COMPUTER NETWORK SECURITY IDS TOOLS AND TECHNIQUES (SNORT/SURICATA)

Okasha Eldow*,Prashant Chauhan **,Punit Lalwani,M.B.Potdar****
*Gtu Pg School, Gandhinagar
Bhaskaracharya Institute For Space Applications And Geo-Informatics
**Bisag, Gandhinagar
Gujarat, India
Okashamahi@Gmail.Com

Abstract— The growing fast of the computer networks require a very high security, to keep the networks , data and , the resources of the network as much safe as possible and to get sure safely and trusty communication between the networks members . The security issues is rising as it is facing a growing problems of unauthorized access , viruses , malicious , etc. so it demand an updated technologies to face all of these circumstance ,The growing rapidly of networks as we said coming with security risks , so every computer network should be fully secure and safe unfortunately it is something can't be possible easily . In the paper we will look to the security issues and count measures of the computer networks and going further also about the intrusion detection systems . SNORT which it's open source system and also SURICATA and also comparison of these two tools

Keywords—introusion detection systems t; IDS; SNORT ; SURICATA .

INTRODUCTION

[1]The demand is increasing for the opening networks the security issues is also growing very fast to achieve the goals of network security **integrity, confidentiality and Availability.** Integrity: the system will allows only the authorized clients or users to modify the information, and to ensure the information is complete .Confidentiality: the server or system will only provide information or the data for the authorized clients or users .Availability: only the authorized clients or users can get the required data or information from the server or the system .

NETWORK SECURITY TECHNOLOGIES

The existing network security technologies which are being used nowadays are:

1- Authentication technology

2- Encrypt data or (data encryption)

3- Firewall technology

4- IDS (intrusion detection technology)

And now we are going to see every technology of these technologies which mentioned above .

A. AUTHENTICATION TECHNOLOGY

is to verify the authentication of the entity. It is based on cryptography, identity authenticity, message authenticity, access authority and finally digital identification

(1) Identity Authenticity

It check the user identity by authentication, which is already known before clients access to the network mostly "Username and password"

(2) message authenticity

The both sides client and the server or the service provider of communication confirm and ensure that:

_ the data was sent and confirmed by the sender;
_ The data do not modified while transmission;
_ The data was sent to the destination .

To guarantee we can apply private key in both sides of communication can be applied to build the message identity information. The message which send by the sender contain data about the message , if there was no difference between the summary of data which send and which had received then it means no any kind of modification happen to the message

(3) access authority

The access authority it means the authorized clients Have accessed to the system after authentication. Mostly systems has a list (ACL) access control list

(4) digital identification

Digital identification is mainly to get sure that the receiver Could prove the authentication of packets which had already received . and it is based on encryption technology: Symmetric key , a symmetric key and hybrid key

B. ENCRYPT DATA OR (DATA ENCRYPTION)

The main purpose of data encryption technology is to get sure and improve that the server only provides the data for authorized clients and mainly it used two kinds of encryption

1. Symmetric key encryption
2. A symmetric key encryption

(1) Symmetric-Key Encryption

Symmetric-key encryption is also called as private-key encryption or single-key encryption. It applies the same key to encrypt and decrypt the message, which is shared by both the sender and receiver. Symmetric-key encryption is simple and fast, thus has been widely used. The most popular algorithms are RC2, RC4, DES, 3DES, SKIPJACK, IDEA, CAST-128, etc. The most important problem in these algorithms is how to transmit the private-key securely to each other it has another name also they call it private key cryptography or single key encryption . the mechanics of this method is to apply the same key for the encryption and also for the decryption ,so it means it is shared between the client and the server or the sender and the receiver . the advantages of this method is simple and fast

I. RC2/RC4 (Rivest Cipher) .
II. DES /3 DES (data encryption algorithm)

And also some others IDEA ,SKIPJACK,…etc. The most important thing is how to share the key securely

(2) Asymmetric-Key Encryption

The public key encryption it is good and secure as well. It has two key public key and also private key it is more complicated than symmetric key The message which encrypted by public key it can only be decrypted by trying to match the private key . The most famous algorithm is RSA (Rivest –Shamir-Adelman).

C. FIREWALL TECHNOLOGY

[2]Firewall technology simply it is a kind of system which work between the internal and external network . which it can easily control the access between these networks , it help the admin to protect his network against illegal access to his resources

the firewalls can :

- Filtering all the packets in the network
- Controlling the access to the network
- Record the logs information and activities
- Alarming and detecting against different attacks

The filtering of the packets in the network, gateway and the proxy can be used individually or in combination of all .the packet filtering is basically checking all the packets and according to the security rules can allow the packet to pass or block it. Application gateway has the opportunity of keeping the network safe by hiding the internal network topology and also the log files and source and destinations addresses . the hybrid firewall is containing the both technologies the packet filtering and the gateway .The proxy is the technology which works on the application layer and every application has to be specified first to work with proxy. The proxy can easily monitor the network as every packet Hast to come throw the proxy and also it is shielding the internal network details

D. INTRUSION DETECTION SYSTEMS

[3]The IDS or the intrusion detector systems it is a security technology it is similar to fire wall but have also some advantages .basically it is works by collecting the data of the internal network and the all resources of that network and try to figure out by analyzing these data generally it used to :

- Monitoring
- Attack recognition
- Security auditors
- Also it helps for improving network integrity

There are two types of intrusion detectors

A- Anomaly detection
B- Misuse detection

Anomaly based uses technique of trying to figure the behavior of the network according to saved Information about the activities which it is normal or strange , looking after any abnormalities behavior and detect it or alert the admin about it. the most advantage of this technique is the high rate detection for the new intrusions. A signature technique is using , every single thread It has an a unique signature so simply this works By creating a log of different type of attacks or malicious Signatures and try to match it with whatever signature That comes through the network . it has another name Pattern matching . The disadvantage of this technique can easily try to change the signature so it would be unknown or the system so it can't be detected .so it needs regularly update or each and every signature

RELATED WORK

There are some definitions which are related to the intrusion detection systems

E. NETWORK IDS

[4]Is kind of software or hardware or also can be a combination of both that used to detect the intruder the most famous network intrusion detection system is SNORT .Snort is open source IDS freely available and will talk about it in the next section . and also it depends upon the companies or the users needs whether it is software or hardware or combination of both . also it may use the anomaly based or the pattern based or the combination of both .

F. HOST BASED IDS

The host based intrusion detection systems HIDS it works as an agents on the host Which can look after the application log files And system to find where is the abnormal Activities and it is two types

1. Reactive which it can only just monitoring and alert you and inform you if something happen .
2. Proactive this one can sniff the traffic of Network which HIDS has installed and let you Know by alerts in real time

THE PLACEMENT OF THE IDS IN THE NETWORK

[5]It is depending to the topology of the network and to which type of activates that you want to be detected :internal activities ,external activities or both . so if you have only one bath for the internet so better to place it in the first point which it can be router or firewall . if you have multiple paths to the internet so you have to place the IDS in each and every entry point . the more us of IDSs means more cost as you have to do more work more resources and also more maintenance . so

we can finalize that by saying it depends to the user and the security systemor policy which he wants to apply to his system. In this next image we can see where IDS is paced in the network which it has only one path to the internet .

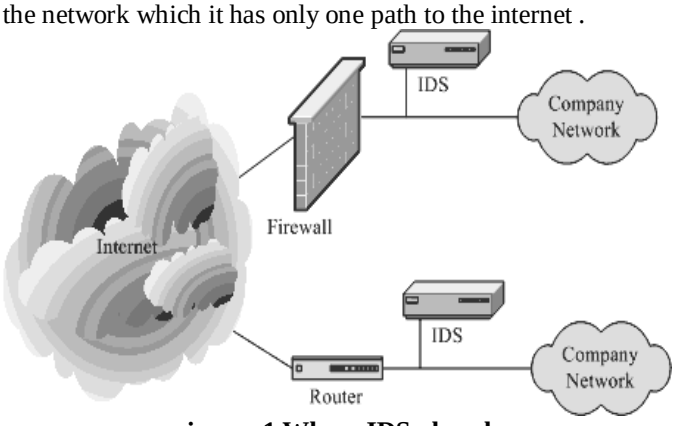

image 1.Where IDS placed

EXISTING IDS TECHNOLOGIES

in this part we will see some of the technologies which used nowadays . actually we will be working on two technologies :

1. SNORT
2. SURICATA

1- SNORT

Snort is open source IDS which is available free of any costs , you can get it from http://www.snort.org . it is based on the rules which the call it snort rules which is regularly updated .

1.1- SNORT COMPONENTS

The below images shown the components of the SNORT

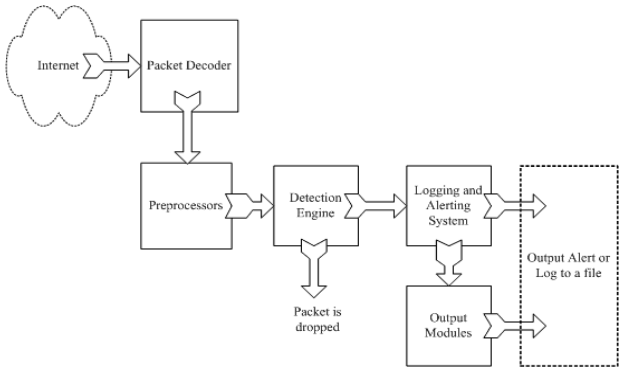

image 2.snort components

1.1.1- Packet decoder

It takes the packets from different interfaces and send it to preprocessed or to the detection engine ,these interfaces can be Ethernet ,serial line internet protocol ,etc. .

1.1.2- Preprocessors

It is very important for IDSs , by applying the preprocessing you can easily analyze the packets ,find the abnormal packets ,and also it generate some alerts so it is playing important role for intrusion detection systems .

1.1.3- Detection engine

The most important part od the IDSs is this part , the detection engine has the responsibility of detecting any stranger activities which might be exist on the packets , it apply the snort rules or this detection .so if any of these packet has matched any rules then immediate action will be taken else it will drop that packet . so it means packet will be logged or generating an alert . the stronger IDS has strong detection engine . when are you building an IDS keep these on mind

- Set of the rules as much as it can detect all o the possible attack so it means should be updated .
- The machine which you installed the snort should be have some features .
- Also the internal buses should be very fast
- Also the network load .

1.1.4- Logs and alerts

After the detection engine checking the packets so it might log the activity or also alert and log this alert into tcp dump file or txt file or whatever form ,you can easily manage the logs by changing the location or whatever action you want to .

1.2- INSTALLATION OF SNORT

Actually we will be installing snort on Linux 14.04 VMware Using the guide lines of the installation of the snort from the book snort for dummies[6]

1.3- TOOLS WHICH WORK WITH SNORT

- Barnyard2 : it is tool which works with snort to store the data temporally.
- PulledPork : it is toll to keep snort updated by downloading the latest rules .
- BASE : basic analysis security engine which it works as web page GUI to make easier to the end user to work with snort .

DENIAL OF SERVIECE ATTACK

in brief the DOS attack is kind of attack which affect the quality of services of the network or example by flooding the bandwidth to make it not possible to carry the packets .

1- TYPES OF DENIAL OF SERVICE ATTACK

there are several types of denial of service attack which we can see below :

- PING flood
- SYNC flood
- UDP flood
- SMURF attack

[7]PING of death is kind of flooding the victim by thousands of ping packets , SYNC flooding occurs when attacker tries to drain the TCP/IP stack ,attacker will keep sending using spoofed sources and the victim ACK/SYNC packets to the spoofed address . UDP flooding it uses the user datagram protocol so the attacker can attack single destination or different ports .[8] SMURF attack is DDOS attack which flood large number of internet control message packets (ICMP) ,it attack the IP broadcast address in the network .

2- TOOL FOR GENERATING DOS ATTACK

For our implementation and testing part we will be using [9]HPIG3 which it is scanner tool used packets from spoofed

sources , also it is use to send files , test the firewall rules and so many uses

Simple SYNC flood

hping3 -S --flood –V (victim's IP)

hping3: name of the application binary

S : set SYN tcp flag

Flood : flooding without caring about the replies rom the destination .

V: to enable verbose out put and will be shown as :

Len= , ip = , flag = ,seq = ,

SYN attack

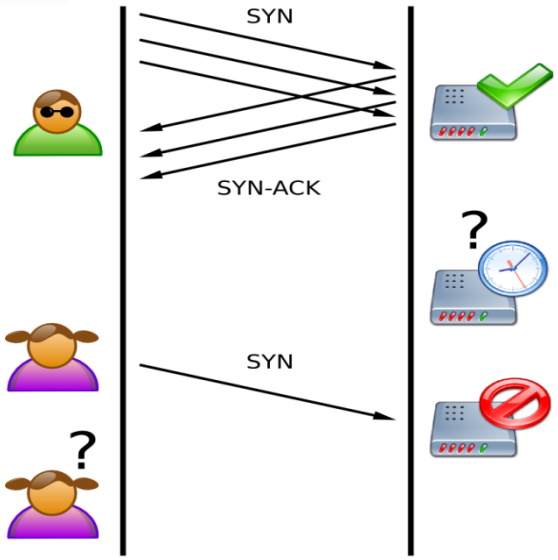

image 3.SYN ATTACK

We have implemented sync attack using HPING3 for generating the attack and we let snort work on daemon mode to detect the attack and we saved the logs and used BASE to show it up

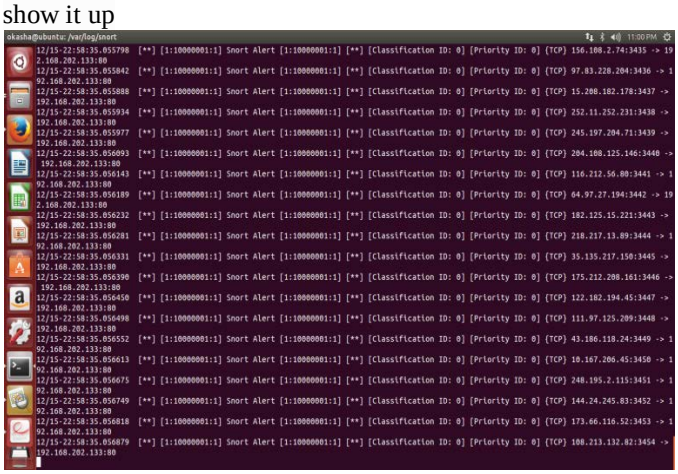

image 4.Banyard logs

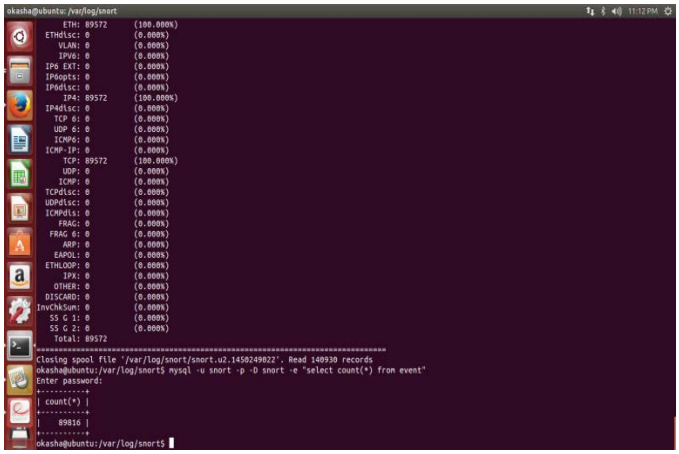

image 5.Count the logs

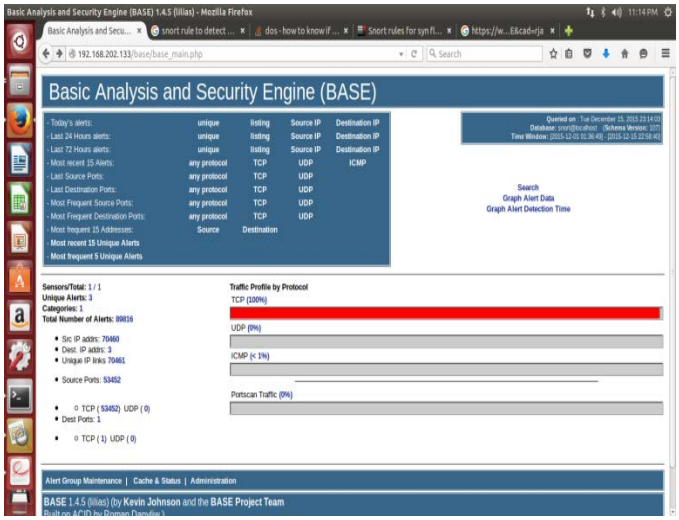

image 6.BASE engine

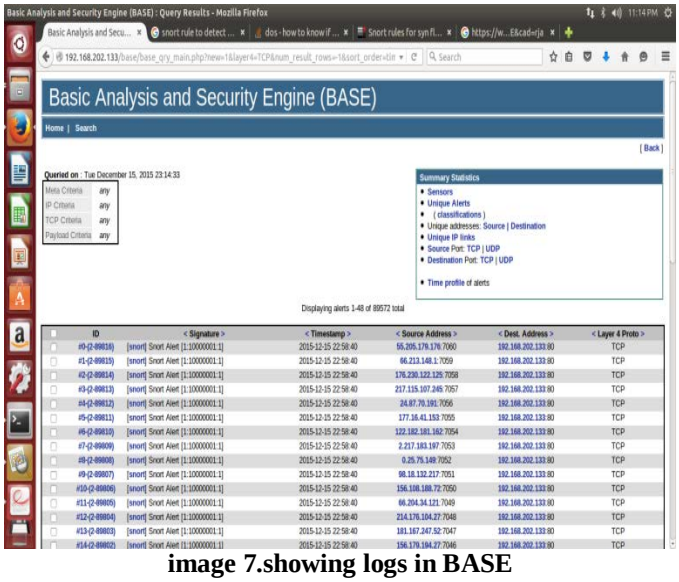

image 7.showing logs in BASE

SNORT VS SURICATA

Suricata is an open source IDS system developed by Open Information Security Foundation it uses also the same set of rules of snort but the important advantage of suricata among snort is the multithreading .According to the test SNORT and SURICATA have detected same results of DOS attack . so in the future and the growing fast of the suricata it might be used instead of snort as we said it is supporting the multithreading which it means reducing the time and also giving high performance . [10]David and Benjamin have analyzed snort and suricata and conclude that suricata has higher accuracy rate more than snort .

CONLOUSION

in this paper we have studied the intrusion detection system and we have also tested some of the tools , we did one experiment of generating SYN attack using HPING3 and we have detected it using SNORT , also we have shown the logs of snort into BASE .
in the future we can work on comparison of suricata and snort based on different or specific type of attack

REFERENCE

1. Yan, F., Y. Jian-Wen, and C. Lin. *Computer Network Security and Technology Research*. in *Measuring Technology and Mechatronics Automation (ICMTMA), 2015 Seventh International Conference on*. 2015. IEEE.
2. HUANG, Z.-j., A. ZHAO, and H.-x. XU, *Network security and firewall technology*. Journal of Naval University of Engineering, 2002. **1**: p. 013.
3. Atefi, K., et al. *A hybrid intrusion detection system based on different machine learning algorithms*. in *Proceedings of the 4th International Conference on Computing and Informatics, Sarawak, Malaysia*. 2013.
4. Karadkar, C., et al., *Review on Implementation of Intrusion Detection in Physical Network*.
5. Rehman, R.U., *Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID*. 2003: Prentice Hall Professional.
6. Scott, C., P. Wolfe, and B. Hayes, *SNORT for Dummies*. 2004: John Wiley & Sons.
7. Erickson, J., *Hacking: the art of exploitation*. 2008: No Starch Press.
8. edia.org, e.w., *Smurf-attacks* Smurf-attacks IEEE/IFIP 2004., 2004.
9. *HPING3*. http://www.hping.org/manpage.htm.
10. Day, D.J. and B.M. Burns. *A performance analysis of snort and suricata network intrusion detection and prevention engines*. in *The Fifth International Conference on Digital Society*. 2011.