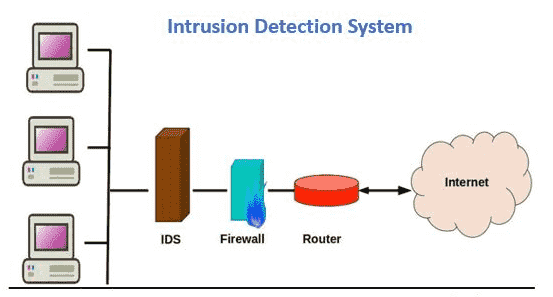
## Synopsis

## Network intrusion detection system



**Abstract** :

Computer networks are exposed to cyber related attacks due to the common usage of the internet, as the result of such, several intrusion detection systems (IDSs) were proposed by several researchers. Among key research issues in securing networks is detecting intrusions. It helps to recognize unauthorised usage and attacks as a measure to ensure the network’s security. Various approaches have been proposed to determine the most effective features and hence enhance the efficiency of intrusion detection systems, the methods include, machine learning-based (ML).

The increasing occurrence of network attacks is a devastating problem for network services. Various research works are already conducted to find an effective and efficient solution to prevent intrusion in the network in order to ensure network security and privacy. Machine learning is an effective analysis tool to detect any anomalous events occurring in the network traffic flow.

**Nutshell :**

Worldwide, the Internet is connected across the country. There are threats of network attacks in this Internet environment. The risk of integrity and confidentiality has also increased with the density of information and global reach. Security breach has become too easy. These days the improvement of network security is therefore highlighted. Protection of the Network allows the unintended interference to some form to network and avoid it. It consists of software for network intrusion detection that tracks the network. NIDS is positioned in the network in a strategic location to track tra c inside the network from source to destination apps. The machine would optimally screen both inbound and outbound tra c, but that would create congestion that would hinder the system's overall pace. Finally, these methods include machine learning algorithms that render the device exible and deliver reliable performance. Intrusion activities leave evidence in the auditing data, so it is possible to learn and distinguish the pattern of ordinary and malicious activities with machine learning algorithms. Machine training techniques can learn normal, anomalous patterns from training data, and create classi ers for computer system attacks.

**HISTORY**

The main aim of intrusion detection is monitoring the network assets to detect anomalous behaviour and misuse in network. Intrusion detection was first introduced in early 1980’s after the evolution of internet. Since then, several events in IDS technology have advanced intrusion detection to its current state. James P Anderson's, a pioneer in information security and member of the Defense Science Board Task Force on Computer Security at the U.S. Air Force, produced “Computer Security Threat Monitoring and Surveillance,” a report that is often credited with introducing automated IDS. During the late 1980’s, with a growing number of shared networks, enterprise system administrators all over the world began adopting intrusion detection systems. In the 1990’s, IDS technology improved to address the increasing number and sophistication of network attacks. Big data also plays an important role in the growth and importance of intrusion detection today. The world’s data doubles every 20 months, and as cloud-hosted databases expand exponentially, it’s no wonder IDS is more important than ever.At Threat Stack, we’re honored to play an important role in this evolution and to support the IDS community There are a variety of tools providing a certain level of comfort with acceptable risks used in the defence and surveillance of computer networks. Defence-in-Depth is a term encompassing comprehensive analyst training, hardware deployed in strategic positions and a strong security policy necessary for achieving this objective. Every day, we have tools at our disposal to reach this goal. The aggregation of data comes from routers, the host itself, firewalls, virus scanners and a tool strictly designed to catch known attacks; an Intrusion Detection System (IDS).

**INTRUSION DETECTION**

Intrusion detection is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

**INTRUSION DETECTION ATTACKS**

**A. Denial-of-Service (DOS) Attacks** There are two main types of denial of service (DoS) attacks: flooding and flaw exploitations. Flooding attacks can often simply implement. For example, one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim. As another example, a SYN flood attack sends a flood of TCP/SYN packets with a forged source address to a victim. This will cause the victim to open half open TCP connections - the victim will send a TCPSYN/ACK packet and wait for an ACK in response. Since the ACK never comes, the victim eventually will exhaust available resources waiting for ACKs from a nonexistent host.

**B. Eavesdropping Attacks** It is the scheme of interference in communication by the attacker. This attack can be done over telephone lines or through email.

**C. Spoofing Attacks** This attacker portrays another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker.

**D. Intrusion attacks or User to Root Attack (U2R)** An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data.

**E. Logon Abuse Attacks** A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages.

**F. Application-Level Attacks** The attacker targets the disabilities of the application layer.

**CAUSES OF INTRUSION IN NETWORK**

We observed some commonly occurred causes of intrusion in a network. These are as follows.

a. Bad packets (produced from corrupt domain name system (DNS) data, software bugs) and local packets may not be detected significantly, which causes high false-alarm rates (false positive).

b. The encrypted packets may cause intrusion, which is not preventive without effective IDS.

c. IDS may not effectively imply the identification and authentication for weak access in the network. When an attacker gains admittance due to a soft authentication mechanism, then IDS is preventive for the misconduct.

d. NIDS systems can be subject to some protocol-based attacks, then hosts in that network may be vulnerable to illegal data, and Transmission Control Protocol/Internet Protocol (TCP/IP) stac

**Work :**

Machine Learning Algorithms will be applied on Datasets of IDS for accuracy and prediction. It will also help in analysing and visualisation of datasets.

**FUTURE SCOPE**

IDS implementation depends on the deployment success. Planning is important for the design and implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS. The decision can vary between organisations. A network based IDS is an immediate choice for many organisations because of its ability to monitor multiple systems and also the fact that it does not require a software to be loaded on a production system unlike host based IDS. Some of the organisations provide hybrid solutions. So, the available resources are needed for a system before installing a host based sensor. The IDS technology is still reactive rather than proactive and this technology works on attack signatures. Signatures are defined as a pattern of attacks which is defined earlier. The signature database needs to be updated whenever a different kind of attack is detected and they are fixed in the database and the frequency of signature update varies from vendor to vendor.