International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2394-2819
Email: editor@ijarets.org Volume-3, Issue-5 May- 2016 www.ijarets.org

# INTRUSION DETECTION- A TECHNIQUE IN WIRELESS NETWORK SYSTEM TO SECURE FROM ATTACKS

**Ashu**
Research Scholar
Dept. of Computer science
NIILM University Kaithal

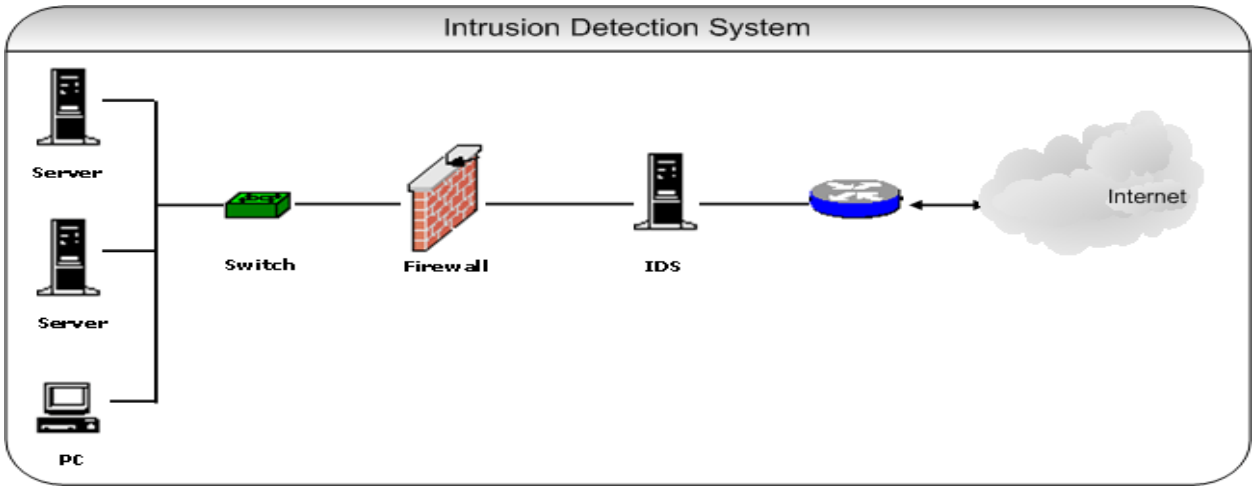
**Dr. Anil Kumar**
Associate Professor
Dept. of Computer science
NIILM University Kaithal

**ABSTRACT:** In today's booming age, every business including the 'brick and mortal' is connected to compete for market share in the cyberspace. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Many intrusions in our system are present which are not so easy to detect. To detect this intrusion a system is approached known as intrusion detection system. This system monitors the network or system activities to find if there is any malicious operation occurs. The term IDS actually covers a large variety of products. ID systems are being developed in response to the increasing number of attacks on major sites and networks,

**KEYWORDS:** intrusion detection, detection methods

## INTRODUCTION

Intrusion detection is a security management system for computers and networks. Intrusion detection systems are designed to analyze network traffic for potentially malicious behavior and to report possible intrusions to a centralized management node. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack. The main function of an IDS product is to warn you of suspicious activity taking place − not prevent them. An id system follows a two-step process. First procedures are host based and are considered the passive component which includes inspection of the system's configuration files to detect inadvisable settings, inspection of the password files to detect inadvisable passwords and inspection of other systems areas to detect policy violations. The second procedures are network based and are considered the active component mechanisms are set in place to reenact known methods of attack and to record system responded.



## FUNCTIONS OF INTRUSION DETECTION SYSTEM

1. Monitoring and analyzing both users and system activities
2. Analyzing system configurations and vulnerabilities
3. Assessing system and file integrity
4. Ability to recognize patterns typical of attacks
5. Analysis of abnormal activity patterns
6. Tracking user policy violations

## CLASSIFICATIONS

Intrusion prevention system can be classified into four different types

***Network based intrusion prevention system*** – a network intrusion detection system analyzes network traffic and hosts to locate potential intrusions when setting up a network intrusion detection system, the monitoring points are setup at high traffic areas on the network to examine the network data packets for potentially malicious actions.

***Wireless intrusion prevention systems*** – a wireless intrusion prevention system monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.

***Network behavior analysis***- network behavior analysis examines network traffic to identify threats that generate unusual traffic flows such as distributed denial of service attacks, certain forms of malware and policy violations.

***Host based intrusion prevention system***- these are designed to have one network host agent that uses application logs, file system modifications, and system calls analysis to locate intrusions to the network. The sensors in a host-based intrusion detection system normally consist of software agent(s). A common example of HIDS is OSSEC and tripwire.

***Detection methods***

There are a multiple ways detection is performed by IDS. The majority of intrusion prevention systems utilize one of the three detection methods signature based, statistical anomaly based and stateful protocol analysis.

***Signature based detection***- signature based ids monitors packets in the network and compares with pre-configured and pre-determined attacks patterns known as signatures. This is useful for finding already known threats, but does not help in finding unknown threats, variants of threats or hidden threats.

***Statistical anomaly based detection***- an ids which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify which is 'normal' for that network-what sort of bandwidth is generally used, what protocols are used that it may raise a fake positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured.

***Stateful protocol analysis detection***- this method identifies deviations of protocol states by comparing observed events with predetermined profiles of generally accepted definitions of benign activity.

## PASSIVE IDS

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.

## REACTIVE IDS

Reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat.

## LIMITATIONS

Intrusion detection systems are not perfect. Depending on the design of the system a number of false positive results can be generated. Intrusion detection software provides information based on the network address that is associated with the IP packet r\that is sent into the network. This is beneficial if the network address contained in the IP packet is accurate. However the address that is contained in the IP packet could be faked or scrambled.

## REFERENCES

1. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-today-tomorrow-341
2. http://www.computerweekly.com/tip/Network-intrusion-detection-and-prevention-systems-guide
3. https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-detection-system-ids
4. .http://krazytech.com/wp-content/uploads/Intrusion-detection-system-image.png
5. https://www.techopedia.com/definition/3988/intrusion-detection-system-ids
6. https://www.alienvault.com/solutions/intrusion-detection-system