Subject: Information and Communication Technology (ICT)
Topic: Intrusion Detection System
Lesson: One
Teacher: Chinyere **.**E. Ikpah
Class: Senior Secondary Class 2
Duration: 80 Minutes

Objectives:

At the end of this lesson, students should be able to:

- define the term intrusion detection system (IDS),
- describe brief concept of (IDS),
- explain the Classification of (IDS),
- explain detection methods of IDS,
- explain advantages and disadvantages of IDS.

Introduction

For years now, network security has been one of the main investments organizations of all sizes make to protect their networks, users and data.

Much of this focus has come about to address the sheer volume and sophistication of cyber threats in today's landscape. The rise of malicious actors seeking to compromise data, steal information, disrupt services and cause damage has led to the implementation of numerous defense strategies, practices and technologies.

Encrypting data, using firewalls to prevent unauthorized traffic entering the network, employing antimalware solutions and a variety of other tools are upheld as a standard for more or less every organization, and are used to detect cyber attacks and ultimately stop them. Another tool that is just as universal is the IDS, or intrusion detection system. Next to packet analysis, log aggregation, proxy firewalls and similar blue team tools, IDS is an indispensable tool for defense teams to detect attacks.

Intrusion detection systems have been around for decades, and while they've gone through many iterations and innovative advancements, the IDS still stands as a fundamental part of good cyber hygiene. Just as a home alarm system is designed to alert you to an intruder's attempt at breaking in, IDS will in the same way monitor network traffic and notify you of suspicious activity.

What is intrusion?

An intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality, availability of a resource.

Intrusion Detection System (IDS)

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administrator. IDS monitor a network or system for malicious activity and protect a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between ‘bad connections’ (intrusion/attacks) and ‘good (normal) connections’.

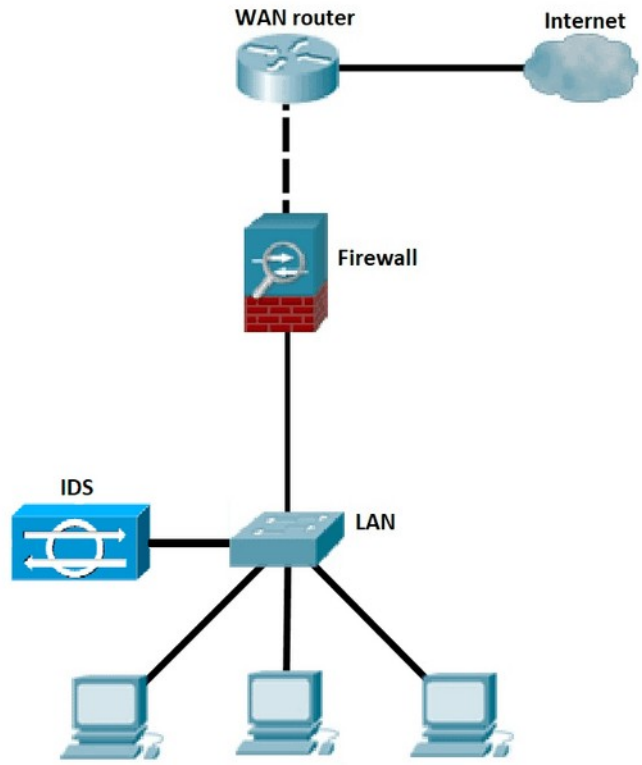

Fig 1: Overview of Intrusion Detection System

Concept of intrusion detection

Anderson at the NSA with his "Computer Security Threat Monitoring and Surveillance" report. Then, in 1986, Dorothy E. Denning wrote "An Intrusion-Detection Model"—an academic paper that shaped the foundation for many systems still in use today. The model presented in the paper was used to develop the Intrusion Detection Expert System, or IDES.

The IDES model detected behaviour patterns of a potential intruder by using statistics for anomaly detection based on profiles of users, host systems, and target systems. The earliest concept of intrusion detection systems was set forth in 1980 by James

From the 1980s all the way to the early 2000s, IDS was considered a security best practice. But, at that time, the noisy and turbulent nature of networks led to many false positives from IDS, labeling it unreliable in the eyes of many.

In recent years, however, their dominance and the challenges of cloud computing have shined a new light on intrusion detection systems, a longtime staple of enterprise security. And while many organizations invest in proactive security measures and other preventative strategies, they can still fail. Detecting attacks that may occur afterwards remains crucial.

How an IDS work

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detect something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Classification of Intrusion Detection System

IDS are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

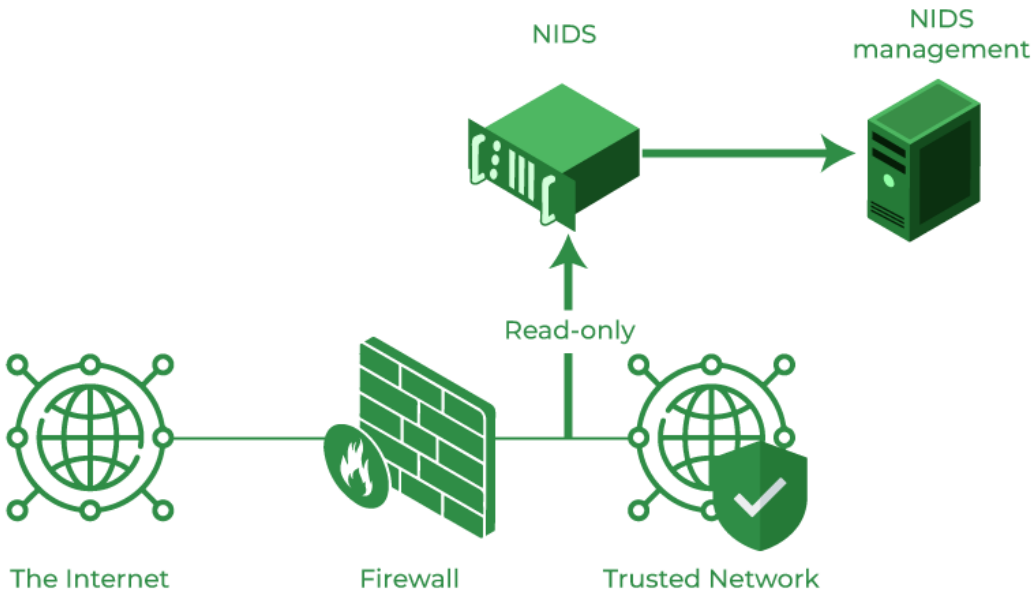

Fig 2: Network Intrusion Detection System architecture.

- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

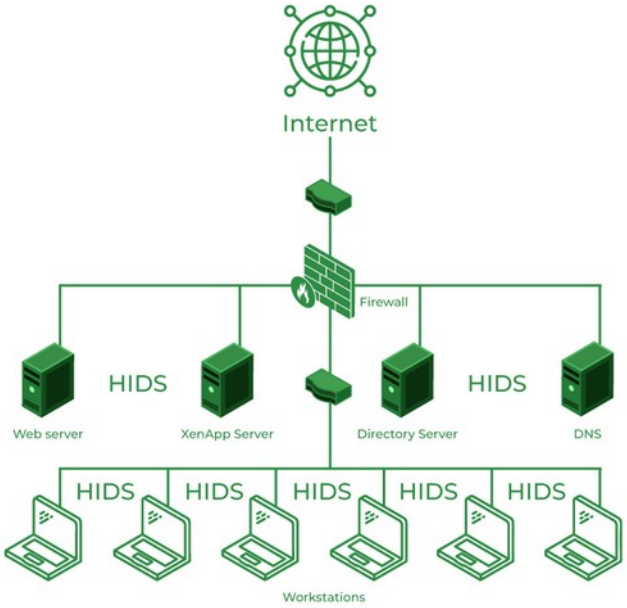

Fig 3: Host Intrusion Detection System architecture.

- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the Hypertext Transfer Protocols (HTTPs) stream and accepting the related HTTPs. As HTTPs is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPs.

- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL (Structured query language) protocol explicitly to the middleware as it transacts with the database in the web server.

- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS

1. **Signature-based Method:** Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
2. **Anomaly-based Method:** Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.
3. **Hybrid Detection Method:** A Hybrid method uses both Signature and Anomaly-based intrusion detection methods together. However, the main reason behind the development of a hybrid detection system is to identify more potential attacks with fewer errors.

Advantages and Disadvantages of IDS

Advantages

- **Response capabilities:** Though they probably will be of limited use, you may require allowing some of the response aspects of the IDS. For example, they can be organized to end a user session that disrupts policy. Definitely, you must consider the threats of taking this step, as you may unintentionally end a lawful user session. Though, in some cases, it can be a key tool to avoid harm to the network.

- **Visibility:** An IDS offers a clear view of what is going on your computer or network. It is a valuable basis of information about malicious or suspicious network traffic. There are some useful options to IDS which enable you to monitor network traffic in depth.

- **Tracking of virus transmission:** As soon as virus first hits your network system, IDS will inform which mechanisms it compromised, as well as how it is spreading through the network system to infect other mechanisms. This can be much helpful in stopping or slowing a virus's growth and ensuring you remove it.

- **Defence:** An Intrusion detection system adds a defense layer to your security profile, offering a valuable backstop to some of your other security procedures.

- **Evidence:** Appropriately configured IDS can generate data that can form the basis for a criminal or civil case against someone who exploits your network.

Disadvantages

- **More maintenance:** Unluckily, an Intrusion detection system does not replace a virus scan, firewall or any other security measure. Therefore, when you install it, it will need extra maintenance effort and will not remove much, if any, of the present problem.

- **Personnel requirements:** Managing IDS needs qualified personnel. The less qualified your personnel are, the more duration they will spend responding to false positives. So you will be making not only more work for the IT department to manage but more tough work in some cases.

- **False positives:** IDSs are known for situation of false positives, i.e., sounding the alert when nothing is amiss. Though you can pull the situations to decrease the number of false positives, you'll never entirely remove the requirement to respond to false positives.

- **False negatives:** Intrusion detection systems can also fail to detect intrusions. Day by day technologies are improving, and IDSs may not necessarily catch everything. This means, it is not all the systems you need to be protected. You need to use more solutions.

Summary:

In this lesson, we were able to:

- ❖ define the term intrusion detection system (IDS),
- ❖ describe brief concept of (IDS),
- ❖ explain the Classification of (IDS),
- ❖ explain detection methods of IDS,
- ❖ explain advantages and disadvantages of IDS.

Evaluation:

1 What is the correct name for device or software application that monitors a network system for malicious activity or policy violation sends only alert?

A. Intrusion defensive system.
B. Intention detection system.
C. Intrusion detection system.
D. Intention defensive system.

2 Where, is an IDS commonly placed in a network?

A. In front of the firewall

B. In line with the firewall
C. In promiscuous mode
D. On the end users device

3 IDS are classified into how many types?

A. Two
B. Three
C. Four
D. Five

4 Which system is set up at a planned point within the network to examine traffic from all devices on the network?

A. Host Intrusion Detection System
B. Protocol-based Intrusion Detection System
C. Application Protocol-based Intrusion Detection System
D. Network Intrusion Detection System

5 What is the full meaning of the acronym **NIDS?**

A. Network Intrusion Declaration system
B. Network Instruction Detection System
C. Network Intrusion Detection System
D. Network Instruction Declaration System