ISSN NO: 2347-4890
International Journal of software & Hardware Research in Engineering
Volume 1 Issue 2, October 2013

INTRUSION DETECTION BY INTRUSION DETECTION SYSTEM (IDS)

SACHIN MALVIYA
Student, Department of Information Technology, Medicaps Institute of Science & Technology, INDORE (M.P.)
Sachinm.research@gmail.com

SUNEET JOSHI
Assistant Professor, Department of Information Technology, Medicaps Institute of Science & Technology, INDORE (M.P.)
suneetjoshi_2000@gmail.com

ABSTRACT
Secure communication or sharing on an unsecure network has a major problem in the area of security over the last few years. The attackers or hackers are always tries to break through the system to gain access to the resources to which they are not permitted. The illegitimate attempt to access over the unsecure network & creates a potential threat to the integrity of the system is the task performed by hackers. As the network become wider day by day & the information are circulated over the network this problem is even getting worse. This problem is given a name intrusion.
As the intrusion is a process of trespassing the system or network to gain illegitimate access over the network the person who is doing intrusion is intruder which gives rise to the system which is able to detect such intrusion done by an intruder & this system is given name intrusion detection system. The process of detecting intrusion by intrusion detection system is Intrusion Detection.
The electronic data has now become the bone of communication & network uses electronic form of transfer & to protect it from the unauthorized world the intrusion detection system is needed.

KEYWORDS
Intrusion Detection system, web security, security in network, hackers, IDS Architecture.

GENERAL TERMS

Hackers-
Hacker is someone who seeks & exploits weakness in a computer system or computer network.

Intrusion-
An intrusion is a deliberate unauthorized attempt successful or unsuccessful, to break into, access, manipulate, or misuse some valuable property.

Intrusion Detection-
The process of detecting intrusion in a system by intruders is intrusion detection. The intrusion detection is done by predefined rules.

Intrusion Detection System-
An intrusion detection system is a device or software application that monitors network or system behavior for malicious activities or policy violations & produces reports to a management station.

1. INTRODUCTION
An intrusion detection system is a system which attempts restricts the loss of integrity, confidentiality or availability of resource [2].Over the past few years the IDS has a deep impact on the study of security over the computer network. Some systems may attempt to stop an intrusion & prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, & repeating attempts [1].
An IDS is able to detect the intrusive activities & inform the administrator for such scenario & attempt to resolve it [3].

2. IDS vs. FIREWALL
IDS & Firewall both are related terms in network security. Both provide some features which relates to a security on network. But an IDS is differ from a firewall in that a firewall looks outwardly for intrusion in order to stop them from happening.
Firewalls limits access between networks to prevent intrusion & do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place & signals an alarm. Ids also detects an intrusive activities originate from within a system [4].

3. APPROACHES TO IMPLEMENTS AN EFFECTIVE IDS

Some of the approaches which are basically used to implement IDS:-

3.1 Anomaly Detection-

ISSN NO: 2347-4890
International Journal of software & Hardware Research in Engineering
Volume 1 Issue 2, October 2013

The anomaly based systems are the learning system which is that they run continuously creating logs of actions & activities. These logs are later than uses to identify malicious activities that might results an intrusion [4].
In anomaly detection, we are able to build a profile of users, applications or system resource usage & identified as the bad activities or anomalous activities [4].
In this approach, the identification engine observed activities & compares it with rules of profiles & identified it as intrusive activities [4]. In this the profile is being created which then use to evaluate the specific behavior of that profile.
The profile is being classified as:-

3.1.1 Individual Profile
Individual profile is being created by collecting common activities a user is expected to do & if any unusual behavior is shown on this profile this can be detected [4].

3.1.2 Individual Profile
Group profile represents the group of users with a common work pattern [4].

3.1.3 Group Profile
Group profile represents the group of users with a common work pattern [4].

3.1.4 Resource Profile
Recourse profile monitors how executable programs use the system resources [4].

3.2 Misuse Detection-
The misuse detection assumes that each intrusive activity is represented by its unique pattern or signature & the slight variation of the same activity produce new signature & therefore it can also be detected. Therefore, It can also be known as signature system [4].

4. TYPES OF IDS-

The intrusion detection system can be classified based on their monitoring scope [3]. According to scope they can be classified as:-

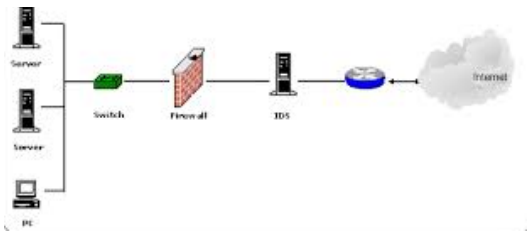

FIG. 1

4.1 Network-Based IDS (NIDSs)
The NIDSs can cover the whole network & take it as the monitoring scope. The NIDSs monitor the traffic on the network for the detection of any type of intrusive activities. NIDSs are responsible to detect anomalous, inappropriate, or other data that may be considered unauthorized & harmful occurring on a network [5].

4.2 Host-Based IDS (HIDS)
The HIDS take an individual or single system as the monitoring scope for the detection of intrusion on this single computer. The HIDS uses software that monitors operator system specific loss including system, event & security logs [5].

4.3 Hybrid Intrusion Detection System
For the realistic applications of intrusion detection system we need features which are present in both the network-based intrusion detection system & the host-based intrusion detection system, the combination of both the intrusion detection system forms hybrid intrusion detection system [5].

5. ARCHIECTURE OF IDS

An intrusion detection system consists of several elements to monitors the intrusive activities:-

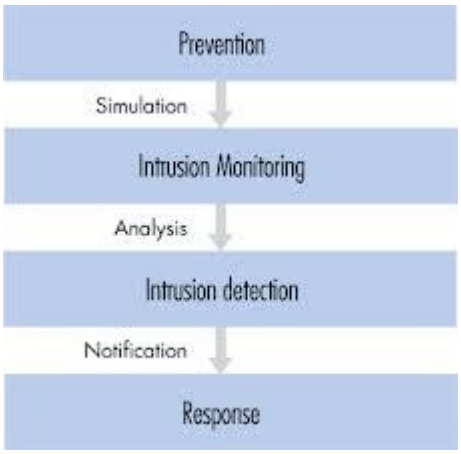

FIG. 2

5.1 Network Load Balancer
Network load balancer gathers data from all over the network and distributes it to all he network monitors [4].

5.2 Network Monitors

The computer program that runs on a targeted system or device for detection of malicious activities is network monitor [4].

5.3 Analyzer

The activities monitors by network monitors are then analyze to classify it as intrusive or not [4].

5.4 Alert Notifier

This can create a proper notification to the responsible person or administrator to take required action [4].

5.5 Command Manager

Command manager is the administrator of the system who has the authority to control it [4].

5.6 Response Subsystem

This subsystem gives the capability to take some action against the threat to the target systems [4].

5.7 Database

The database is the collection of knowledge which can provide base rules to detect intrusion or simply the definition of intrusion [4].

6. Conclusion

In this paper, we have been trying to understand the problem related to the communication & sharing on the network. The problem of intrusion by intruder can cause security threat, for such problem the solution is the intrusion detection system.

The intrusion detection system is a software application or a program that monitors the network or targeted system for any type of malicious activity & detects an intrusion.

7. REFERENCES

[1] Towards Cellular Automata Based Network Intrusion Detection System with Power Level Metric in Wireless Ad hoc Networks (IDFADNWCA).
2008 International Conference on Advanced Computer Theory and Engineering

[2] INTRUSION DETECTION IN WIRELESS AD HOC NETWORKS.
IEEE Wireless Communications • February 2004

[3] A System for Power-aware Agent-based Intrusion Detection (SPAID) in wireless Ad Hoc Networks.

[4] "Cryptography and Network Security: Principles and Practice" William Stalling.

[5] "Cryptography and Network Security" by Atul Kahate (2nd Ed.).

