International Journal of Modern Communication Technologies & Research (IJMCTR)
ISSN: 2321-0850, Volume-2, Issue-9, September 2014

Intrusion Detection Systems

Ahmed Abdelrahaman Eltom, Amin Babiker A / Nabi Mustafa

***Abstract*— The main goal of IDS (Intrusion detection Systems) is attack detection whether the subject to attack was a single computer or an entire network. Despite the major effort to provide a more security to Information systems , and keeping it as safe as possible, it is not possible to provide fully secure These systems , in addition to the fact that even a truly secure system is vulnerable to abuse by insiders who abuse their privileges .**
Therefore, there is a massive need for the existence of intrusion detection systems performing constant monitoring to the system traffic and efficiently detect any apparition of intrusion attempts whether it came from inside or outside the network .

***Index Terms*— IDS, network**

I. INTRODUCTION

Cyber crime grows rapidly and every day threatening widespread internet business applications like E-commerce, financial transfers and other important sensitive business being done online. Information system as a subject of attack must have their own surveillance technologies to make an alert if any intrusion occurred which lead them to the usage of Intrusion detection systems.

Intrusion detection is the process of monitoring computers or networks for unauthorized entrance, activity, or file modification. Computer hackers always target their victims using sophisticated ways after finding vulnerabilities and security holes or some other times just benefiting from regular security mistakes like using common and easy passwords in order to gain access to network resources and even after achieving the intrusion successfully they may stay hidden without been detected .

Intrusion Detection Systems help information systems prepare for, and deal with attacks. These devices will provide important information about the intrusion in order not just taking immediate response as corrective actions, but also to take preventive procedures to make sure the system will no longer be violated by intruders through tracing back the steps and activities of intrusion closing security holes and fixing former security mistakes and weaknesses.

II. THE NEED OF IDS

The common solution when it comes to protect any network is the firewall. Firewall alone will not be enough due to some causes like :

The fact that not all access to the Internet occurs through the firewall and not all threats originate outside of the firewall . In addition to that firewalls only set barriers in the front gate of the network guarding the doors to the internet so if the traffic reflecting security breaches did not flow through the firewall, it will not have the ability to detect the problem. Finally Firewalls are subject to attacks themselves and here come the great need for IDS as they perform as "the logical complement to network firewalls.

Regarding data inspection firewalls inspects packets headers and depending on that information makes the decisions. these examinations does not include inspecting the entire contents of the packet which leaves IDS the only proactive means to detect inside or outside attacks though investigating the entire packet contents and detecting any malicious activity even if it was embedded within normal traffic . Monitoring and constant surveillance detects intrusion incidents and its source , enhancing detecting probability and providing deeper packet analysis compared to a firewall or a router specially incase of sophisticated attacks.

III. IDS FUNCTIONALITY

Intrusion detection provides In addition to Monitoring both system and user activities along with analysis to alerting any attack attempts or suspicious activity, a great capability of auditing the system specially the sensitive systems which probably a subject to attacks and finding vulnerabilities to take the proper action enhancing the information system security and making the intrusion as hard and complex as possible.

IV. IDS CLASSIFICATION

Intrusion detection system could be classified into three types
1. Host based IDS
2. Network based IDS
3. Hybrid based IDS

A. Host-Based IDS (HIDS)

In HIDS the examination of the data is done on hosts having a great advantage of being close to end user location it is so easily to detect any case of insider abuse and any user suspicious activity or file modification will be spotted efficiently. HIDS is actually inefficient in large networks consisting of a huge number of endpoints .

B. Network-Based IDS (NIDS)

Unlike the Host based IDS, Network Based IDS examines not the data originated on a computer but the packets being sent over the network. Packet analysis and comparison is so essential to verify packet nature. The technique is so similar to packet sniffing, capturing and pulling the data from any protocol packet such as TCP/IP . While Host based IDS is effective to detect insider abuse and related suspicious activity, Network Based IDS is efficient in detecting attacks from outside the network such as unauthorized access attempts , denial of service and bandwidth theft and other attack types that come from outside the trusted network .

C. 3.Hybrid based IDS

Hybrid based IDS is the logical complement to NID and HID achieving central intrusion detection management.

Hybrid based IDS is the logical complement to network based IDS and host based IDS achieving central intrusion detection management.

As the name Hybrid suggest Hybrid IDS combines several techniques in one IDS system which lead the combination of many examination techniques achieving better intrusion detection and security enhancement . Although the differences of the types IDS and how they work have an advantage of greater detections by making them work together as they actually they complement each other the risk of interoperability stands still although there is still no proven industry stander of interoperability of intrusion detection. Finally the complexity of Installation and management of Hybrid IDS is another major consideration.

V. IDS TECHNIQUES

The following techniques are used for investigation by all IDS types . For each of these types, there are four basic techniques used to detect intruders:

1 . Anomaly detection.
2. Misuse detection (signature detection).
3. Target monitoring.
4. Stealth probes.

A. Anomaly Detection

Its main goal is to detect abnormal patterns of behavior through defining a baseline describing normal behavior, and then detects deviations.

Any action which is significantly distinct from that pattern will generate an alarm and considered as possible intrusion.

B. Misuse Detection or Signature Detection

Relay on characteristics of known attacks and vulnerabilities (called signatures) to catch an attack. Despite its advantages such as accuracy and low rate alarms, it has the disadvantage of not discovering new or known attacks.

Target Monitoring

Two major advantage of Target monitoring are the absence of the need for continuous search for misuse and the absence of need for constant monitoring since Target monitoring looks for specific file modifications. That could be considered as corrective action since it takes place after the existence of the intrusion.

C. Stealth Probes

This technique attempts to detect any intruders compromising system security over prolonged periods of time. Attackers tend to wait after finding vulnerability and wait even longer to launch the attack in addition to the fact that may stay hidden for a very long time after intrusion.

Through collecting massive data from all over the system Stealth probes checks for any methodical intrusions over a long time period.

VI. EFFICIENCY OF INTRUSION-DETECTION SYSTEMS

The efficiency of an intrusion detection system could be evaluated by the following factors :

- **Accuracy.**

Accuracy of IDS could be defined by the actual detection of attacks and absence of generating false alerts. Inaccuracy occurs when an IDS generates an alert coming from authorized action of a legitimate user reporting it as a suspicious activity.

- **Performance.**

IDS performance is vital to accomplish the main duty of IDS of detection. It is defined by the rate at which audit events are processed.

- **Completeness.**

Completeness can be defined by IDS ability to detect all attacks.

- **Fault tolerance.**

There is no doubt that IDS itself should not compromise in the natter of security by hackers specially when they watch sensitive information system that most like targeted by hacker.

- **Timeliness.**

The time factor is one of the most important factors in achieving the efficiency of IDS. Considering the technical capabilities that usually hackers have and the time they can take to create massive damage the systems ,creates a massive need of immediate actions and quick analysis if the information system security has been compromised and.

VII. SIMULATION

The simulation is done under virtualization environment of VMware Software and consists of three major devices:

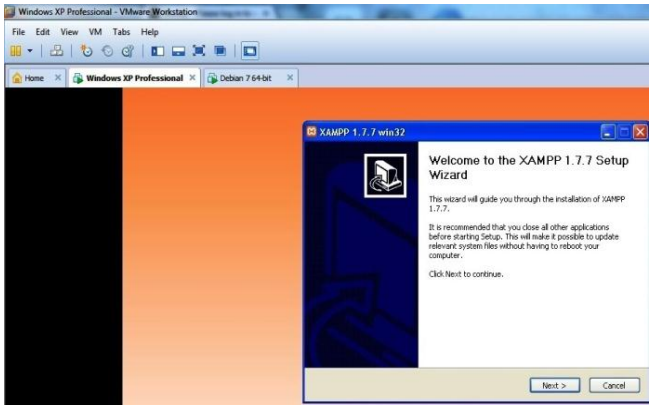
The first one is the hacker devise operating on Win7 lunching an attack on the second device which is an online server deployed based on Win XP environment and connected to IDS which should efficiently detect the attack . Configuration, Monitoring, management, and finally attack detection is the steps of the entire procedure.

A. Simulation steps

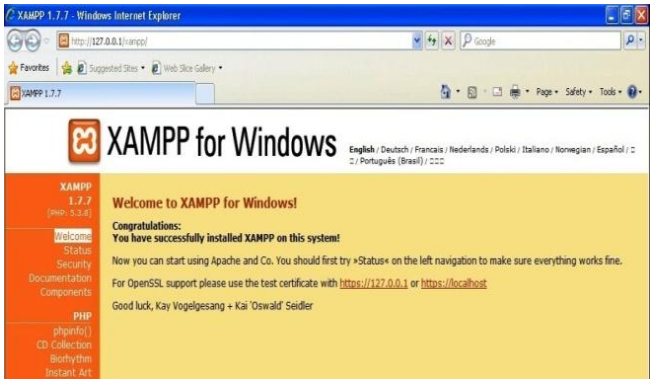
1 . Windows XP devise (attacked Server –XAMPP application):

Installing the server on Windows XP environment using XAMPP Software in order to create a server along with related applications, the choice of the software was based on the efficiency , ease of installation , it is free and the absence of the need for configuration to make APATCHE , PHP & MYSQL compatible with each other.

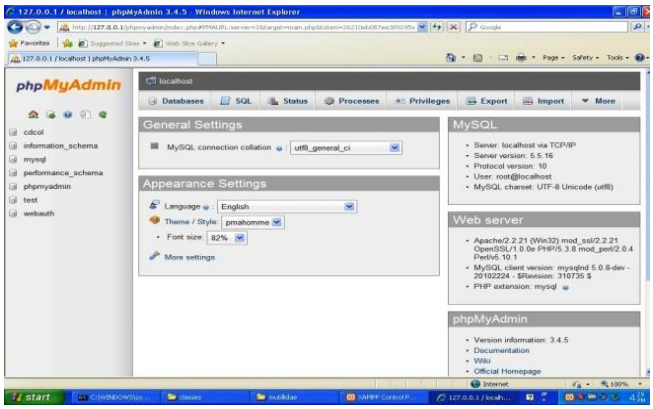
The following figure 1 shows XAMPP installation on WinXP environment.



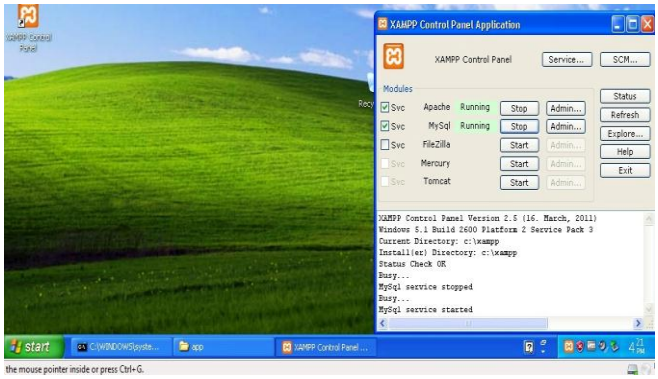
the next figure 2 shows the success of installation procedure.



The following figure 3 shows Database



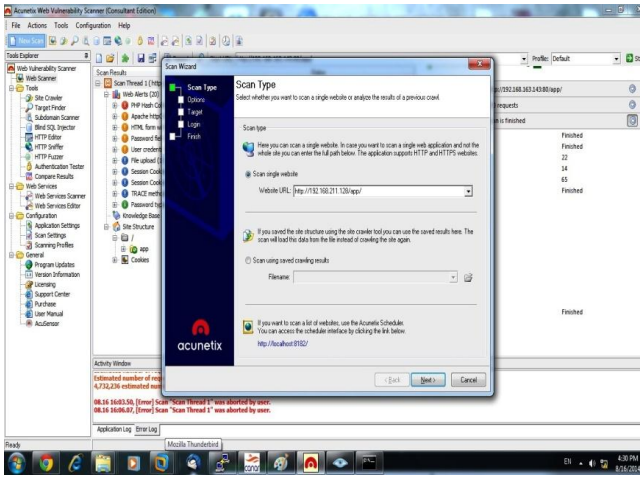
The following figure 4 shows APPATCHE running properly in the server.



B. Intruder Device :

Based on Windows 7 environment , running a web vulnerability scanner which its main job is to find any security holes in order to perform illegal activity to the system , later an attack on the server will be lunched through its IP address targeting the server application .

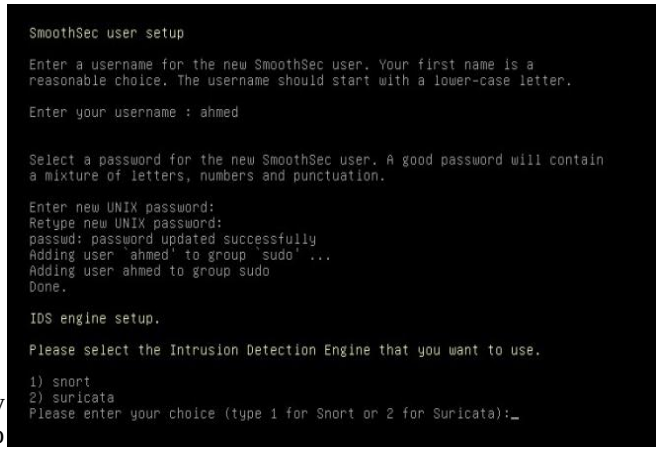
The following figure 5 shows using server IP to address to target server application server.

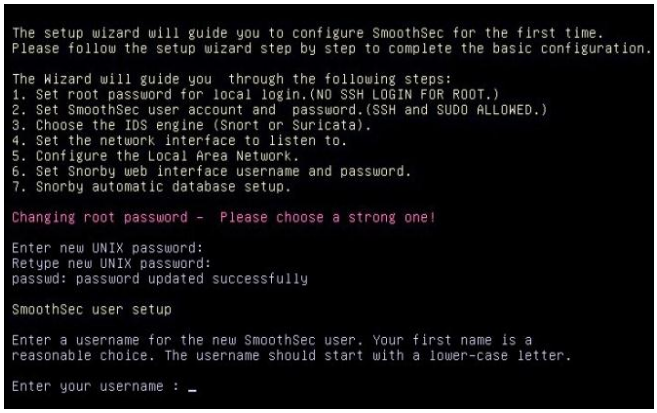


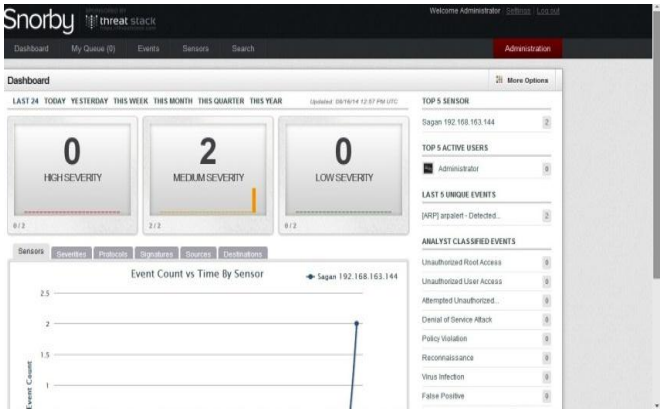
C. IDS configuration

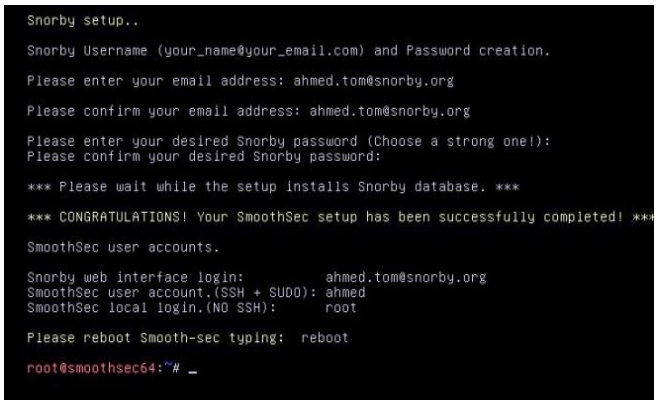
The IDS used is smoothsec *which is functioning under Linux Dabian and based on the multi threaded* Suricata IDS/IPS *engine and* Snorby *.As an efficient network monitoring tools and with proper configuration should be able the detect the attack to be lunched.*

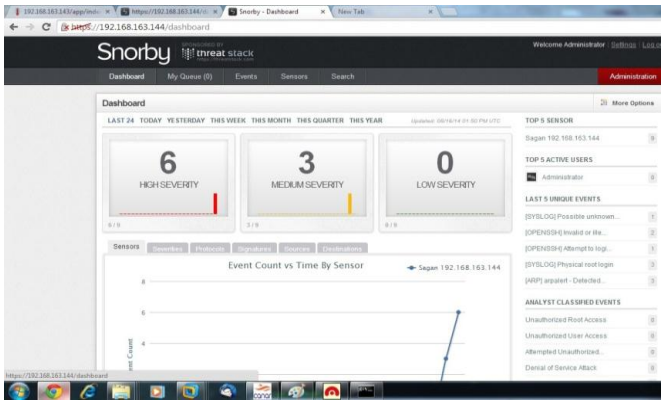
The following figure 6 , 7 , 8 , 9 , 10 , 11 , 12 shows Smoothsec IDS installation , configuration , mentoring , normal activity , traffic before and after attack and attack details in order .

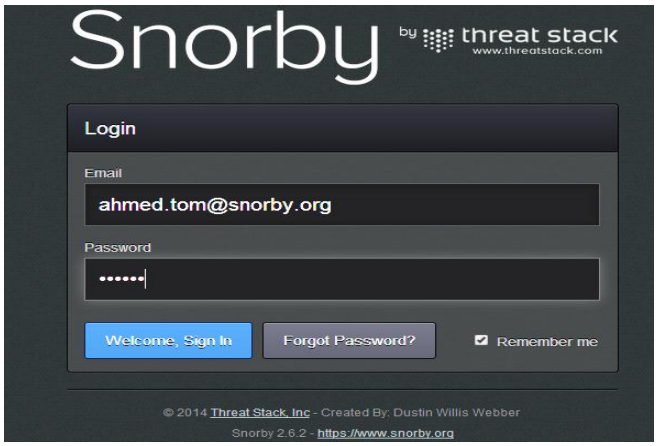


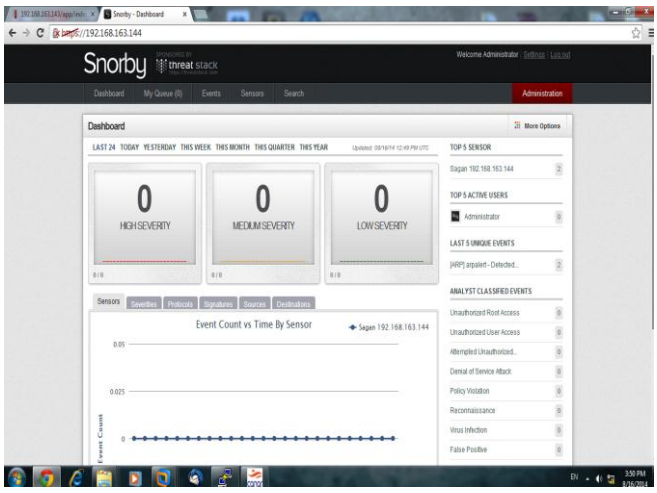












After lunching the attack based on the server IP address the IDS provided real-time alerts for suspected intrusions, displayed to a user console clearly identifying major threats (high severity) .

VIII. Conclusion

This paper insures the that IDS is a necessary tool in any information system environment . With the rise of systems intrusions IDS tools are becoming increasingly necessary. Once configured correctly can provide very important information and can detect any intrusion attempts giving clear and detailed alerts and warnings playing a major part in the protection and defense plan .

References

[1]Understanding Intrusion Detection Systems SANS Institute InfoSec Reading Room

[2]An Introduction to Intrusion Detection Systems by Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC Washington, D.C. http://www.symantec.com/connect/articles/introduction-ids

[3]International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 1 ISSN 2229-5518 IJSER © 2010 http://www.ijser.org

[4]Importance of Intrusion Detection System (IDS) Asmaa Shaker Ashoor (Department computer science, Pune University) Prof. Sharad Gore (Head department statistic, Pune University)

[5]Next Generation Intrusion Detection Systems (IDS) By Dr. Fengmin Gong, Chief Scientist, McAfee Network Security Technologies Group WHITE PAPER networkassociates.com http://www.ciscopress.com/articles/article.asp?p=25334&seqNum=4

.