IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NETWORK INTRUSION DETECTION SYSTEM

[1]MOGAL ABDUL RAHEEM, [2]D MURALI

[1]Research Scholar, [2]Associate Professor

[1]Computer Network,

[1]Quba College of Engineering and Technology, Nellore, Andhra Pradesh, India

Abstract : - This report discusses the research done on the chosen topic, which is Network Intrusion Detection System. This project shows that monitoring and detection of the network will reduce the down time of the network and reducing future attacks. In addition, a comprehensive and organized analysis is conducted to verify the causes of the attack. It has been found that most household internet user lacks the means to strengthen their internet connection or networking system. The problem of this project is an unauthorized access into a home networking system that may cause harm by stealing private and confidential information as firewall and anti-virus won't be sufficient against a determine attacker. The scope for this project is to develop an intrusion detection system that will improve the security of home network as that is the potential user of this system. The objective of this project is to investigate the methods needed to detect any unauthorized access into a home networking system. The detection system will use an open source system that are readily available but will be tuned for the usage of home user and based on Windows operating system. The literature review component talks about all the research that has being done prior to the pre-development and post-development of the project. All about intrusion detection and prevention system and its research are further discussed in detail. In methodology section, it will discuss regarding the usage of Iteration Development Model as the methodology used in developing this project. In the results and discussions section, the preliminary findings consist of the findings from literature review research, own research and the use case diagrams of the system. Then, the prototype development process and results together with the testing results will be discussed in detail. All the justifications are made clearly. In the recommendations section, all the related recommendations and some improvements that can be done for the future of this project are listed and elaborated. The conclusion section concludes the overall project. The project phases are also being discussed in detail. The project will focus on developing a network intrusion detection system for Windows-based operating system.

Index Terms – Intrusion, anti-theft system, home security, network security

I. Introduction

1.1.Background of study

Almost all of the people use the internet to carryout essential activities such as bill payment, bank transfer and etc. But attacks towards home network are not uncommon nowadays as everybody is connected to each other through the internet and the attack has been growing more frequent and severe. When an attack do occur, it is essential that a comprehensive and organized analysis is conducted to verify the causes of the attack and the damages of the attack. A thorough and timely investigation and response can serve to minimize network downtime and ensure that critical business systems are maintained in full operation.

The level of connectivity worldwide has provided opportunities for cybercriminals who make a living breaking into networks, as well as amateur hackers who have too much time on their hands. The determined hacker can find a way into your network either by establishing some type of connection and entering your virtual "front door" or by using social engineering tactics to obtain user ID and password information. Whatever the method used, the fact is that an intruder can get into your network and harm your business.

Problem Statement

The problem statement of this project is:

- An unauthorized access into a home networking system.

Firewall and anti-virus won't be enough against any intrusion. Without a good detection system, a computer network will be access by an unauthorized individual. This individual may do harm to others by stealing other people's data not to mention confidential information would be compromise. A Denial of Service (DoS) attacks may also occur.

Objectives

The objectives of this project are:

- To monitor the traffic flow for any malicious activities of a network in real-time.
- To prevent abuse or overload from bandwidth and Denial of Service(DoS)attacks.
- To develop an intrusion detection system for Windows-based operating system.

The rapid advancement of technology gave us information in an instance. Network connection is vital in personal usage as with this connection we may gain an extra edge in knowledge information. With this advancement come a few problems such as spam, virus and etc. Therefore, a solution is needed to prevent those attacks before it happens.

Intrusion can occur internally or externally. An internal intrusion is an intrusion from within own networking system. They have an access to the networking system. It may be a friend, partner, employee, or even disgruntled client. External intrusion as it sounds is an intrusion from outside of the network system. Also known as attack from the internet.

Network-based intrusion detection places sensors inside a private network, between routers or a switch. This breaks up a network into multiple smaller networks. The sensors test programs at the network level, and the sensors recognize the activity of the program as normal or abnormal, based on existing comparison parameters. The sensor determines if the program is from outside the network, and how to treat it if it is. Educatinghouseholdinternetuseronthebenefitofhavinganintrusiondetectionsystem on top of firewall and antivirus.

II. LITERATURE REVIEW

Types of Network Intrusion Detection System

Stated by (Kazienko & Dorosz, 2003), an Intrusion Detection System is a defense mechanism, which detects hostile activities in a network. System will be compromise if the intrusion is not detected and possible prevented. One of the major benefits of intrusion detection system is it provides an overview of any unusual unscrupulous activities. According to (Amoroso, 1999), intrusion detection is "a process of identifying and responding to malicious activity targeted at computing and networking resources".

Even though there are firewall and antivirus programs installed to protect their computer from any unwanted access, it can still be vulnerable to any unauthorized user. With the inclusion of network intrusion detection and prevention system, there will be another protection layer against potential hackers.

Intrusion detection and prevention systems are much more secure than common firewall technology. Although considered to be an expansion of the original intrusion detection system, they are actually more a way of controlling who has access to a computer network. They not only control access, but also detect entry to the network, so the two systems are closely linked.

Outsourced Decryption in ABE Systems: Green et al. introduced the concept of outsourced decryption in ABE systems. This involves outsourcing complex decryption operations to a cloud server, leaving only one exponentiation operation for a user to recover the plaintext.

Online/Offline ABE: Hohenberger and Waters proposed online/offline ABE, dividing the algorithm into two phases. The offline phase involves most encryption computations before knowing attributes/access control policies, generating an intermediate ciphertext. The online phase assembles the ABE ciphertext with the intermediate ciphertext after finalizing attributes/access control policies.

The reason why an attack from the inside hurts more is that the insider (attacker) will take advantage of trust and physical access as resources on the local area network of the company are deemed trusted. Practically, we do not firmly restrict their activities because an attempt to control these trusted users too closely will impede the free flow of business. With the increasing numbers of internal intrusion in the industry and tougher regulatory and compliance requirements, organizations are facing tough challenges to protect both their sensitive data against internal threats and meet regulatory and compliance requirements.

Statistics from(Magalhaes,2003):

- Almost 90% of interconnected networks that use Intrusion Detection Systems detected computer security breaches in the last 12 months, even though there are several firewalls installed.
- The Computer Security Institute, on 4/7/02, reported that 80% reported financial losses in excess of $455M caused by intrusion and malicious acts thereafter.
- Millions of jobs have been affected because of intrusion.
- Only 0.1% of companies are spending the appropriate budget on Intrusion Detection Systems.
- Intrusion Detection System are mostly mistaken as a firewall or its substitute.
- By using Intrusion Detection System will act as an additional barrier on top of an antivirus. Most organisations using antivirus software do not use IDS.

Network Intrusion Detection System

Intrusion Detection System monitors all incoming and outgoing network activity and distinguishing weird patterns that show an attempt to break into the network. ID Scan serve to confirm secure configuration and operation of other security mechanisms such as firewalls.

(Rozenblum,2001)Mentions some of the intrusion detection system functions:

- Monitoring and analyzing both user and system activities.
- Analyzing system configurations and vulnerabilities.
- Assessing system and file integrity.
- Ability to recognize patterns typical of attacks by using signature or rules.
- Analysis of any abnormal network activity patterns.
- Tracking for any policy violations.

By identifying your network topology and its incoming points, Intrusion Detection sensors may be installed and configured to report to a central management console. An administrator would review the logs, manage the sensors and update the signatures.

III. PROJECT WORK

Project Methodology

The methodology for the project delivery involved discussions between the developer and the client. The process or procedure used during the research and development phase was determined through collaborative conversations between the two parties. The methodology used in this project is iterative development model. All phases in System Development Life Cycle are included in iterative development. Phases in iterative development model are:

- Planning–To plan what is needed to bed one to make sure this system can be implemented on time.
- Analysis &Design–To determine the problem and solution.
- Implementation–To take the solution and implement it. Building the system.
- Deployment- Install the system and provide user manual, training and maintenance.
- Testing-Testing is conducted to make sure that each unit meets the user's requirement.
- Evaluation– Does the system follow the standards given?

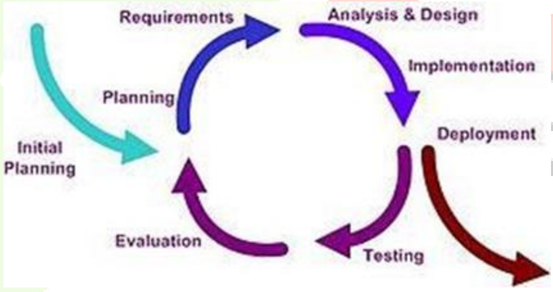


Figure1: Iteration Development Model

Below are the project activities involved in developing a Network Intrusion Detection System:

- Planning is conducted during the early stages to determine the purpose of the system and the needs of the potential user.
- Design of the system was done after the requirements have been identified by the developer based on the planning stage.
- Construction (implementation) of the system was made with code from the design stage.
- Testing of the system was conducted in the testing stage to determine if the system meets the requirements gathered during the early part of the development.
- Evaluation is the stage where testing is conducted on the system based on the requirements.
- Deployment will be conducted after the system meets the requirements and if there are no additional requirements.

🟩 Process

🟥 Milestone

Table1: Gantt Chart for FYP1

o.	**ct Activities**														
	tion of Project Title	🟩	🟥												
	earch for Project Title	🟩	🟩												
	oject Title Approval		🟩												
	ission of Proposal for rch		🟩	🟥											
	riting Project Proposal		🟩	🟩											
	ubmit Proposal and Approval			🟩											
	ission of Extended osal			🟩	🟩	🟩	🟥								
	erform Literature Review esearch			🟩	🟩	🟩									
	entify Project Methodology				🟩	🟩									
	esign Project Flow and Gantt hart					🟩	🟩								
	ubmit Extended Proposal						🟩								
	osal Defence/ Progress ation						🟩	🟩	🟩	🟩	🟥				
	repare Presentation Slide						🟩	🟩	🟩	🟩					
	resent Proposal Defence										🟩				
	ission of Interim Report										🟩	🟩	🟥		
	roject Works Continue										🟩	🟩			
	ubmission of Interim Draft eport											🟩			
	nterim Report Approval												🟩		

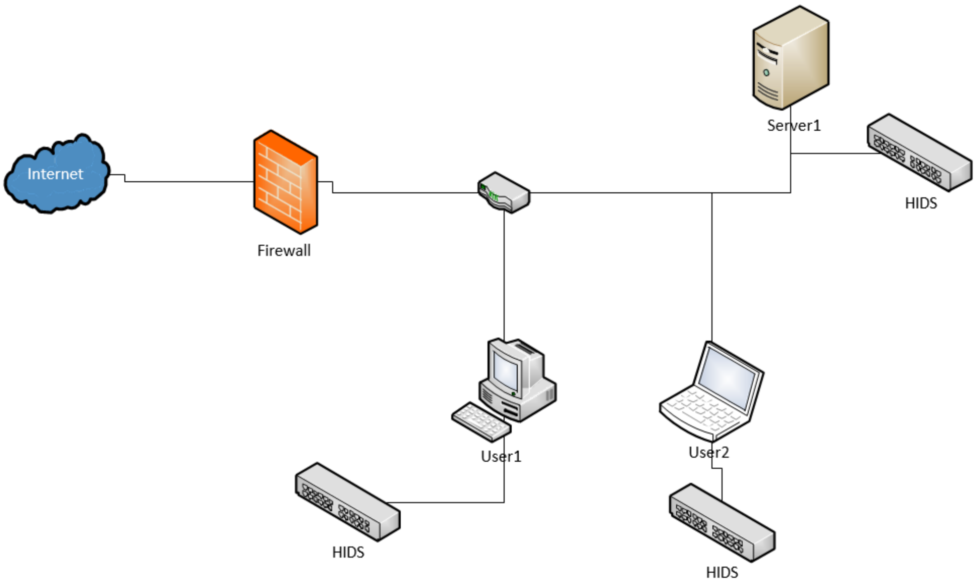


Figure2: Detailed network diagram of HIDS location

IV RESULT&DISCUSSION

Expected Feature of the System

From the literature review, it is to be known some of the feature of the system. The features are:

- Datalogging
- Real-time detection
- Installed in host/user computer. No need third party peripherals.

There are two types of detection method:

- Signature/Rule detection. The system detects known phishing by comparing them with pre-configured and pre-determined attack patterns.
- Anomaly detection. The system detects phishing when anomalous traffic is detected.

As of now, the system will be using signature/rule detection but anomaly detection may also be used if there is any free-time.

Snort

Snort is an open source network intrusion detection and prevention system. Real-time analysis and packet-logging on IP networks. Analyzing each packets closely to detect any suspicious anomalies (Rouse M. , 2005). Snort uses a flexible rules language to describe traffic that it should collector pass, as well as a detection engine that uses a modular plug-in architecture.

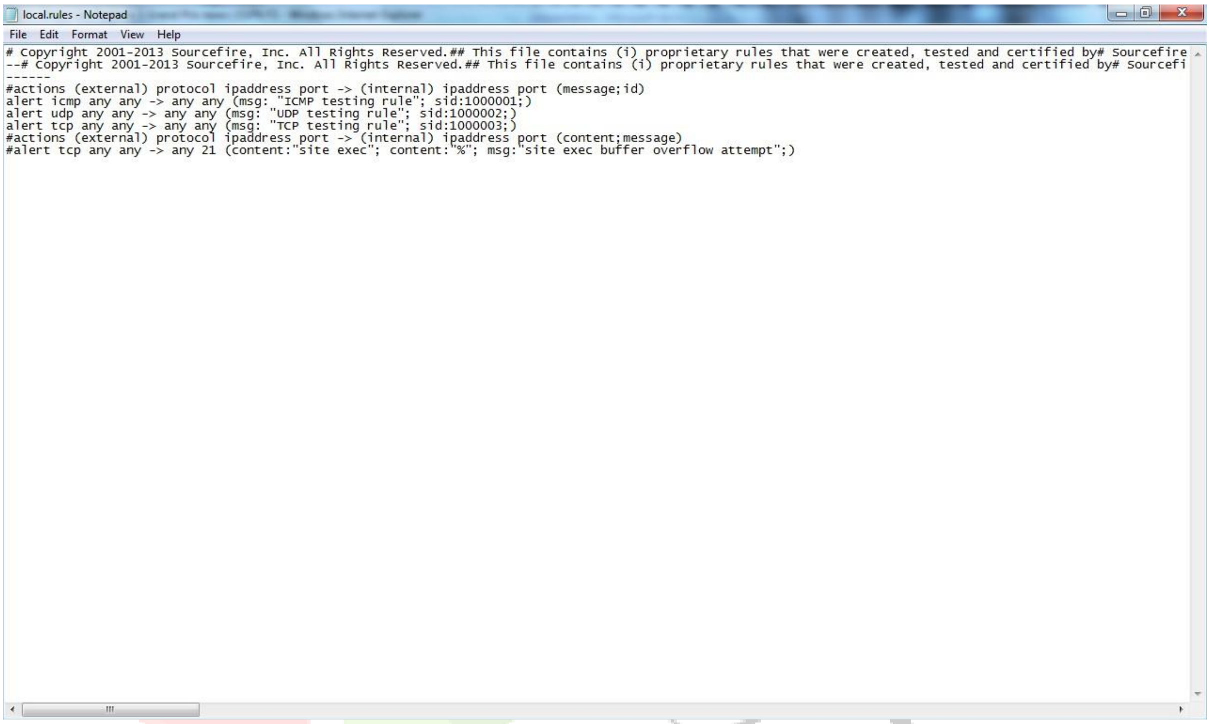
"NSS Group, a European network security testing organisation, tested Snort along with intrusiondetectionandpreventionsystemproductsfrom15majorvendorsincludingCisco, Computer Associates, and Symantec. According to NSS, Snort, which was the sole open source freeware product tested, clearly out-performed the proprietary products" mention by Rouse M.

System Development

At this stage, the project enters the development and implementation phase where the software will be developed. The project was started by redefining the literature review and some part of the problem statements, scope of study and methodology. After that the process of software development started.

After a further study, the chosen program that will be developed into intrusion detection system is SNORT. This is because SNORT has a lot of user usage and with that there is more documentation to help first time user in using it. Also, implementing the rules in SNORT is a bit easier.

The main idea is to help home user in developing the intrusion detection system by themselves. There will be a guide on how to install and configure the program. Not to mention developing own rules to detect any abnormality in network usage. This development is to encounter the problem stated before which is to add another boundary to prevent an unwanted access into the network that may cause problems for the users.

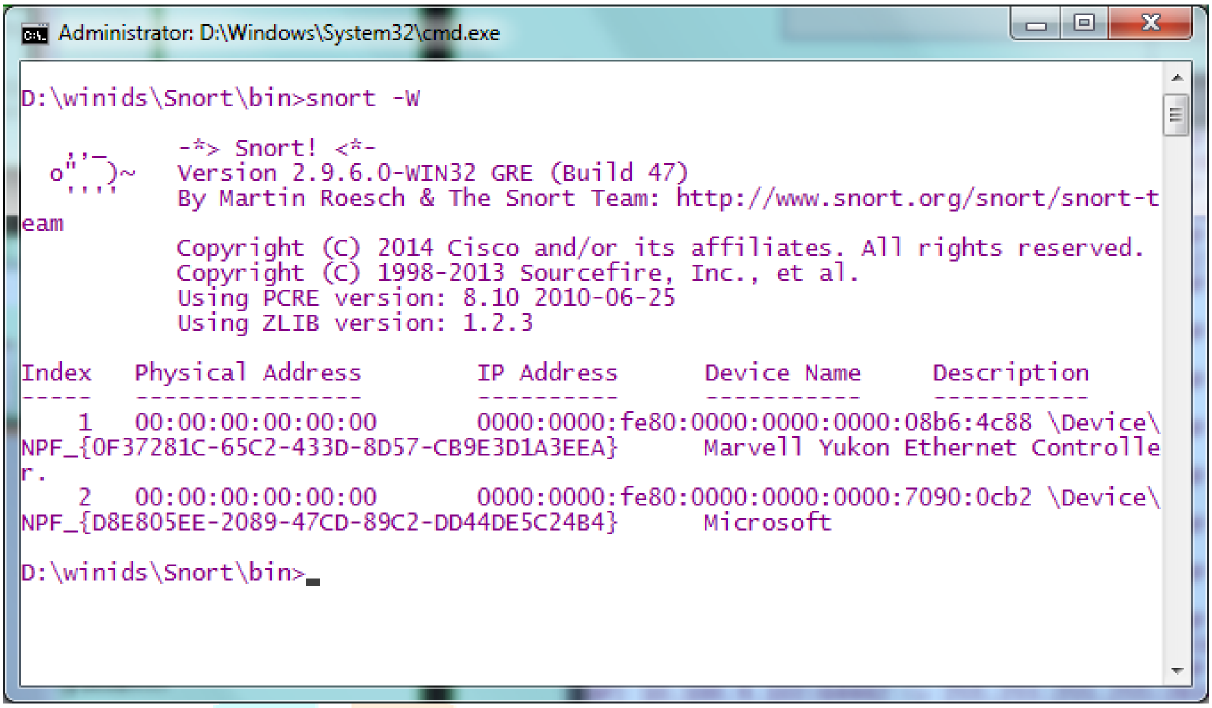


```
# Copyright 2001-2013 Sourcefire, Inc. All Rights Reserved.## This file contains (i) proprietary rules that were created, tested and certified by# Sourcefire
--# Copyright 2001-2013 Sourcefire, Inc. All Rights Reserved.## This file contains (i) proprietary rules that were created, tested and certified by# Sourcefi
------
#actions (external) protocol ipaddress port -> (internal) ipaddress port (message;id)
alert icmp any any -> any any (msg: "ICMP testing rule"; sid:1000001;)
alert udp any any -> any any (msg: "UDP testing rule"; sid:1000002;)
alert tcp any any -> any any (msg: "TCP testing rule"; sid:1000003;)
#actions (external) protocol ipaddress port -> (internal) ipaddress port (content;message)
#alert tcp any any -> any 21 (content:"site exec"; content:"%"; msg:"site exec buffer overflow attempt";)
```

Figure 6: Sample rules to test the program

This rule describes an alert that is generated when the program matches a network packet with all of the following attributes:

- TCP packet.
- Sourced from any IP address on any port.
- Destined for any IP address on the any home network on port21.



```
D:\winids\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0-WIN32 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:08b6:4c88 \Device\
NPF_{0F37281C-65C2-433D-8D57-CB9E3D1A3EEA}      Marvell Yukon Ethernet Controlle
r.
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:7090:0cb2 \Device\
NPF_{D8E805EE-2089-47CD-89C2-DD44DE5C24B4}      Microsoft

D:\winids\Snort\bin>_
```

Figure7: Showing the network inter face of the user’s computer

Future Work

This assessment is only focus on developing intrusion detection system for home-based networking system. In future, a prevention mechanism is to be introduced for Windows-based system, thus improving the network security by combating attacks such as phishing and denial-of-service attack **(**DoS attack**),** hacking attempts and anything else that might compromise the network. Also as this system in tailored to individual user (household), it would be very helpful if in the future this system would be implemented in large organisation. It will a major stepping stone if this system can be built not only for detecting but also preventing as can be seen that is widely used in UNIX-based operating system.

Also, to have the rules engine to be updated without the help from the user. Auto-update the rules engine by a weekly basis.

V PROBLEMS OR CHALLENGES

There are a few obstacles in developing this program. Some of the problems are:

1. The program is suited best with using UNIX based operating system. Also many of the tools will run on only in UNIX based operating system.

2. Configuration of the program is tedious and understanding on how the program works needs a long period of time.

3. As I’m doing this project for Windows-based system, the Intrusion Prevention System cannot be initiated. UNIX is needed to initiate the Intrusion Prevention System. Because of that only the detection part of the system can be use.

4. To write the rules, I would need to be “attack” before I can write the rules as I need to determine the type of “attack” and its content.

VI CONCLUSION

This paper was written as an approach to detect any abnormal network activity in a home networking system. It has been shown that Intrusion Detection System is very useful for improving network security by adding another layer of security on top of the firewall and anti-virus programs.

However in reality hackers may take advantage of any possible resources to attack a computer network, and these resources may be unstable and very difficult to categorize. These difficulties can reduce the effectiveness of this approach. Thus, a more secured way of using the internet is needed for the user by only surfing the internet with an updated anti-virus and understanding the risk of surfing the "wrong" sites.

VII REFERENCES

1. Adams, K. Types of Intrusion Prevention Systems. Retrieved from eHow: http://www.ehow.co.uk/info_8039841_types-intrusion-prevention-systems.html
2. Amoroso,E.(1999).Wykrywanieintruzów.Warszawa1999:WydawnictwoRM.
3. Bo,J.(30August,2010).PhishingMethodsandPrevention.RetrievedfromYahooVoices: http://voices.yah oo.com/ phishing- methods-prevention-6664318.html
4. Kaspian,P.(23July,2013).NetworkSecurityin2013:IsYourIntrusionPrevention System Ready? Retrieved from Security Intelligence Blog: http://securityintelligence.com/network-security-in-2013-is-your-intrusion- prevention-system-ready/#
5. Kazienko, P., &Dorosz, P. (3 April, 2003). Intrusion Detection Systems (IDS)Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture). Retrieved from WindowSecurity.com: http://www.windowsecurity.com/articles-tutorials/intrusion_detection/Intrusion_Detection_Systems_IDS_Part_Inetwork_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html
6. Liniger,R.,&Vines,R.D.(2005).Phishing:CuttingtheIdentityTheft Line.

Indianapolis: WileyPublishing Inc.