Security in Network

Threats in Network

An isolated home user or a stand-alone office with a few employees is an unlikely target for many attacks. But add a network to the mix and the risk rises sharply.

7 Common Network Security Issues

Internal Security Threats

Over 90% of cyberattacks are caused by human error. This can take the form of phishing attacks, careless decision-making, weak passwords, and more.

Insider actions that negatively impact your business's network and sensitive data can result in downtime, loss of revenue, and disgruntled customers.

Distributed Denial-Of-Service (DDoS) Attacks

Rogue Security Software

Rogue security software tricks businesses into believing their IT infrastructure is not operational due to a virus. It usually appears as a warning message sent by a legitimate anti-malware solution

Malware(malicious software programs)

Ransomware

Phishing Attacks

Viruses

Network Security Controls

Network Security Controls are used to ensure the confidentiality, integrity, and availability of the network services.

These network security controls include:

- Access Control
  how a subject can access an object.
- Identification
  dentification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most common technique used in authenticating the users in the network and applications. Users have a unique User ID, which helps in identifying them.
- Authentication
  Authentication refers to verifying the credentials provided by the user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. A typical user authentication consists of a user ID and a password. The other forms of authentication are authenticating a website using a digital certificate, comparing the product and the label associated with it.
  Example: Password, PIN, etc.
- Authorization
  Authorization refers to the process of providing permission to access the resources or perform an action on the network. Network administrators can decide the access permissions of users on a multi-user system. They even decide the user privileges. The mechanism of authorization can allow the network administrator to create access permissions for users as well as verify the access permissions created for each user.
- Accounting
  User accounting refers to tracking the actions performed by the user on a network. This includes verifying the files accessed by the user, functions like alteration or modification of the files or data. It keeps track of who, when, how the users access the network. It helps in identifying authorized and unauthorized actions.
- Cryptography
- Security Policy

What is a Firewall?

IDS are classified into 5 types:

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching.

Network Intrusion Detection System (NIDS): 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.

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.

Protocol-based Intrusion Detection System (PIDS):
Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server.

Application Protocol-based Intrusion Detection System (APIDS):
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.

Comparison of IDS with Firewalls:
IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Application layer security

Application layer security refers to ways of protecting web applications at the application layer (layer 7 of the OSI model) from malicious attacks.

Since the application layer is the closest layer to the end user, it provides hackers with the largest threat surface. Poor app layer security can lead to performance and stability issues, data theft, and in some cases the network being taken down.

Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as web application firewalls (WAFs), secure web gateway services, and others.

Transport **layer security**

Transport Layer Security (TLS) is a way to secure information as it is carried over the Internet: users browsing websites, emailing, instant messaging, and conversing via Voice Over IP (VoIP). TLS is the successor to Secure Sockets Laye (SSL) and the security it provides is a cornerstone of the modern Internet.

The goal of TLS is to provide a private and secure connection between a web browser and a website server. It does this with a cryptographic handshake between to two systems using public-key cryptography (PKC). They two parties to the connection exchange a secret token, and once this token is validated by each machine it is used for all communications. The connection employs lighter symmetric cryptography to save bandwidth and processing power.

Network layer security

Network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet because they can provide protection for many applications at once without modifying them.

In the earlier chapters, we discussed that many real-time security protocols have evolved for network security ensuring basic tenets of security such as privacy, origin authentication, message integrity, and non-repudiation.

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec