure 4: Snort Architecture

Figure 5: Components of snort

Figure 6: Data flow diagram for snort

Figure 7: Snort Rules

Figure 8: Architectural layers of a WSN

Figure 9: Conceptual model used in Intrusion Detection

Figure 10: IDS Block diagram

Figure 11: Implementation model

Figure 12: NIDS Deployment model

Figure 13: Snort server sample Alerts

Figure 14: Discussion of results

Figure 15: Snort Console

Figure 16: Ping of Death

LIST OF TABLES

Table 1: Possible outcomes of IDS

Table 2: Snort rules

Table 3: Shortcomings for IDS

Table 4: Algorithm for examining intrusion detection

Table 5: Snort defaults classification source

LIST OF ACRONYMS

IDS – Intrusion Detection System

NIDS – Network Intrusion Detection System

WNIDS- Wireless Network Intrusion Detection System

SMB – Server Message Block

TCP- Transmission Control Protocol

CGI- Common Gateway Interface

WSN- Wireless Sensor Network

DS – Detection system

SYSLOG- system log

PCRE - Perl Compatible Regular Expressions

HTTP – Hypertext Transfer Protocol

HIDS: Host Intrusion Detection System

NIDS: Network Intrusion Detection System

DoS: Denial of Service Attack

DDoS: Distributed Denial of Service Attack

ICMP: Internet Control Message Protocol

POD: Ping of Death Attack

CHAPTER ONE

1.1 INTRODUCTION

With the development of new network technologies and applications, network attacks are greatly increasing both in number and severity on private network. Every enterprise using communication devices nowadays it is very important to maintain a high level degree security to ensure safe and trusted communication within and outside the organization. These organizations are not sure of their data security on intrusions from un trusted public network. Intrusion detection is of significant in many applications in detecting malicious or unexpected intruder(s) into the private network (Wang 2013).

The purpose of data security in a network is to secure it from external network intrusion that leads to anomalies within the network communication. Network Intrusion detection systems contain essential components used for securing network through detects these attacks before they widespread and damage the internal networks. Richard, 2000). Intrusion Detection System plays vital roles in detecting different kinds of attacks and securing the internal networks.

An intrusion into a network is any successful violation of a network's security set policy that is already in place (Zhou *et al.*, 2005) [26]. Intrusion detection tools are used to address any problems that are associated with the DoS attacks such as death of Ping, flood attack, SYN attacks, smurf attack etc. NIDS software are used to detect, identify, assesses and report authorized/unauthorized traffic and approved network activities so that appropriate measures can be put into place to prevent and detect any damage on the private network (Abdelhalim, 2010). The Network Intrusion Detection System (NIDS) such as snort or firewall software are used to keep track of IDS functionality and effectiveness based on IDS policies and rules set for network security implementation.

1.2 Background

The intrusion detection systems are used to be able to detect and prevent any intrusion or attacks from untrusted network. Several intrusion detection tools are used to monitor network operations based on set rules and policies.

Akinwale (2004) Snort Intrusion Detection Systems are systems that have the ability capability and to detect any intrusion from both private and public network on computer data and undertake appropriate measures to eliminate them. These tools include Snort, firewall, suricata, BASE, Nice, Sguil, which are used to detect and prevent any network intrusion in most cases denial of service to legitimate users.

The framework examines the snort IDS which is a free open source network intrusion detection and prevention system, developed by Martin Roesch (1998). Firewall and Snort IDS runs on windows and linux implementation environment. Through the use of protocol analysis, data content searching, and various pre-processors devices IDS can detect thousands of worms, port scans, vulnerability, exploit attempts and other suspicious behavior on the network from other networks.

1.3 Problem Statement

Any anomaly intrusion detection system are important in current network security framework but network security devices are still unable to detect high rate of false alarms triggered off by both external and internal attackers.

Wireless networks still pose a number of unresolved challenges and optimization problems in setting of Network security measures like rules and policies that governs the intrusion detection. Also network administrators have not yet implemented proper control necessary to secure networks from any external attacks. Internal networks also face a lot of insecurity threats from public attacks through intrusion and attacks. The research study investigate problems faced by a snort IDS as per set rules and policies in securing the network

1.3.1 Justification

With rapidly growing of unauthorized activities networks, intrusion detection systems as a component of defense- in-depth usage are very necessary because past IDS firewall techniques used cannot provide complete protection against many intrusions (Kobayashi, 2003).

Any network either wired or wireless computer network are all subject to various threats such as attacks from unauthorized access through a given access point either internally or externally this includes virus, worms etc. Intrusion detection systems have become essential key components for computer security is to detecting these attacks before they inflict widespread damage on our network resources (Richard, 2000).

Therefore the main focus relies on the implementation of snort security software that are used to access any data in a given access point to monitor any access to the network from different public network users, thus the implementation of IDS will enable administrators to detect and block any entry of either worms, virus or any form of attack and intrusions.

Intrusion-detection systems are used to monitor the usage of such systems and to detect the insecurity states on a network. Network IDS detect attempts and active misuse by legitimate users of the network systems or external parties to abuse of user privileges or exploit security vulnerabilities of a given network (Herve, 1999).

Snort IDS system was chosen because excellent similar performance and functionality as compared to other commercial IDS solutions, and no other open source IDS comes close to Snort in functionality during detecting unknown attack and the firewall in detection of known intrusion. Another significant of using Snort is large number add on products that can be used to expand its functionality and functionality

1.4 Aim of the study

1.4.1 General objectives.

- i. To develop a framework for detecting any wireless network intrusion using IDSs in securing wireless networks.

1.4.2 Specific Objectives

- i. To investigate the existing frameworks for wireless network Intrusion Detection systems.
- ii. To examine snort operations in detecting any intrusion in the wireless network and documenting the outcomes.
- iii. To design and implement a Framework for Examining IDS operations and its functional requirements in detecting network attacks.
- iv. To test and validate the framework for detecting intrusion in Wireless Network.

1.5 Scope of the Project

The main scope is snort IDS implementation plan that would be to install the security solution in a test network environment, test the rules and policies data filters and then implement the solution in real life situation like in distributed wireless network.

1.6 Significance of the Project

The study and the tool developed shall have a lot of benefits in securing wireless networks by the use of IDS that will help in detecting any intrusion or any attacks to private internal networks from public network attack. The snort software will be implemented within the private network of organization or institution to facilitate monitoring, detection, analyzing and reporting any anomalies within the network through a common access point to the network administrator.

1.7 Project Limitation

In order to undertake the successful implementation of the project I shall require to overcoming some challenges/ limitations that may derail successful implementation of the framework. These include:

1. Knowledge

In the design, development, implementation, monitoring and managing the network security using the security tools requires sufficient knowledge and skill which might be a challenge.

2. Amount of traffic flow

Another problem is associated this IDS tool implementation is the capability of holding a lot of data traffic (in megabyte) that maybe transmitted from the public network to the private network at a given period of time may overwhelm the IDS result to over logging the system.

3. Efficiency of the intrusion detection system processing is also a challenge.

The efficiency of intrusion detection will be determined by the flow of network data traffic so that effectively facilitate the device ability to accurately examine the various operations of snort in intrusion detect making sure that no data packets are lost during transmission time.

1.8 Assumption

The assumption of Intrusion detection systems are based on the fact that the intrusion detection software snort will continue functioning for a specific period of time. And at the same time some attack will be sent or introduced to the private network so that any anomalies will be detected and alert communicated to the network administrator server at that time.

1.9 Definition of Terms

1. Security-refers to safeguarding the computer network data and other related facilitates against any unauthorized access or usage.

2. Sensor- is a hardware device that produces a measurable response signal to a change in a physical condition.
3. IDS- refer to a mechanism that monitors network or system activities for malicious activities or rule and policy violations and produces reports to a management server station.
4. FIREWALL-software that filters incoming traffic and protects the resources of a private network from users from other networks.
5. ATTACK- is any attempt by illegitimate user to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of network device.
6. INTRUSION- is any attempt to make unauthorized access abuse or make unauthorized use of a network resource.
7. A network intrusion detection system (NIDS) - is an intrusion detection system that tries to detect malicious activity on a network resource.
8. Snort: an open source IDS tool which uses rule-based language combining signature, protocol and anomaly inspection methods.
9. A packet sniffer – tool used to capture and display packets from the network with different levels of detail on the console showing various logs and alerts.
10. Packet Decoder- tools that takes packets from different types of network interfaces and decode them.
11. Signatures pattern used inside a data packet and it is used to detect one or multiple types of attacks on a network.
12. Alerts are any sort of user notification of an intruder activity on a network.
13. Log -are messages usually saved in file in network database system.
14. False Alarms - refers are alerts generated due to an indication that is an intruder activity.

CHAPTER TWO

LITERATURE REVIEW

2.0 SNORT

Snort IDS is network an open source security software tool which runs over any networks it analyses all real-time incoming data traffic for detection of any misuses, intrusion and attacks. Snort security software is a network security tool used for intrusion detection system, which have capability of conducting network data traffic analysis and packet logs within networks from public network (Caruso, 2007). Snort IDS performs network protocol analysis, data examination content, matching and detect a variety of intrusion attacks and probes, such as port scans, Dos, CGI attacks, SMB probes etc. (Vyatka, 2011). A firewall software on other hand is a security software used to filter and control data traffic into or outside a private network during transmission, (Gouda and Liu, 2002) [9].

Snort security software Components are logically divided into various components which work together to detect various network attacks and generates output in a required format from the security software. Snort component includes packet decoder, processors, detection engine, logging, alerting system and output modules architecture for detecting any intrusion (Vyatka, 2011).

Intrusion Detection Systems (IDS) eg snort and firewall technologies in computer security domain that identifies, detect and prevent any anomalies into a network computer networks. Snort ids is supported by several network systems due to it flexible configuration, network user online support, snort cost, cross platform implementation, performance and functionality etc. IDSs are Snort installed on a network to identify various attacks and to react by usually generating an alert or blocking suspicious activity to the legitimate users.

Snort IDS is the real time data packet analyser and packet logger used to perform network packet payload inspection through data packet searching and matching algorithms with the

interior of detecting any anomalies. Snort IDS has been considered as a better option to expensive and serious duty (on NIDS). This research work as focussed on analysing the effective functionality and performance of IDS under heavy network traffic conditions communicating to a central access point within the internal private network.

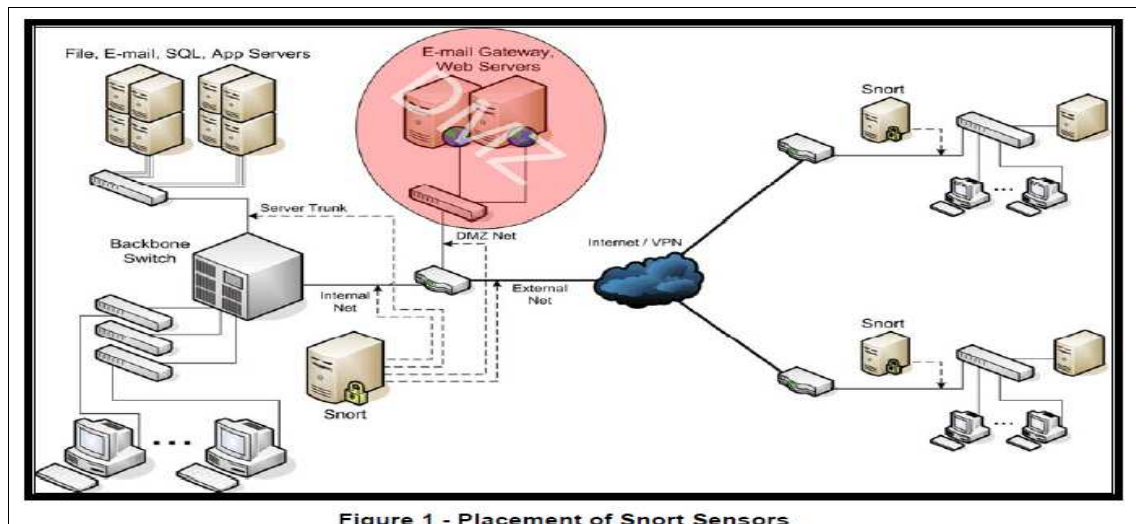


Figure 1 - Placement of Snort Sensors

Figure1. Placement of snort sensor *Source <http://www.sentnix.org>.*

(Source: Snort 2007) Snort IDS security tool should be installed in a standardized dedicated server which acts as the sensor on a given network. Snort software and firewall are used to monitor the network for any threats from public network using set rules, signatures, and pattern matching on a given traffic. Snort also checks on network log activity so that network security administrators can monitor the network. Snort generates various alerts through emails messages, pop-up windows, and SNMP traps.

Snort IDS contains flexible rules with over 2400 exploit signatures in its computer based database (Hwang *et al.*, 2003) [11].

Snort IDS software can also performs protocol analysis, content searching & matching detect a variety of attacks then check on probes such as buffer overflow, DoS, attempts from the external network .

2.1 Snort Requirement

Snort software works in both Linux and windows configurations environments. Snort software is widely used as IDS security tool with wide application documented (Hwang *et al.*, 2003) [11]. The basic snort security software configuration requirement basically classified into functional and nonfunctional requirements. (Hwang *et al.*, 2003)

2.1.1 The functional requirements

1. The snort set up is integrated with IPS to add to the effectiveness implementation of the IDS. It can use snort, firewalls, Virtual Private Networks (VPN) etc.
2. IDSs uses up to 256MB of (RAM) Sensors use 512MB of RAM in their applications.
3. Snort uses layer two/three switch in a segmented the network

2.1.2 Non-functional requirements

1. Requires to provision of physical security to network devices in any configuration.
2. Should have good practices on the use of networked resources like passwords.
3. Requires training students and staff on network use and security rules and policies.

2.1.3 Snort Advantages in wireless network

- i) Markedly accelerated pace of snort development models.
- ii) A vast community of security experts that continually works on snort.
- iii) Security engineers and specialists are required to work with snort.

2.1.4 Required Software

Libpcap and WinPcap are used for supporting saving captured packets to a file and receiving saved packets. They read network data traffic analyzing it, in order to matching the saved data packets to the set rules and policies.

b. PCRE

The PCRE IDS is library software open-source security programs. They are used to detect any attack on private networks.

c. Barnyard – this is an output security system used for intrusion detection in various network set up. Barnyard is reads the saved network data file, and then retransmit the traffic to a database back-end side within the network

2.1.2 Classification of IDS

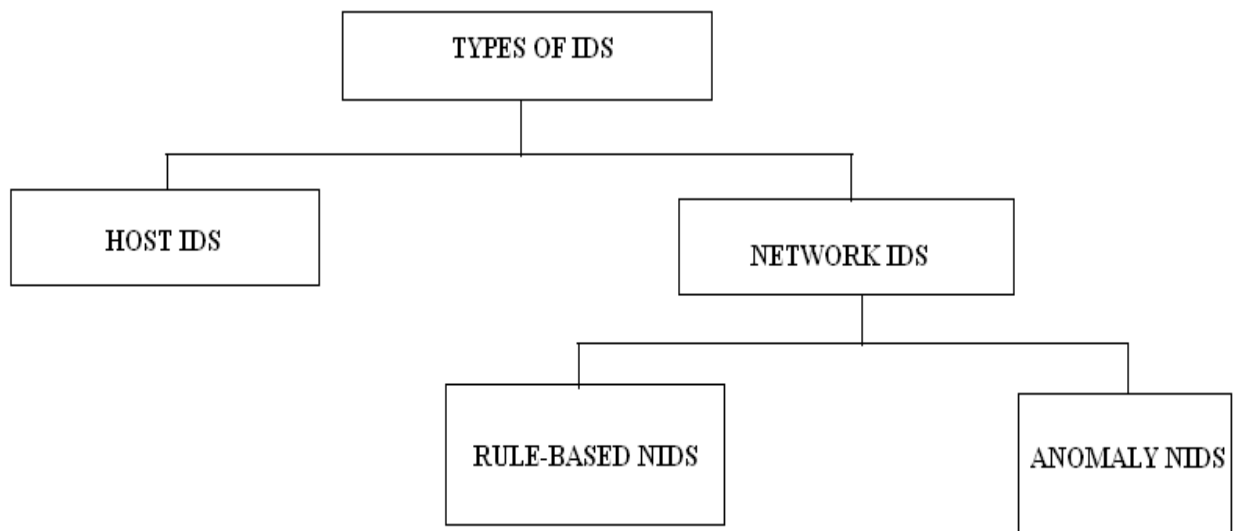


Figure 2: Classification of IDS

2.1.4.1 Network based IDS:

These are set systems used to monitoring network connecting links and associated backbones that are used that are examining all attack signatures. This involves the following:

2.1.4.2 Distributed IDS

These are networks devices functioning as remote sensors in various locations and reports to a central access point.

2.1.4.3 A gateway IDS

This refers to network device deployed between a private network and external network, with application IDSs that understands and parses various application of data traffic and uses underlying network protocol to check on any malicious attack.

2.1.4.4 A network-based IDS

Network Intrusion Detection Systems (IDS) check on various behavior and alerts on potential malicious network traffic system (Baker, 2004). The IDS system is placed on a network segment and keeps track of all incoming traffic on that private segment.

2.1.4.5 A host-based IDS

This type of ids involves installing program on individual computer systems to be monitored. This network program checks the integrity of system files within the network (Joseph *et al.*, 2003) [12]. It checks or monitors host systems within the network that the agents are installed on and do not monitor the entire network activities analysis.

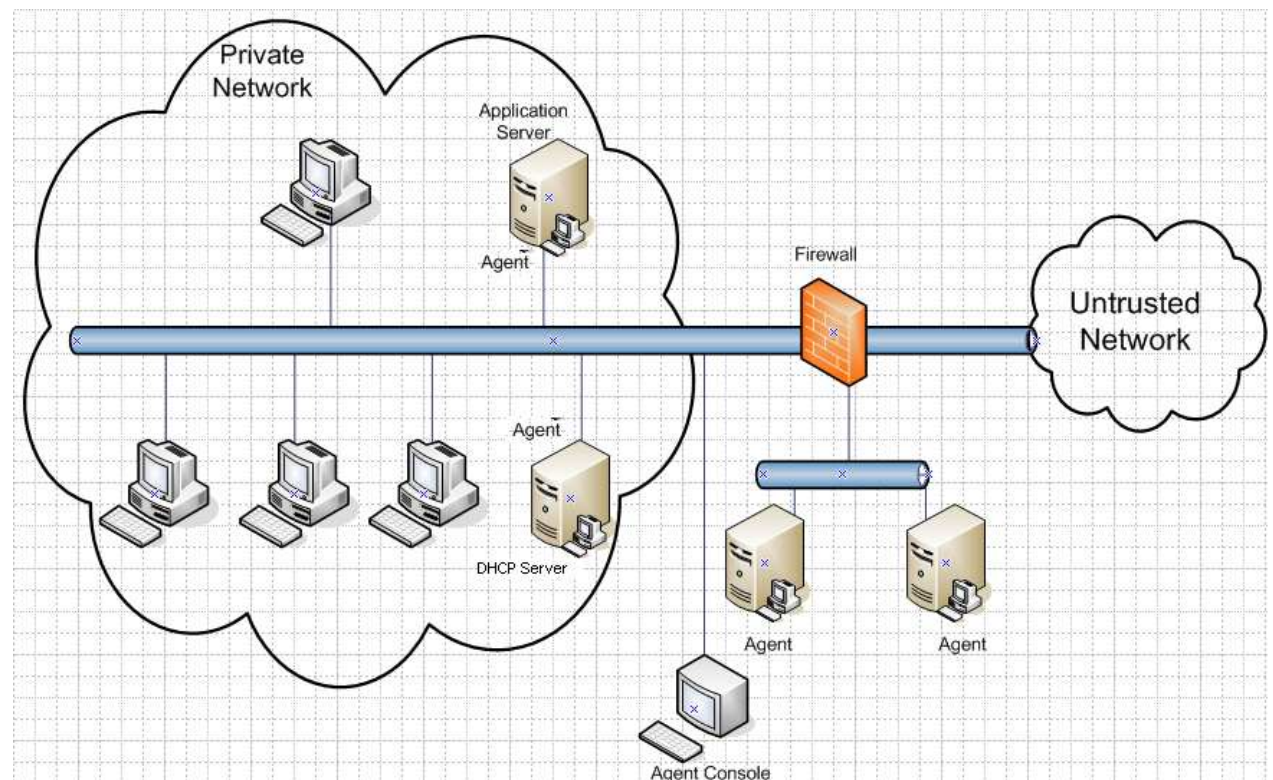


Figure 3 HIDS agent console

2.1.4.6 A knowledge-based (or signature-based) IDS

This ids is used to check the data base of system against various known vulnerabilities and any intrusions and also monitors the behaviour of IDS on security network.

2.1.4.7 A behavior-based (or statistical anomaly-based)IDS

Anomaly detection is any behavior based detection or generic intrusion detection. Model (Joseph *et al.*, 2003) [12]. The IDS are referenced to a baseline or pattern of normal system activity to clearly identify active intrusion attempts to the network. It can generate four results based on intrusion detection system which includes true positive alerts, true negative alerts, false positive alerts and false negative alerts as shown below.

	Intrusive Event	Non-intrusive Event
Intrusive Decision	True Positive	False Positive
Non-intrusive Decision (including missed events)	False Negative	True Negative

Table 1: Possible outcomes of IDS

The table above shows analysis of IDS in evaluating its effectiveness in intrusion detection.

This involves:

1. True Positive: justifies malicious events and report them to the administrator.
2. False Positive: IDS justifies a non- intrusive event as malicious and report alert.
3. False Negative: this refers to when a malicious activity is ignored by the IDS and it fails to report to administrator about it.

2.1.5 IDSs approaches for event analysis

Snort Signature Detection uses over 2400 intrusion signatures in its application database (Hwang *et al.*, 2003) [11]. In short intrusion signatures are stored in MySQL database and detect intrusion through matching incoming traffic to the LAN using the set rules and policies.

2.2 Snort configuration modes

The Snort is configured using various modes such as Sniffer mode that detect the incoming traffic, also uses the packet logger for checking incoming data packets and also network configuration IDS for checking all the associated port used for intrusion attack.

2.3 Snort Architecture

Snort IDS consists architecture packet sniffer allows an application or a hardware device that can eavesdrop on data network traffic within network. The snort ids are also used for analysing, troubleshooting, monitoring performance and analysis the network etc. In Packet sniffer, data packets are saved and processed and referenced as a packet logger. Second parties pre-processor that takes the packets and check them against set plug-ins traffic like port scan in the plug-ins are used for checking packet behaviour. Plug-ins are enabled or disabled on need basis of the administrator. Snort IDS support different kinds of pre-processors attached plug-ins, covering network used protocols. Michael (2004). In a DIDS implementation network sensors are only element of the IDS architecture that is exposed to public network.

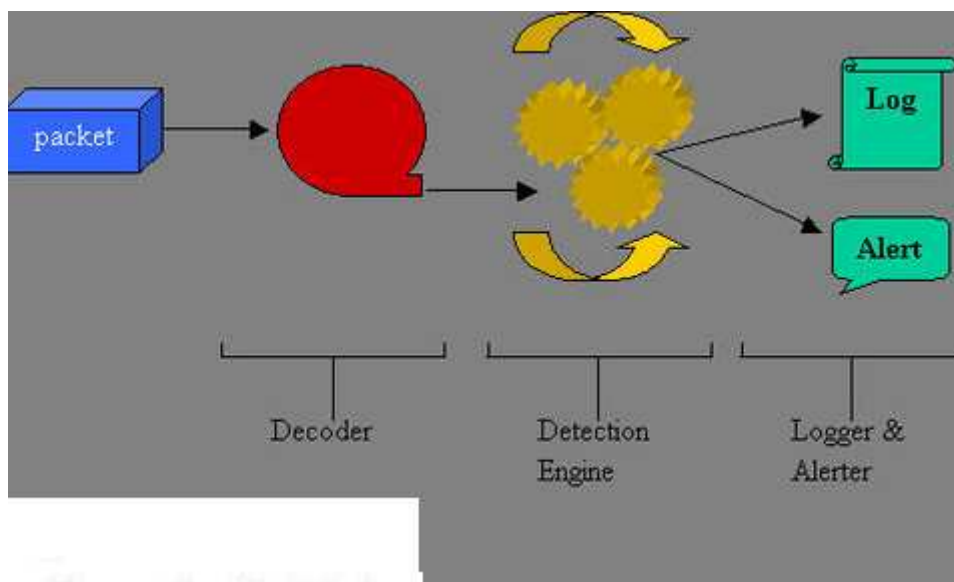


Figure 4: Snort Architecture

From: Nalneesh Gaur 2001

2.3.1 Five Components of Snort

1. A Packet Decoder- this part collects data packets incoming different network interfaces then prepares the data packets for further processing within internal network.
2. Pre-processors component is used for arranging and modifying the data packets so that they can be analysed using the third component of architecture.
3. Detection Engine –they receive the data packets that have passed through the pre-processor part. The detection engine uses the set rules and policies to check the data packets. Matching of data packets against the snort rules on the data base the alert is sent to the alert processor. Also if Snort data packets are processed matching the rules then the alert is triggered.
4. Logging and Alerting System- this part is used to generate alerts and transmit them to a common centralised main master IDS.
5. Nalneesh Gaur (2001) the output modules or plug-ins controls outgoing traffic that is produced after logging and triggering of alerts when attack access. The main function of this IDS is to generate various traffic, traps, attempts logs reports in a common database server.

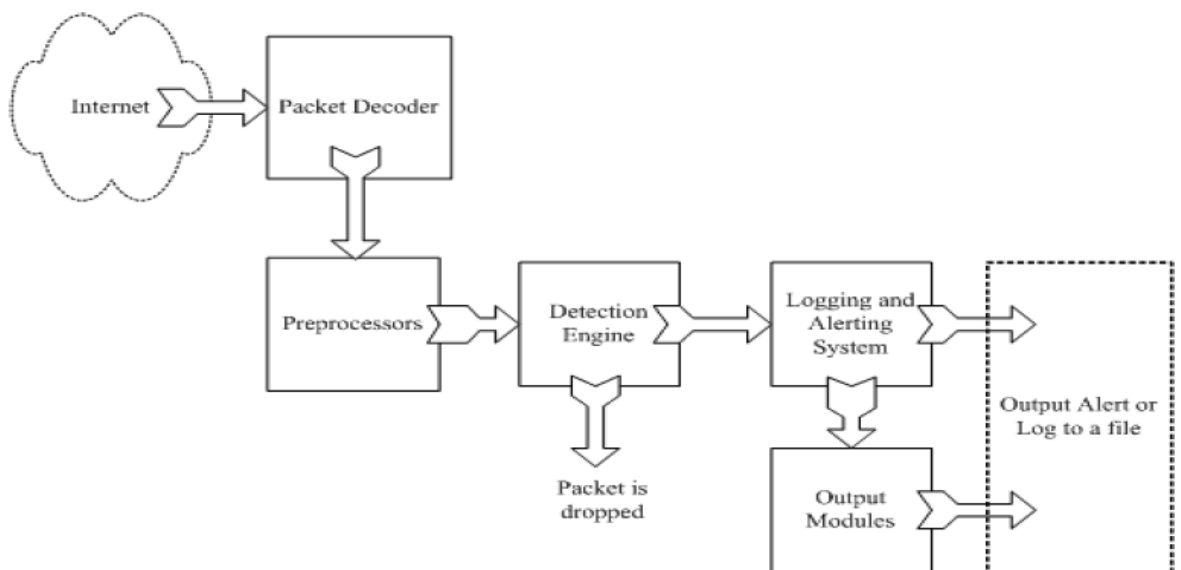


Figure 5: components of snort

2.4 Snort data flow

Intrusion Detection Systems with Snort.

In bigger organisations Snort IDS needs to be installed in different location and run in those locations in avoidance of problem of managing and maintaining bulky multiple database. All sensors are supposed to be centralised and configured in and a common data base with logs.

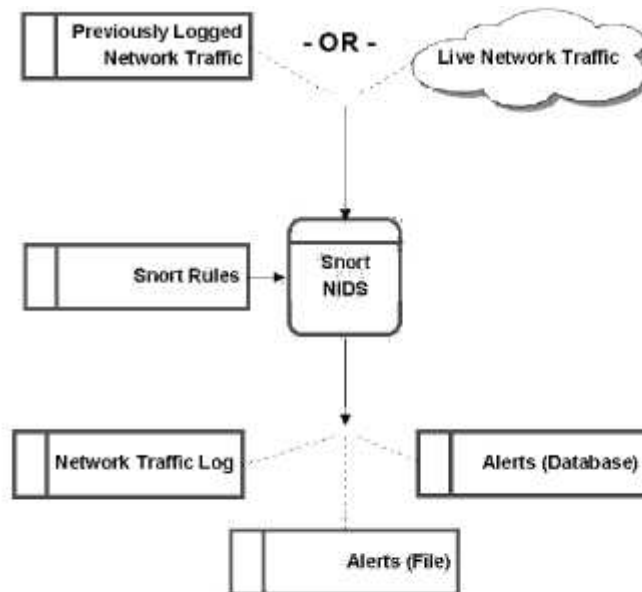


Figure 6 Data-Flow Diagram demonstrating the flexibility in utilising SNORT.

2.5 Discussion

In network sniffer mode data packets are taken to a common database for storage in main database after short configured and therefore made available to network administrator. He checks on all ports, data and time protocols, size, addresses of the frame packet used.

These snort rules and policies must be passed to snort NIDS that facilitate the detection and reporting various network anomalies and alert messages that are sends the message to the network administrator server through alert database.

2.5.1 Benefits of snort

1. File open source software.

2. Combines benefits of protocols, signature and deployed in IDS/IPS.
3. Performs protocol analysis and content or data traffic searching/matching.
4. Used to detect a variety of attacks and probes in detection of intrusion.
5. Available to all users for free.
6. Snort evaluates and fine tunes access control rules on firewalls and routers.

2.5.2 Snort Disadvantages Lawton (2002)

1. Large logs produced during capturing network packets.
2. Collecting and analysing vast log/alert is problem general.
3. The analysis console attempts to reduce the exposure of network vulnerabilities on network segments.
4. Traffic generated is about the normal network traffic captured on different nodes sending to central management server.
5. Snort is more vulnerable to vast amount of alerts, unknown attack thus detect good alert is a problem.

2.5.3 Challenges with snort

1. Misuse detection – avoid known intrusions detection.
2. Database rules grow in large volume.
3. It continues to grow to large volumes.
4. Snort spends 80% work time to do string match to other traffic data.
5. Identify new attacks in Anomaly detection
6. Probability of detection is low in detecting any attack.

2.5.4 How the Snort works with Network packets

1. Snort IDS data is gotten easily.
2. A number of data packets are sent to snort.
3. Snort receives these data packets.
4. The time between two received packets varies from sender to receiver.

2.6 SNORT

This is Network Intrusion Detection System & Packet sniffer/logger basically used for detecting any anomalies to the network to detect any intrusion.

2.6.1 Output modes and destinations of snort.

Using NIDS mode in Snort can be configured in several ways to receive outgoing traffic.

The snort logging and alerting mechanisms are to logs in decoded in ASCII format and use complete alerts. Data packets are logged as binary log files via to the switch for transmission to take place.

The four options modes are (Michel Bisson 2003)used in Snort configuration includes:-

Output Modes

- “A full” writes: for alert message and full packet headers used in data traffic.
- Fast alert which writes: timestamp, alert message, source and destination ports used by data traffic.
- A none turn off alerting for detecting the traffic.

Output destinations

- Unix socket for unsock send alert.
- Screen console for fast style alerts.
- Syslogd alert port.

2.7 Snort rules /protocols/ characteristics/ services/ controls

2.7.1 Snort configuration rules

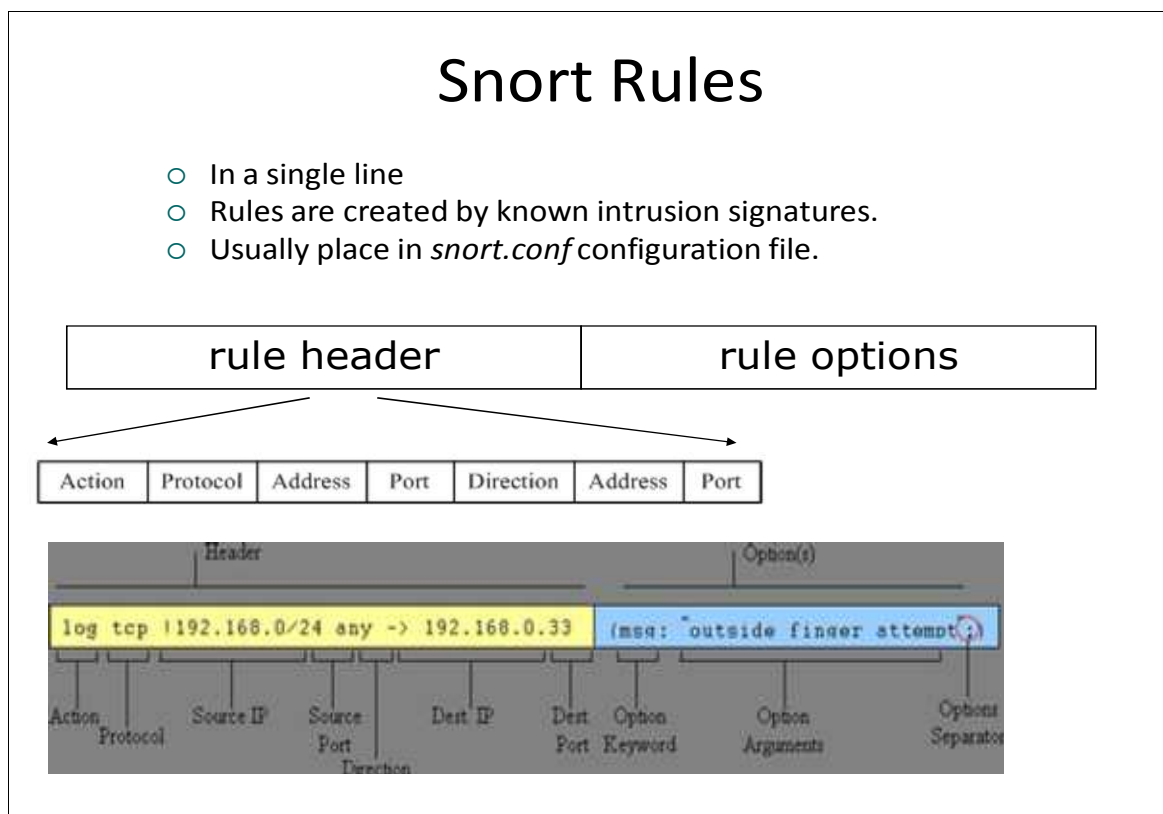


Figure 7: snort rules

Source .Snort rules by Mitchell (1997).

bad-traffic.rules	exploit.rules	scan.rules
finger.rules	ftp.rules	telnet.rules
smtp.rules	rpc.rules	rservices.rules
dos.rules	ddos.rules	dns.rules
tftp.rules	web-cgi.rules	web-coldfusion.rules
web-attacks.rules	sql.rules	x11.rules
backdoor.rules	shellcode.rules	policy.rules
virus.rules	local.rules	attack-responses.rules

Table 2: Snort rules

2.7.2 Snort protocols

Network security protocols: Sohraby (2007)

Secure shell (SSH) these are shell based protocols such as telnet, or other remote logins as well as FTPs and remote file copy protocols like RCP.

2.7.2.1 Protocol Stack levels

A simplified protocol stack for a WSN is summarized in figure below.



Figure 8: Architectural layers of a WSN

Five main levels

- a. Application layer: it defines network interface connection and a set standard of services available to application software. It enables users to interact with computer application.
- b. Transport layer: This layer provide logging and accessing system connected to the Internet or to external networks to maintain flow of data packets.
- c. Network layer: this layer is meant to determine the routing path for the data packets it chooses various route defining the source and destination ports.
- d. Data Link layer: this layer provides medium access control (MAC), multiplexing of data packets, data frameset detection on a network connection.

- e. Physical layer: this layer is responsible for providing network various data signal frequency, power selection, modulation, and data signals encryption in a network system.

2.7.3 Characteristics

The Wireless Sensor Network should Provides an application layer solution in a network.

Wireless Sensor Network uses connection-oriented service using TCP/IP protocol.

Snort IDS also uses public cryptography key in order to prove the authenticity of remote user connection to a public computer network. This system utilizes fingerprint mechanism referred to as snapshot of an individual host's uses as actual public key mechanism.

2.7.3.1 Advantages

1. Secure http sessions (HTTPS) are used to establish VoIP.
2. TCP implementation can better handle longer messages data traffic using TLS supports.

2.7.3.2 Disadvantages

1. In securing the network the server and client should support PKI features implementation.
2. All workstation and solutions can support PKI security technique because of their complex computing environments.

2.7.4 Network service

Network service includes things like data storage, data manipulation, data presentation, data communication etc, which is used implemented using various architecture based on network protocols running at the network application layer of OSI reference model.

Various network services are provided by the network server running connected workstations which can be accessed via a network by main host components running any application. This service offered on a network includes E-mailing, printing, Directory services, File sharing, Online game, Instant messaging and Network file system services are common services on local area networks.

2.7.5 Snort controls

Snort IDS controls are basically configured in order to provide both Linux/windows network environment. The Snort ids configuration first of all performs this command line `_enable_control_socket` option. After this port configuration various control sockets are controlled using the command line argument in configuration. A snort ids command control are installed alongside with snort IDS in the same bin directory during the installation phase of snort to be able to determine intrusions.

2.8 Types of snort

2.8.1 SnoGE

This refers to a Snort IDS that is used to unify various reporting tools used in detecting various processes of data packets and represents them as place-marks on an application like Google Earth.

2.8.2 Pulled Pork

This is Snort IDS software tool that uses snort rules to it is written using Perl program. It consist the following features:

1. Snort automatic rules used for file downloads
2. MD5 verification new set rules prior to downloading files
3. Also snort contains Full handling of Shared Object rules sets.
4. Stub files are used to generation snort rules
5. Snort state should have modified rule set

2.8.3 PE Sig

PE Sig is another snort tool which is written in Ruby programme that generates various signatures used by portable executable files in various program applications.

2.8.4 DumbPig

DumbPig is Snort IDS tool which is used to detect various automated bad-grammar based on snort rules for snort IDS. DumbPig basically works by parsing various set rules

in a file and reporting on fake or incorrect utilization of data traffic, detect badly formatted entries to the network, and any other alerts to the possible network performance issues.

2.9 FIREWALL

Firewall refers to security program software that is used to filter the incoming data traffic from external network or from internal network to public. It is network devices hardware associated with protecting the network resources of private network users from public networks by filtering the incoming data packets to allow or block unwanted traffic in the private network. The following model shows a conceptual framework connecting various devices that communicate with external network to the private network. The firewall checks on known intrusions and attacks using set firewall rules and policies. This tested traffic is either allowed entry or blocked from reaching the internal network. The snort IDS then is used to detect unknown attack also should perform the testing therefore allowing or denying the entry of data traffic into the private network. It also consist of central server where network administrator should monitor any intrusion or attack where set rules used. The network internal users can effectively communicate to external network. Also users computer are installed with ids to support security.

CONCEPTUAL MODEL

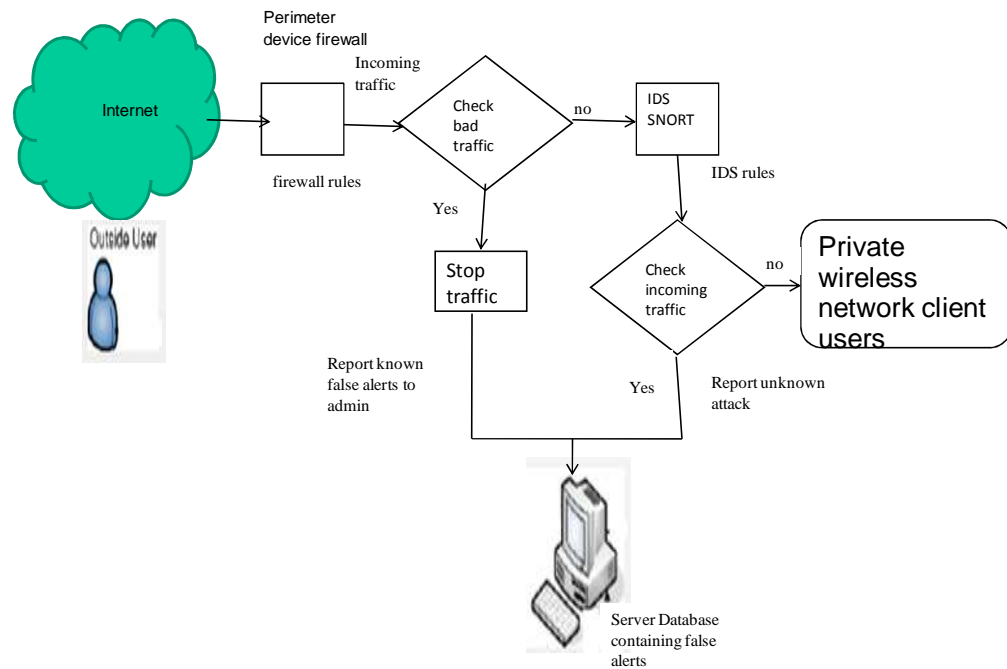


Figure 9: conceptual model used in intrusion detection.

2.9.1 How firewall works

Firewall is software installed between the private and public networks as intrusion detection software that next to router and server. Therefore, firewall examines the incoming traffic and outgoing traffic and filters the incoming data to private network. Firewall software also is able to detect and prevent any penetration or attacks un trusted networks. This device is able to stop illegitimate ingoing traffic from external network. Firewall is also able to detect any information that passes through to the private network from external network then it passes the right data packets Crothers, Tim (2003).

Firewall program/software also defines the rules for access or passing the data packet by examining bad traffic and blocking the known attack and allows the data entry to the IDS the unknown attack that passes the firewall. The snorts IDS should able to detect all unknown attack or intrusion the pass right to internal users otherwise report the intrusion to the network administrator through logs and alerts. The network administrators should be able to

protect and enforce good security policies and rules to ensure that network is secure. The purpose is to prevent occurrence of denial of services to legitimate users.

2.9.2 Benefits of Firewall

(Gouda, 2008), (Brian, 2010) and (Sheth, 2011):- Security features installed, configured and implemented to provides individual users, organizations and institutions in line their security policies interests to provides the majorly the following benefits to the entire network connections. These benefits include the following:

- i. it provides protection of internal network against external attacks using set rules and policies
- ii. It provides inspection using port states on all data packets of all data packets both on inbound and outbound traffic based communication.
- iii. The firewall operates in three layers on OSI model i.e network, transport and application layers.

2.9.3 Limitation of Firewall

However Firewalls IDS cannot provide complete protection against some attacks and intrusion coming from external network (Kobayashi, 2003). Firewalls have various limitations, such as inability to prevent or detect un known network attack from external attacks (Katkar, 2010).

Others include (Brian Komar, 2010) and (Sheth, 2011):-

- i. The firewall can't stop all anomalies in network traffic;
- ii. Firewalls software does utilize manually configured set of rules and policies on a network.
- iii. The firewall can't react to a network attack once a static policy is defined within the network (NIST 2010);
- iv. Network packets pass are that through Firewalls are only examined
- v. Firewalls have no sufficient capability to analyze network traffic.

2.9.4 Firewalls in Network Security

Firewalls IDS controls all inbound and outbound intrusion data traffic coming from the public network and private network with security rules as seen in OSI ref model. Firewalls also embrace the use of static security rules, manually configured security rules and policies that differentiate legitimate data traffic from non-legitimate data traffic coming from public network. In security implementation firewall will examine any intrusion based on network using set rules and policies to govern the network security issues.

2.9.5 Shortcomings of Intrusion Detection

	Intrusion Detection				Data Leakage		EWS
	Signature-Based Host	Signature-Based Network	Behavior-Based Host	Behavior-Based Network	Host	Network	Network
Configuration	×	×	√	√	×	×	(√)
Zero Days	×	×	√	√	⊖	⊖	√
Signature Delays	×	×	√	√	⊖	⊖	√
Bandwidth	×	×	√	(√)	√	(√)	(√)
Database Sizes	×	×	√	√	√	√	(√)
Application Layer	(√)	(√)	(√)	×	√	(√)	√
Encrypted	√	×	√	(√)	√	×	×
Communication	√	×	√	(√)	√	×	×
Targeted Attacks	×	×	(√)	(√)	⊖	⊖	×
Distributed Attacks	×	(√)	×	√	⊖	⊖	√

√ means uncritical while × shows shortcomings of the particular systems, () means restricted applicable, ⊖ stands for not applicable. Note that EWS are inherently network-based, therefore there is no column for host-based systems.

Table 3: shortcomings for IDS

: are summarized as follows

1. Complex configuration of IDS.
2. Delays for signature updates of IDS
3. There is much data Rising bandwidth and data volume in a network
4. Increases in volumes Sizes of pattern databases
5. There are frequent Application-Layer attacks
6. Encrypted network connections occur

CHAPTER THREE

METHODOLOGY

3.0 Introduction

In order to ensure security is effectively implemented to a computer network there is a need to implement various network IDS to enhance the efficient communication and sharing of resources. The implementation of wireless network involves several steps that try to solve problems associated with them the following steps.

3.1 Problem identification

The purpose of this research is to formulate information that can be gathered from various publications in order to clearly show the operations of the snort as used in wireless network. Wireless network usually faces insecurity problems due to the attacks subjected to them from public or external network. This research aims at identifying the main problem faced by individual, private and public organizations and to come up with objectives of research, scope of research identify importance of research and limitations faced in implementation of wireless network system.

3.2 Snort security evaluation

This framework gives an opportunity to audit network devices such as snort, firewall network analyser etc to quickly and efficiently to be able to monitor operational practices of these devices. The framework is used in evaluating various capability of the securing the network from external attacks and intrusion to the private network. The ids will be evaluated as per its performance and efficiency in the detection of any anomalies and sending an alert to the network-administrator

3.2.1 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 IDS details.

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

3.2.2 Snort design

This defines the architectures of running the snort that contains the firewall IDS that facilitates the detection and security issues. The firewall should be able to detect any known intrusion and snort IDS should be able to monitor unknown attack.

3.2.3 Snort database/information

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

3.2.4 Testing snort intrusion penetrations.

Test will be performed as per set rules and policies on IDS devices, the attempted intrusion 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 that covers the results of the two devices.

3.2.3 Testing snort basis principles:

The test should be based on the basic rules governing the implementation of the firewall and snort in wireless network basically check on the:

Snort security issues

- i. Confidentiality of the network data packets
- ii. Access control implemented within the network
- iii. Incoming and outgoing transmission of data packets on the network.

- iv. Availability of services to legitimate users.
- v. Functionality of the firewall and snort IDS.
- vi. Check for services availability with the network.
- vii. Should also check intruder's activity from public network.

3.2.4 Snort intrusion verification:

This is done to detect 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 logs and false alarms to private network. Therefore the firewall and snort should be able to detect any attempted attack.

3.3 WIDS Simulation design and configuration models.

An IDS can serve the purpose of confirming network security configuration and other security operation mechanisms such as snort tool. Within its limitations, the IDS is useful as one portion of a network defensive posture, but should not be relied upon as a sole means of protection.

3.3.1 Implementation phase

After design and testing of the models the WIDS is installed within the firewall and snort that communicates with internal and external network that snort is installed with WIDS software that enables detection of any intrusion from the attack. This should facilitate the operations of IDS that contains firewall and snorts to the implementation the capabilities of WIDS and Snort performance and operations in detecting any attacks and intrusions to internal network from outside network.

Implementation of Intrusion Detection system and Snort

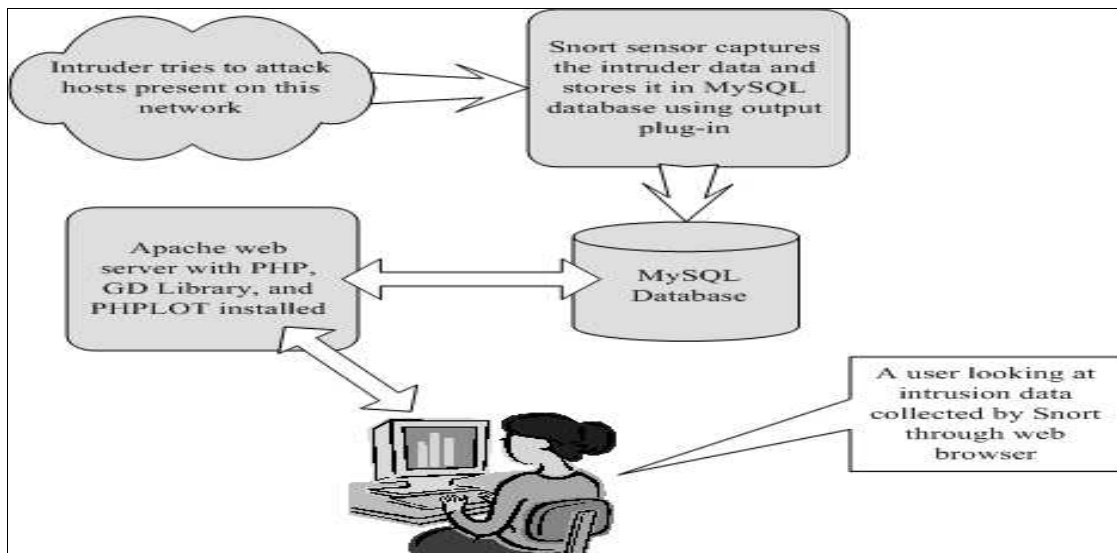


Figure 10: IDS Block diagram consisting of Snort, MySQL, Apache, ACID, PHP, GD Library applications used in setting up the implementation.

3.3.2 Discussion

Rehman (2003) in above diagram data traffic is captured and analyzed by IDS security mechanism. The IDS Snort stores this data in the MySQL database using the database output plug-in files. Apache web server application then takes the help from ACID, PHP, other packages in order to display this data in a browser window when a user connects to Apache application this displays the contents to user. Different users can then make different types of queries on the forms displayed in the web pages to analyze, and check on different application of web server traffic.

3.4 Validity and reliability

The purpose of this approach is to verify that IDS enable snort to be aware of the network environment in which it is operating in the configuration of the private network server under attack. To validate any intrusion detection system implementation, the IDS observes the reaction of the network server to a given request that is sent to it from the other networks.

According to Zhou et al., (2005) network intrusion verification method has also been used because:

1. The approach eliminates system mapping being monitored and host based verification.
2. There is a need to determine attack results analysis of the data packet header field.

This framework validity test is used to strengthen qualitative research that is used to propose whether the findings and conclusions are accurate from stance of the researcher (Creswell and John 2008).

Reliability is used for checking the performance of the IDS with the purpose of reducing errors and biases that might have occurred during research work. During validation and reliability testing one should focus on problem data collection, literature reviews, design implementation and testing different models that are used during research study.

3.5 Result Analysis and evaluation

The focus in this framework is to examine the operation of a snort in a wireless network to detect network intrusion using WIDS. Sufficient results will be gotten from how the firewall and snort designed, installed and configured in the Wireless Network that secures the network from any attack or intrusions. The snort framework 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.

CHAPTER FOUR

4.0 IMPLEMENTATION AND CONFIGURATION

4.1 Introduction

The purpose of developing this framework for detecting any intrusion into the private network from external network with the purpose of examining snort IDS operations using Wireless Network Intrusion Detection Systems internally and externally according to defined rules and policies for network implemented.

4.2 Framework Design, Development and Implementation

The intrusion detection implementation design provides a framework for the modeling of effective intrusion detection systems. Integration of intrusion detection systems with a line of intrusion prevention mechanisms will greatly improve on the network system security performance.

The WIDS framework consist the following main components router, firewall, Snort, centralised access point server, and a LAN switch providing implemented within network perimeters as shown on the figure below

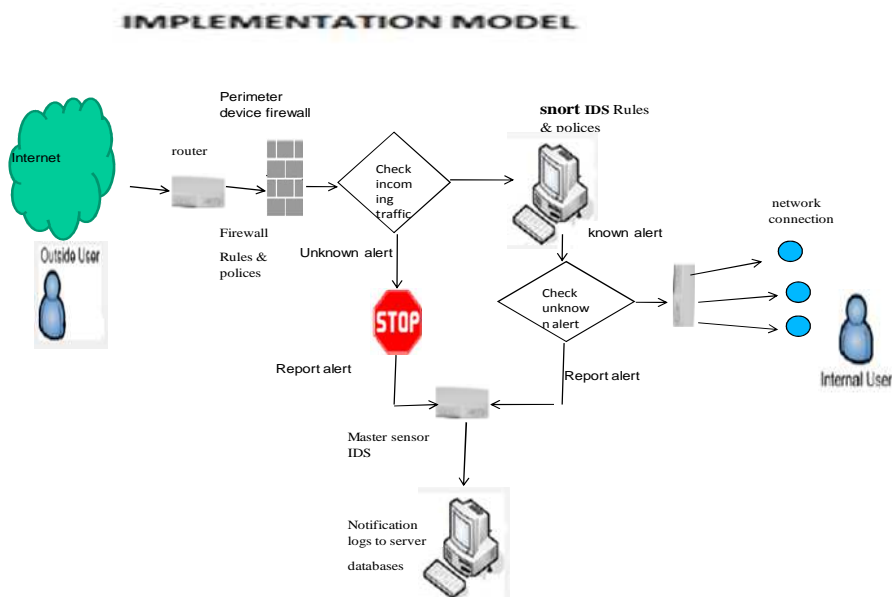


Figure 11: Implementation model

4.2.1 Discussion

The above framework developed consists of a public network that is communicating to internal organizational network LAN connecting the firewall and ids snort device using a media or a wireless connection. The firewall and snort ids are implemented and configured to keep track of network traffic checking on any intrusions and any network anomalies from public network. These devices are connected to the access point server containing snort security software to filter traffic and detect and report any attack or unauthorized materials from public networks according to the defined snort rule and policies configured on these devices.

Snort ids are implemented on a network to perform protocol analysis and content searching/matching against the stored database. Snort ids- software are used to detect a variety of attacks and probes. Firewall and Snort security software uses a various flexible rules and policies set to describe network traffic that it should be blocked or passed.

4.2.2 Algorithm for Examining intrusion detection using IDSs

In this algorithm the framework is configured to monitor the incoming data packets from public network, the system is configured to block or allow the entry of some data packet to a network like block data traffic from public network using firewall, snort security software. The wireless network intrusion detection systems are used to detect any incoming data traffic and allow or denies the access to the private network. The network intrusion detection sensors should be able to examine and detect any the incoming traffic materials associated with network IMAP traffic and block then before they reach to the private network through the snort security software.

The following table shows framework algorithm used for examining any attack associated with IMAP messages.

DATA TRAFFIC FLOW	STATUS	IF EITHER NIDS 1 OR 2		ACTION
		NIDS 1	NDIS 2	SNORT CHECK
INCOMING PACKETS	BLOCK	Alert	No alert	Ok
		Alert	Alert	ATTACK
	ALLOW	Alert	Alert	OK
		Alert	NO Alert	ATTACK
OUTGOING PACKETS	BLOCK	NO Alert	Alert	OK
		Alert	Alert	ATTACK
	ALLOW	Alert	Alert	OK
		NO Alert	Alert	ATTACK

Table 4: Algorithm for examining intrusion detection

4.2.3 Role of NIDS in Combating Attack

A NIDS can detect attacks, and different anomalous conditions, additionally they can also provide a number of key information which can be used to identify the nature of attack, its origin and propagation characteristics (Sailesh & Kumar (2003). The IDS often reports the location of the attacker or hacker (from where the attack has been triggered). However, the location is commonly expressed as an IP address, in the attack traffic also called IP address spoofing

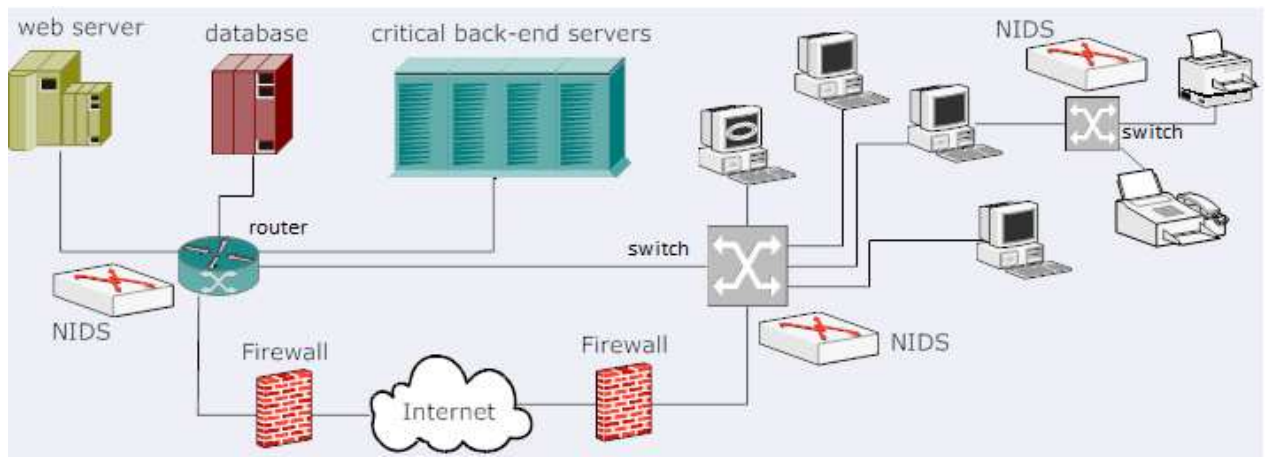


Figure 12: NIDS deployment mode Source Sailesh Kumar 2003

Sommer V. Paxson, (2003) The key aspect is to determine key source IP address reported by the NIDS and classify the attack to the network and then determine if the attack requires the reply messages or not. Attacks like DoS, flooding attack, the attacker need not only to examine the reply sent, and can easily spoof its address for a given access point.

4.3 Main Networks Devices and Configurations

4.3.1 Types of Router

A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination.

Types

1. Cisco 4400 Series Integrated Services Routers they are used for delivery of services to high-end office to promote a high-quality application
2. Cisco 3900 Series Integrated Services Routers (ISR) they deliver virtualized applications and highly secure array of WLAN connectivity at high performance that offers concurrent services at up to 375 Mbps.

3. Cisco 3800 Series integrated services routers, are used medium-sized to large branch offices for at a lower operational costs and complexities of any network operations deployment and management of the network,

4.3.2 Types of Switches

1. Unmanaged network switches used at home, in small companies and businesses
2. Managed switches are customized to enhance the functionality of a certain network.
3. Enterprise managed switches / fully managed switches.

4.3.3 Sensors

Network sensors are used to monitor the network by capturing network data packets.

4.3.4 Master sensor

Master sensor examines and analyses data packets according to rules and policies defined in them. They also confirm if snort security software truly enforces the configured rules and policies. Normal packet then it passes to the private networks, the packet reaches the destination, and packet ends the life cycle. If the packet is originating from the private networks then it is vice versa as packet originating from public networks.

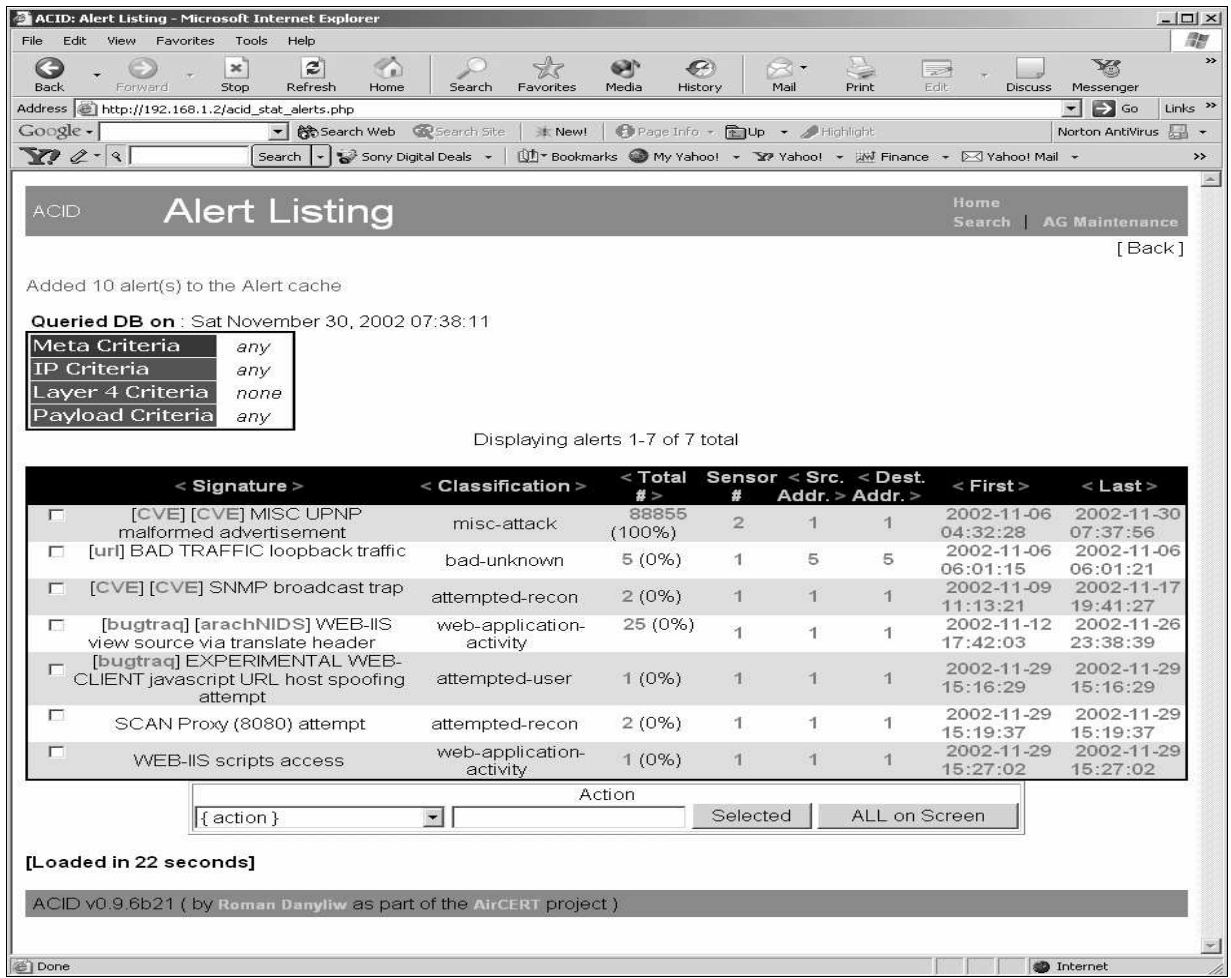


Figure 13: Snort server sample alerts

4.3.5 Discussion

Snort ids have ability to find a data pattern inside LAN data packets that are transmitted from external network to internal LANs. Newman (2002) an alert does not necessarily mean the attack identification but sensors have detected incoming traffic that is matched with signature or pattern in a network.

CHAPTER FIVE

TESTING AND EVALUATION

5.1 Introduction

Snort software is most famous open NIDS signature based software that uses alert based system to detect the suspicious activities within the network. The snort IDS alert comprises of traffic source address and destination information address alongside with signature ids and timestamp with associated protocols. In testing the snort operation different Attacks/intrusions to the network are injected to determine the intrusion detection quality of the system under different conditions. The results have identified a strong performance limitation of Snort and capability to detect any anomalies happening to the network. Snort was able to detect some anomalies but was unable to withstand few hundred mega bits per second of network traffic. This has generated queries on the performance of Snort and opened a new debate on the efficacy of open source systems. Also the snort faces the problem of emerging new intrusion attacks. Methods used include.

5.2 Methods of attack and facilities

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate/right users of a service from using that service or resources available to them.

5.3 Framework Validation

These rules are tested for experimenting and testing the snort framework implementation as follows

5.3.1 Snort intrusion detection classification rules

Classtype	Description	Priority	level
attempted-admin	Attempted Administrator Privilege Gain	High	4
attempted-user	Attempted User Privilege Gain	high	3

inappropriate-content	Inappropriate Content was Detected	high	2
policy-violation	Potential Corporate Privacy Violation	high	2
successful-admin	Successful Administrator Privilege Gain	high	3
successful-user	Successful User Privilege Gain	high	3
trojan-activity	A Network Trojan was detected	high	2
unsuccessful-user	Unsuccessful User Privilege Gain	high	3
web-application-attack	Web Application Attack	high	2
attempted-dos	Attempted Denial of Service	medium	1
network-scan	Detection of a Network Scan	low	1
not-suspicious	Not Suspicious Traffic	low	1
protocol-command-decode	Generic Protocol Command Decode	low	1
Unknown	Unknown Traffic	low	1

Table 5: Snort Default Classifications source (manual.snort.org/node31.html)

5.4 .0 Discussion of results


 NETWORK INTRUSION DETECTION SYSTEM SNORT CONSOLE											
Latest Events											
	<Sensor>	<Ssn ID>	<Signature>	<timestamp>	<srcIP>	<Sport>	<Dest. Ip>	Dport	Sbyte	Dbyte	<Attack Type>
Examine Events											
Server Management	Snort ids	104691	Snort Alert 1	2013-09-07 17:20:36	192.168.120.100	113	192.168.150.10	52	688	560	Backdoor
Client Management	Snort ids	104691	Snort Alert 2	2013-09-09 10:05:22	192.168.0.128	324	192.168.150.10	53	720	30	DOS
Report	Snort ids	104691	Snort Alert 3	2013-09-09 15:55:07	173.168.150.1	993	192.168.150.10	80	823	30	HTTP
Management Account	Snort ids	104691	Snort Alert 4	2013-09-10 08:05:22	10.1.1.66	80	192.168.150.10	79	142	23	Finger protocol
Management Log time	Snort ids	104691	Snort Alert 5	2013-09-11 13:18:36	192.168.20.100	139	192.168.150.10	139	1003	790	DDOS
Administrator Account	Snort ids	104691	Snort Alert 6	2013-09-11 17:01:50	62.10.0.100	80	192.168.150.10	21	62	60	Trojan spyware
Client User	Snort ids	104691	Snort Alert 7	2013-09-12 07:35:11	192.168.15.10	All	192.168.150.10	All	235	235	No alarm
Type of attack	Snort ids	104691	Snort Alert 8	2013-09-13 18:15:02	173.168.150.1	22	192.168.150.10	445	10	0	TCP

Figure 14 Discussion of results

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.

5.4 .1 Experiment one

This aims at examining if a snort enforces filters on incoming and outgoing spoofing and spying traffic.

5.4 Backdoor

Backdoor being executable network attack that can be used to spy and spoof the target host. After it has been installed it provides a hidden means by passing normal authentication that obtains remote access to the internal user. This software should differentiate itself to be ICQ installation program that failed during installation as security measures. After completed installation the program opens a port that allows attackers or intruders to gain network access to the internal user. The backdoor consists of two parts for the client and server implemented on a network. The server machine 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.

5.4.1 Results Analysis

From the alert.ids file it shows Remote Procedure Call an attack based on buffer overflow exploit which is classified as Misc activity with high priority which is rank as low level attacks according to WIDS snort rule based listing. The host executing the attacks host with eg IP Address 192.168.120.100 targeting host with IP Address 192.168.0.128 which in this case is mail server based application. The port being used is port 52 where the snort cannot filter the incoming data packets. 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
[Cr] [sr]	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
[Cr] [sr]	2013-09-07 17:22:00	192.168.120.10	complab	192.168.150.10	1125-56	TCP	[Snort: backdoor subseven 22]	Details
[Cr] [sr]	2013-09-07 17:56:30	192.168.120.12	complab	192.168.150.10	1125-56	TCP	DOS	Details

Figure 15: snort console

5.4.2 Experiment 2

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 this testing is used to test death of ping attack and also test whether snort has ability and capability in detecting the traffic both from internal network and public network.

The IDS tools are aimed to be installed on network servers by sending infinite data packets.

The target central application server should response to all ping packets sent to the internal network from the intruders. Configured snort rules and policies should stop this death ping

immediately as soon it appears to the firewall and snort IDS system. The command used ping

< IP target host> -t _1 65500. This command will send packet at 125kbs. The target host test is mail server with ip_address 192.168.0.128 as shown below:-



```
I:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

I:\Documents and Settings\Nacho>cd..
I:\Documents and Settings>cd..
I:\>ping 192.168.0.128 -t -l 65500

Haciendo ping a 192.168.0.128 con 65500 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
Respuesta desde 192.168.0.128: bytes=65500 tiempo=11ms TTL=128
```

Figure 16: Death ping

5.4.2 Results Analysis

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

about the status of host machine in the private network. The traffic is detected through the port 53.

The other intrusion includes the HTTP, Finger protocol, Trojan horse, virus, worms attack etc.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

Snorts are network devices which provide protection to private networks against any intrusions and attack subjected to them from external network. Therefore the IDS snort are used to monitor any network operations noting any occurrences of anomalies and reporting them based on rules and policies governing firewall and snort software uses the network intrusion detection system to facilitate its functioning.

The framework examination allows analyzing network traffic matching from external network against Snort operations by the defined rules, performing several actions, alert notification and reporting based on real time simulation and flow of data from public networks.

The framework embraces the use of set rules and policies, algorithms, signature matching and patterns implementation of within the private network.

Thus network administrators monitors IDS software operations, limitations and shortcomings can adjust snort rule and policies -set formulation and configuration to provide network capability of protection available.

The implementation of this framework facilitate the detection of the real network-based attack to the private networks therefore the snort software will be able to detect any intrusion and attack by filtering the incoming data and checking which data packets to be blocked and which to be allowed. Also it should be able to detect any weaknesses, threats and anomalies that might be subjected to the network.

6.2 Findings

Networks are always subjective to various anomalies that are sent by various user external users to gain access to internal private networks. Various attacks are sent to the internal network to gain access to the network with purpose of destroying the organization data. The research finds that un trusted network sent logs such as Backdoor attack DOS, HTTP, Finger protocol, Trojan horse, flood attacks, death of ping, smurf attack etc. all these attacks ends up destroying the internal network. Therefore the network administrator using the IDS can be able to prevent and detect such kind of attacks. With the implementation of ids the research study finds that various rules and policies can be incorporated to the security software. The IDS can be implemented to both Windows/Linux environments and implement same rules and policies governing the security features of the network. Various protocols are also set that governs the management of the network and any network login.

6.3 Conclusion

The purpose of the research was to design, develop and implement a framework for examining IDS operations in checking intrusion detection on network using wireless network intrusion detection systems that will facilitate the management of a private network guarding it against public networks. This framework focuses on the following major objectives. First, To identify the existing framework for intrusion detection systems. The second was to develop a Framework for Examining snort ids performance and functional requirement using Wireless Networks Intrusion Detection Systems.

Third was to develop and implement Framework for Examining performance and functional requirement using Wireless Networks Intrusion Detection Systems. Finally was to test and validate on reliability of the proposed framework for WS. The above objective facilitated the achievement of the snort implementation and in the private networks.

The structured methodology approached was used to design and develop the snort framework through which the following devices were used router, switches, NIDS, master

sensor, snort security software all these devices are installed between the public and private network. This framework aims at evaluating the worthiness of the framework on monitoring advantages of implementation, usefulness to protect the private network against external intrusions and related threats to the private networks.

The framework examines the snort operations using the IDS used specifically to detect real time attacks/intrusion and identify any weakness or shortcoming for the implementation of snort security software for intrusion detection.

6.4 Recommendations

The proposed framework can be used for network monitoring for any intrusion detection and reporting for such attacks since snort it can able to trace the packet details which are useful as evidence that identify that networks has been attack or intruded. The snort IDS software should be implemented with other network intrusion detection systems. Intrusion prevention systems should be implemented to be able to protect the network from any attack. Network administrators should be able to identify various security measures to be implemented to secure various networks especially from external networks. Various devices are supposed to be implemented in setting up the network. Network administrator should also be able to implement various network rules and policies that governing the network functionality.

6.5 Future Work

The research however leaves several issues on effective intrusion detection for future work, i.e. there is a need to integrate various approaches in network intrusion detection system and host intrusion detection system in a major operational devices so as to monitor the all network anomalies. The research leaves a room for future work in terms of implementing intrusion detection system into all devices used in network containing rules and policies governing network security.

6.6 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. Danyliw, Roman. 9 Oct. 2002. *ACID: Installation and Configuration*. URL: http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html Key Jun. 2003).
7. *Generation over Anomalous Internet Episodes*. *IEEE Transactions on Dependable Computing* 4(1):41-55.
8. 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)*
9. Hwang,K.,Cai,M.,Chen,Y. Qin,M. (2007). *Hybrid Intrusion Detection with Weighted Signature*
10. Joseph, S and Rod, A (2003). *Intrusion detection: methods and systems. Part II*. *Information Management and Computer Security* 11(5):222-229.

11. John, W. C., 2008. *Qualitative Inquiry and Research Design: Choosing Among Five*
12. Kobayashi, Y. B. a. H., 2003. *Intrusion detection systems: Technology and Development*.
IEEE Computer Society Press.. Nihon Univesity and Beihang University , IEEE
Computer Society Press..
13. Mahendra Pratap SinghTeam: WhitehatPeople 2004) *Intrusion Detection
System/Intrusion Prevention System (Snort)*
14. Mohammod(2012) *International Journal of Network Security & Its Applications (IJNSA)*,
Vol.4, No.2, March 2012
15. Nalneesh Gaur 2001, *Snort: Planning IDS for your enterprise*
16. 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/2002/0624security1.html>*
17. Rafeeq Ur Rehman (2007) *Intrusion Detection Systems with Snort: Advanced IDS
Techniques with Snort, Apache, MySQL, PHP, and ACID*
18. 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
19. Sailesh Kumar *Snort: Lightweight intrusion detection for networks," In Proc. 13th
Systems Administration Conference (LISA), USENIX Association, November 2003 pp
229-238. www.snort.org/*
20. Sailesh & Kumar (2003) *Intrusion detection systems using snort IDS*
21. Snort website 2007. *Intrusion detection system using snort software.*
<http://www.snort.org>

22. S. Kumar et al., "Algorithms to accelerate multiple regular expressions matching for deep packet inspection," *Proc. ACM SIGCOMM*, 2005.
portal.acm.org/citation.cfm?id=1159952
23. Tripti Sharma, Khomlal Sinha (2011) *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249 – 8958, Volume-1, Issue-2, December 2011
24. Vyatta,., 2011. *Intrusion Prevention System Web Filtering*, US and Canada: VYATTA, INC.
25. William, R. C. S. M. B. A. D. R., 2003. *Firewalls and Internet Security: . s.l.:Repelling the Wily Hacker by Addison-Wesley. Judy 2002 ids*
26. Zhou, J., Carlson, A and Bishop, M (2005). *Verify Results of Network Intrusion Alerts Using Lightweight Protocol Analysis: Proceedings of the 21st Annual Computer Security and Applications Conference(ACSAC 2005)*