AFRICAHACKON

DISCLAIMER

All materials provided in this Cybersecurity Training Program, whether online or physical, are the intellectual property of AfricaHackOn and Cyber Guard Africa. Unauthorized sharing, reproduction, or distribution is strictly prohibited and may result in legal action.

By participating, you agree to use the materials solely for this program and comply with copyright laws.

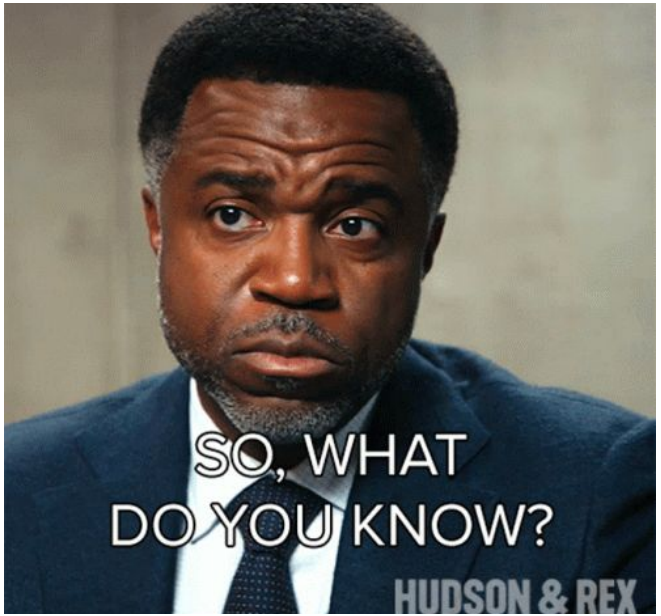
For inquiries, contact academy@africahackon.com

AFRICAHACKON

AH 200
NETWORK SECURITY

By: Samuel Mutuku & Stacy Alwanga

www.africahackon.com



What do you know about Network Security?

AFRICAHACKON

What you will learn…

1. Computer Networks Overview
2. OSI Model Overview
3. Introduction to Network Security
4. Multi-Layered Network Security

AFRICAHACKON

MODULE 1:
COMPUTER NETWORKS OVERVIEW

By : Samuel Mutuku & Stacy Alwanga

https://africahackon.com/

AFRICAHACKON

Computer Networks Overview

A **Computer Network** is a group of interconnected nodes or computing devices that exchange data and resources with each other.

A network connection between these devices can be established using a cable or wireless connection.

The following are certain building blocks that make computer network operations possible;

1. **Network Devices** - Nodes are physical devices, also known as nodes, that are data communication equipment connected within a computer network.
2. **Links** - This is a transmission medium that connects nodes and allows them to communicate with one another
3. **Protocols** - These are rules that all network nodes and links must follow when transmitting data.

AFRICAHACKON

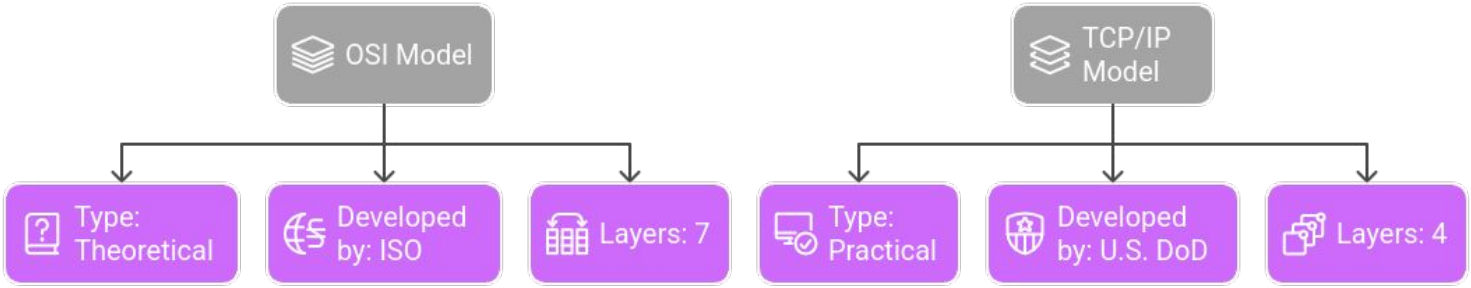
MODULE 2:
OSI Model Overview

By : Samuel Mutuku & Stacy Alwanga

https://africahackon.com/

OSI Model Overview

- **The OSI model (Open Systems Interconnection model)** is a conceptual framework used to understand and standardize how different computer systems communicate over a network. It divides the communication process into 7 layers, each with specific roles.
- The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is a **real-world, practical model** used for network communications — it's the foundation of the **modern Internet**.



AFRICAHACKON

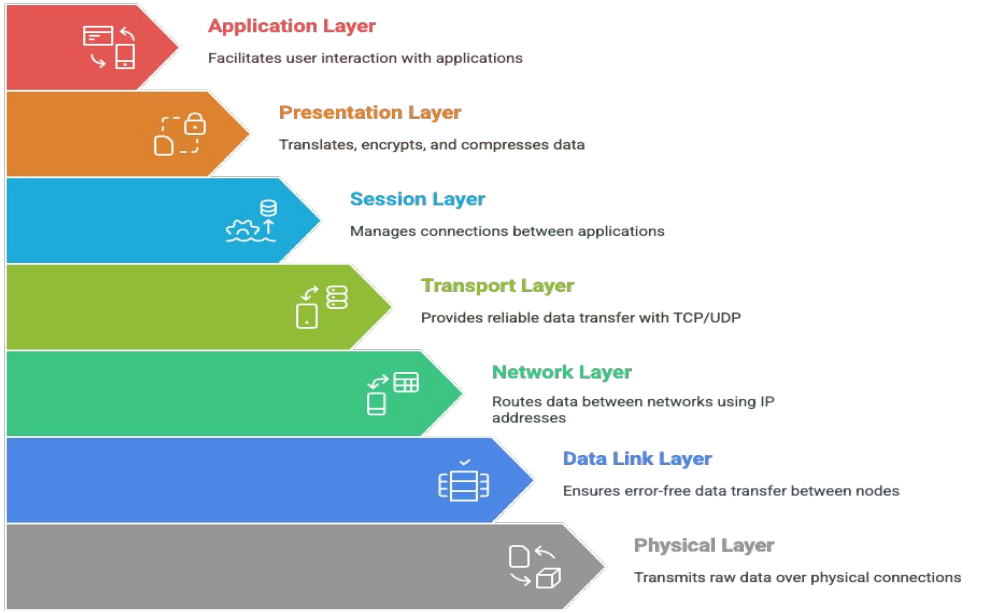
Real Life Example of TCP/IP

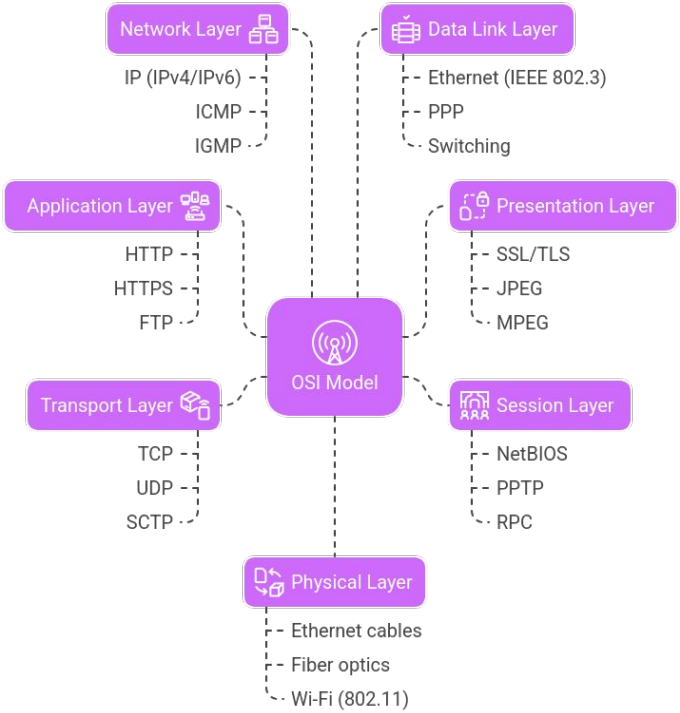
When you visit a website:

1. **Application** – Your browser uses HTTP to request a page.
2. **Transport** – TCP ensures the request reaches the server reliably.
3. **Internet** – IP finds a path to the server (via routers).
4. **Network Access** – Data is sent over Ethernet/Wi-Fi hardware.

AFRICAHACKON

OSI Model Overview





AFRICAHACKON

Importance of the OSI Model

- Helps understand how data moves through a network.
- Aids in **troubleshooting**, **network design**, and **security analysis**.
- Each layer serves the one above it and is served by the one below.

AFRICAHACKON

MODULE 3:
Introduction To Network Security

By : Samuel Mutuku & Stacy Alwanga

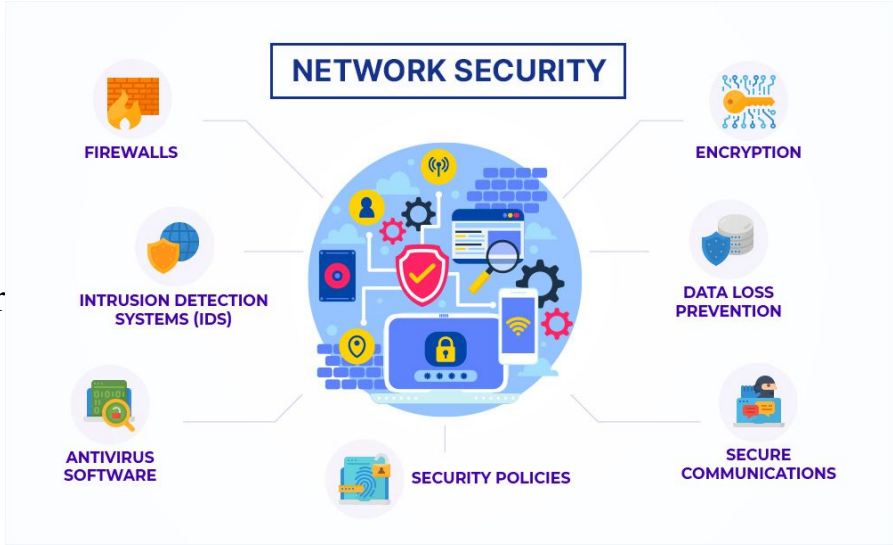
https://africahackon.com/

AFRICAHACKON

Introduction to Network Security

Network Security refers to the technologies that are intended to safeguard the integrity and usefulness of your data and network.

Network security aims to protect a computer network from unauthorized access, misuse or attacks.

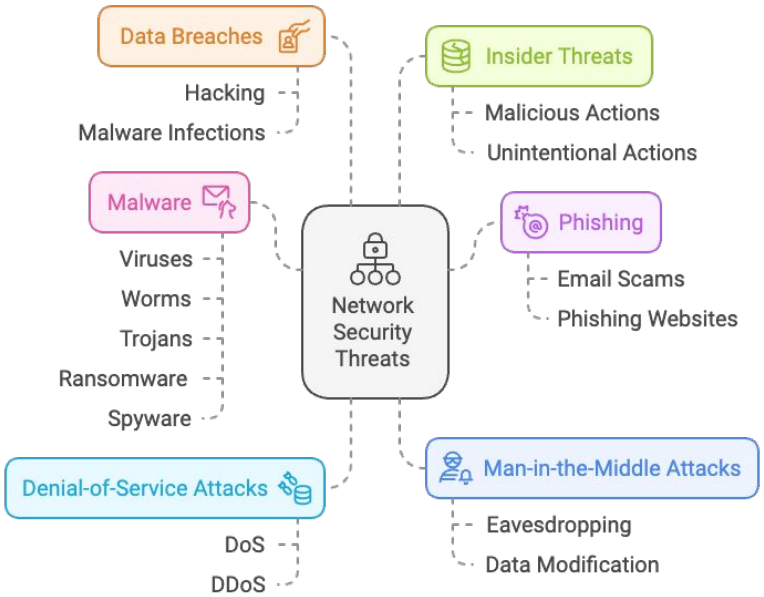


AFRICAHACKON

Network Security Threats

The following are different types of Network Attacks;

1. Data Breaches
2. Malware
3. Denial of service attacks
4. Insider Threats
5. Phishing
6. Man-in-the-middle attacks



Key Objectives in Network Security

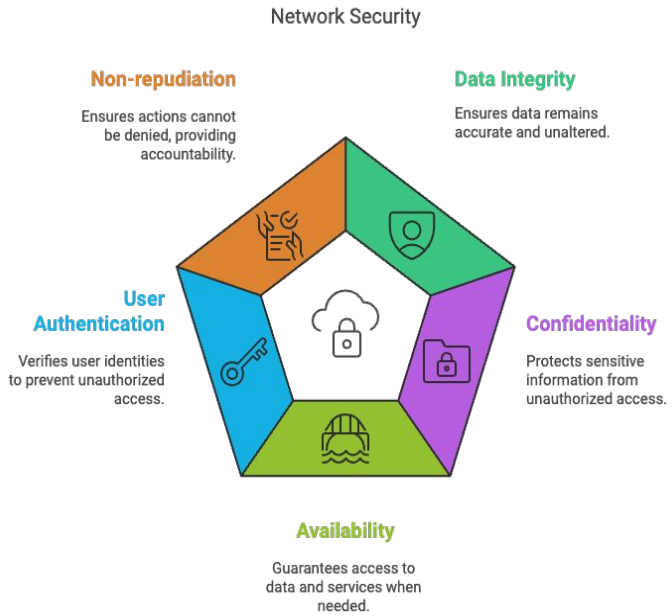
•**Confidentiality**: Ensuring sensitive information is only accessible to authorized users and protecting it from unauthorized disclosure.

• **Integrity**: Maintaining data reliability and trustworthiness to prevent unauthorized modifications.

• **Availability**: Ensuring consistent and reliable access to data and services for uninterrupted business operations.

• **Authentication**: Verifying user identities before granting access to prevent unauthorized access.

• **Non-repudiation**: Ensuring that neither sender nor receiver can deny the authenticity of their communications.



How Does Network Security Work?

How Network Security Works

Network security employs multiple layers of protection, both at the network perimeter and within its internal systems. Each layer enforces rules and controls that govern access to network resources, ensuring the security of vast amounts of stored and transmitted data.

Levels of Network Security

1. **Physical Network Security**
   - Prevents unauthorized personnel from accessing network hardware (e.g., servers, routers, data centers).
   - Uses security measures such as biometric authentication, keycards, and surveillance systems.
2. **Technical Network Security**
   - Protects data stored within the network and during transmission.
   - Utilizes firewalls, encryption, intrusion detection/prevention systems (IDS/IPS), and VPNs.
3. **Administrative Network Security**
   - Manages user behavior and access authorization.
   - Implements policies such as role-based access control (RBAC), multi-factor authentication (MFA), and regular security audits.

AFRICAHACKON

Importance of Network security

- It ensures network sophistication and suggests necessary infrastructure amendments.
- Importance of Network Security: Protects sensitive data and intellectual property.
- Prevents unauthorized access and cyberattacks.
- Ensures the integrity, confidentiality, and availability of network systems.

AFRICAHACKON

MODULE 4:
Multi-Layered Network Security

By : Samuel Mutuku & Stacy Alwanga

https://africahackon.com/

AFRICAHACKON

Multi-Layered Network Security Overview

Multi-layered security is a security architecture where you do not rely on a single control to protect your environment.
Instead, you use **multiple, independent, overlapping layers** of security so that:

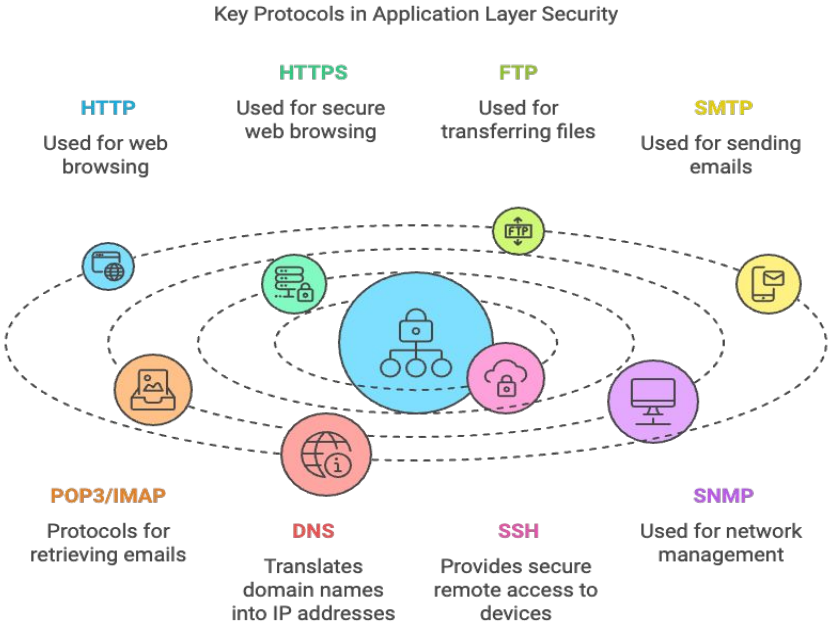
- if one layer fails, others still protect the system
- attackers are slowed, giving defenders more time to detect
- security is resilient, not dependent on perfect configuration
- each layer compensates for weaknesses in another

AFRICAHACKON

Application Layer Overview

Key Functions:

- **User Interface:** Provides a user-friendly interface for interacting with network applications.
- **Protocol Selection:** Chooses the appropriate protocol for a specific task.
- **Data Presentation:** Formats and presents data in a human-readable format.



Application Layer - Email Security Attacks

Email Security is paramount in today's digital age. It involves safeguarding sensitive information and preventing unauthorized access to email accounts and data.

Common Email Security Threats:

Phishing: Deceiving users into revealing personal information.
Social Engineering: Manipulating individuals to gain access to sensitive data.
Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
Ransomware: Encrypting data and demanding payment for decryption.
Malware: Malicious software that can damage systems or steal data.
Spoofing: Disguising as a legitimate sender to trick recipients.

Man-in-the-Middle Attacks: Intercepting and manipulating communication between two parties.
Data Exfiltration: Stealing sensitive data from email accounts.
Denial of Service: Overwhelming email servers to disrupt service.
Account Takeover: Gaining unauthorized access to email accounts.
Identity Theft: Stealing personal information to impersonate someone.

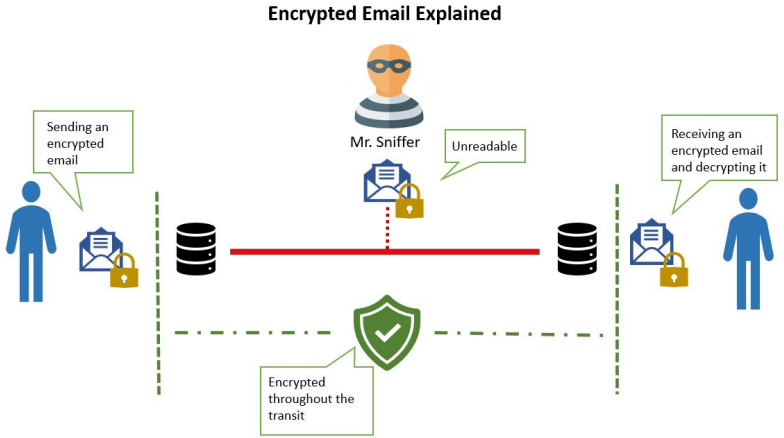
Application Layer - Email Security

Encryption:

Email Encryption ensures that email content remains confidential and inaccessible to unauthorized users.

Email Encryption Protocols:

- S/MIME and PGP are common protocols for email encryption.
- Both offer security features like encryption, digital signatures, and message authentication.
- Ensuring email content remains confidential and inaccessible to unauthorized parties.



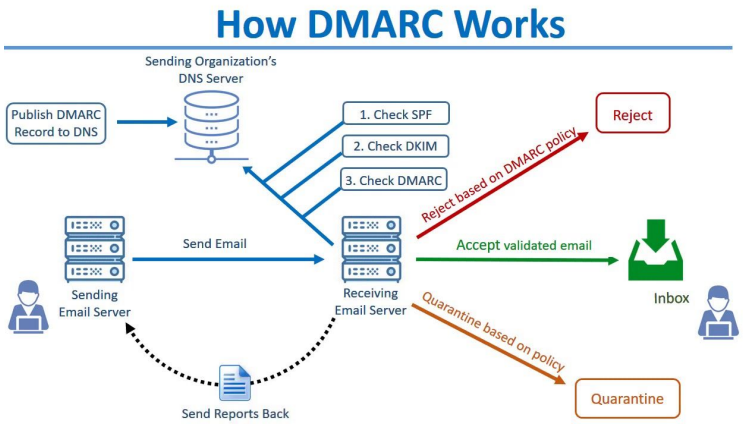
Application Layer - Email Security

Authentication:

Verifying the sender's identity helps prevent spoofing and phishing attacks. This can be done using techniques like DKIM, SPF, and DMARC.

Email Authentication Techniques

- **DKIM (DomainKeys Identified Mail)** adds digital signature to verify email origin.
- **SPF (Sender Policy Framework)** identifies authorized IP addresses for email sending.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)** aligns DKIM and SPF policies and reports on email authentication results.



Application Layer - Email Security

Email security can also be practiced in the following ways:

- **Message Integrity:** Ensuring emails aren't tampered with using cryptographic hashes or digital signatures.
- **Spam Filtering:** Blocking unsolicited emails to reduce malware and phishing risks.
- **Phishing Awareness:** Educating users about phishing scams and their identification.
- **Two-Factor Authentication (2FA):** Providing two forms of identification to prevent unauthorized account access.
- **Secure Email Protocols:** Using protocols like S/MIME, PGP, and DKIM for encryption, digital signatures, and message authentication.

Application Layer - DNS Security

• DNS Security Protects Domain Name System (DNS) from attacks compromising internet traffic integrity.

• Converts human-readable domain names into numerical IP addresses.

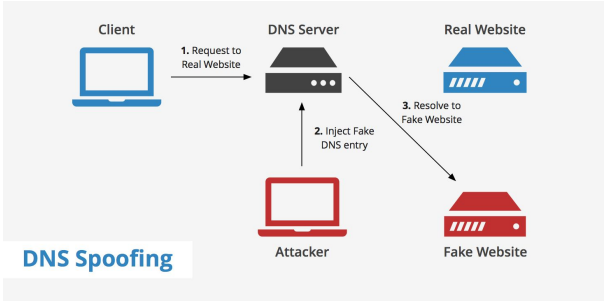
• Cybercriminals can infiltrate DNS, send users to malicious sites, steal data, hijack websites, or inundate servers.

• Different types of DNS-based attacks exist.

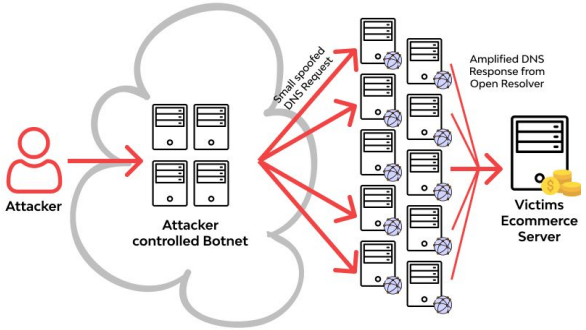
AFRICAHACKON

Application Layer - DNS Security Attacks

DNS Spoofing
DNS spoofing is an attack where an attacker manipulates DNS records to redirect users to malicious websites. This can lead to phishing attacks and malware distribution. DNS security is crucial in protecting the Domain Name System (DNS) from attacks that compromise internet traffic integrity.



DNS Amplification Attacks
DNS Amplification Attacks exploit vulnerabilities in DNS servers to launch large-scale DDoS attacks, disrupting online services like websites and gaming servers by overwhelming the target network with traffic.

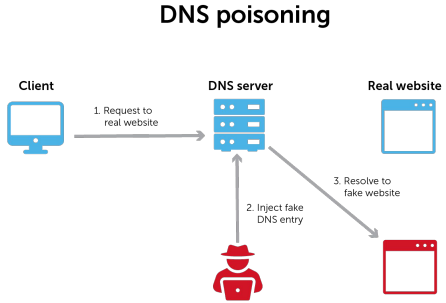


DNS Amplification Attack

Application Layer - DNS Security Attacks

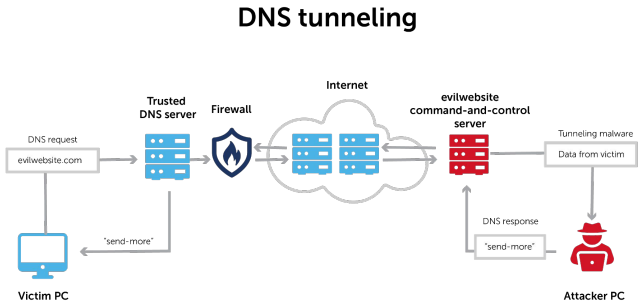
DNS Cache Poisoning

DNS cache poisoning is a malicious attack where false DNS records are injected into a resolver cache, leading to redirect to malicious sites, phishing attacks, malware distribution, and compromised DNS resolution integrity.



DNS Tunneling

DNS tunneling is a cyber attack technique where attackers embed hidden messages or data within DNS queries, bypassing security measures and stealing sensitive data.

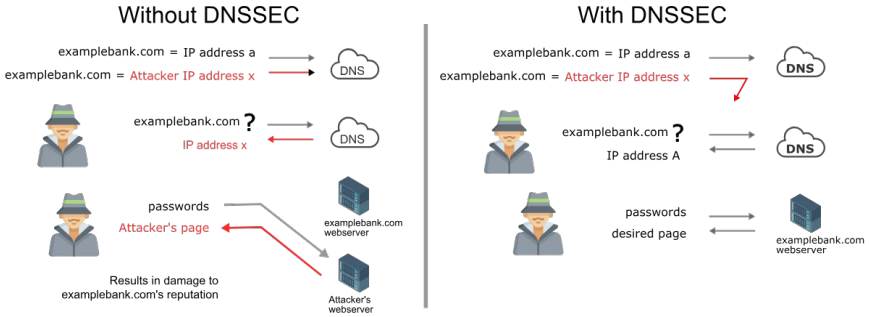


AFRICAHACKON

Application Layer - DNS Security

DNSSEC (DNS Security Extension)

DNSSEC adds a digital signature to DNS records to verify their authenticity, preventing DNS spoofing attacks and protecting users from being redirected to malicious websites.



- **DNS Filtering:** Blocks access to malicious domains and IP addresses.
- **DNS Monitoring and Logging:** Tracks DNS traffic to detect suspicious activity.
- **Web Application Firewall:** Blocks malicious DNS queries and provides advanced threat detection.
- **Regular Updates and Patches:** Ensures protection against vulnerabilities and strengthens DNS infrastructure security.
- **Employee Training:** Educates employees about DNS attacks and empowers them to identify suspicious activity.

Application Layer - Web Security

Web Security is the practice of protecting websites and their users from cyber threats.

Web Security utilizes various techniques to safeguard data and prevent unauthorized access.

It prevents hacking, malware, unauthorized data access, and denial-of-service attacks.

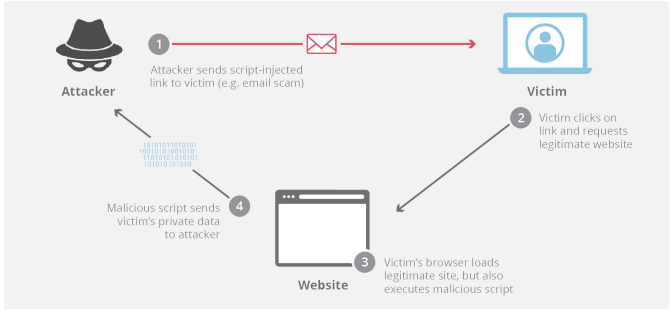
Ensures confidentiality, integrity, and availability of web application data.

Application Layer - Web Security Attacks

The following are common web based attacks

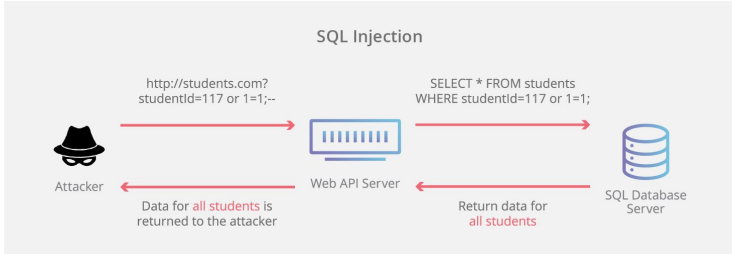
Cross-Site Scripting(XSS)

XSS attacks exploit vulnerabilities in web applications to inject malicious scripts into web pages. These scripts can be used to steal user information, hijack sessions, or redirect users to malicious websites.



SQL Injection (SQLi)

SQLi attacks target vulnerabilities in database queries, allowing attackers to inject malicious SQL code and gain unauthorized access to sensitive data. This can lead to data breaches, identity theft, and other harmful consequences.

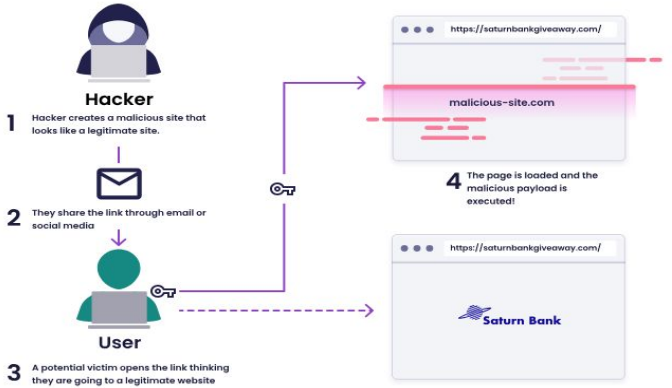


AFRICAHACKON

Application Layer - Web Security Attacks

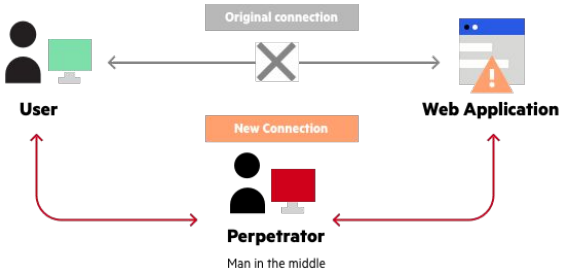
Cross-Site Request Forgery (CSRF)

CSRF attacks exploit the trust relationship between a user and a website to trick users into performing actions they did not intend. By exploiting authenticated sessions, attackers can force users to execute malicious actions without their knowledge or consent.



Man-in-the-Middle (MITM)

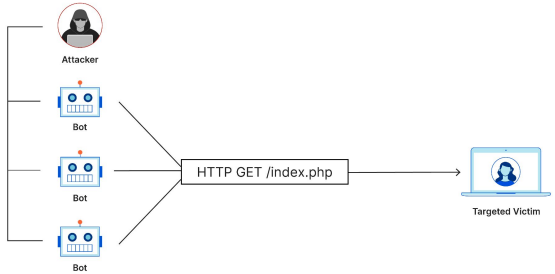
MITM attacks involve an attacker intercepting communications between a user and a website, allowing them to eavesdrop on data, steal information, or manipulate the communication. This can be achieved by compromising network infrastructure or using social engineering techniques.



Application Layer - Web Security Attacks

Distributed Denial of Service (DDoS)

DDoS attacks overwhelm a website or server with a flood of traffic, making it unavailable to legitimate users. These attacks can be launched from multiple sources and can cause significant disruption to online services.



Server-Side Request Forgery (SSRF)

SSRF is a web security vulnerability that allows an attacker to make requests on behalf of the server, potentially leading to unauthorized access to internal resources or other systems. This can happen when a web application fails to properly validate or sanitize user-supplied inputs that are used to construct URLs or requests.

Application Layer - Web Security Strategies

Web Application Firewall (WAF)

• Acts as a security gateway, filtering and inspecting HTTP traffic.

• Protects against common web application attacks like SQL injection, cross-site scripting, and DDoS attacks.

• Can be deployed as hardware appliances, software, or cloud-based services.

SSL/TLS Certificates

• Encrypt data transmitted between a web server and a client's browser.

• Protect sensitive information like credit card numbers and login credentials.

Application Layer - Web Security Strategies

Penetration Testing

• Proactive security measure that simulates cyberattacks to identify vulnerabilities.

• Helps identify potential weaknesses before they can be exploited by malicious actors.

Security Scanning Tools

• Automated software applications that efficiently identify vulnerabilities in web applications.

• Analyze the application's code, network traffic, and configuration to detect potential security risks.

Application Layer - Web Security Strategies

Secure Coding Practices

• Essential for preventing security vulnerabilities from being introduced into web applications.

• Follows guidelines like the OWASP Top 10 to write code more resistant to attacks.

Monitoring Tools

• Essential for maintaining the security and performance of web applications.

• Helps detect security incidents, investigate attacks, monitor application performance, identify vulnerabilities, and ensure compliance with security regulations.

Network Layer Security Attacks

- The network layer is responsible for routing data packets between networks.
- Attacks at this layer can disrupt communication, steal data, or compromise the integrity of network traffic.

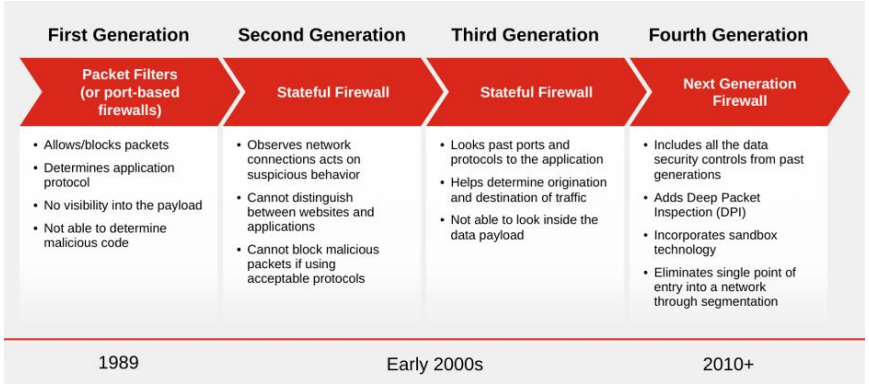
The following are various types of attacks at the network layer.

- DoS attacks overwhelm networks with excessive traffic, making them unavailable to legitimate users.
- DDoS attacks launch from multiple sources simultaneously, making mitigation difficult.
- Man-in-the-Middle (MitM) attacks intercept and alter communication, allowing attackers to eavesdrop or inject malicious content.
- IP spoofing disguises malicious traffic source, IP address spoofing confuses routing protocols, and route poisoning injects false routing information.
- ARP spoofing associates malicious devices with legitimate IP addresses, intercepting traffic.

Network Layer Security Implementations

Firewalls:

- A firewall is a device that prevents unauthorized access to private networks or computers.
- Filters traffic to block malicious packets.
- Can be hardware, software, or a mix of both.
- Types: Hardware Firewalls (permanent network protection) and Software Firewalls (single device protection).
- Next-Generation Firewalls (NGFWs) offer additional features beyond packet filtering, such as Deep Packet Inspection, Application Control, Intrusion Prevention Systems, Advanced Threat Protection, and Cloud Integration, providing a comprehensive network security approach.
- Stateless firewalls examine incoming packets independently, based on predefined rules, without maintaining connection state information. Stateful firewalls, on the other hand, maintain information about active connections, allowing or denying packets based on connection state for better security.

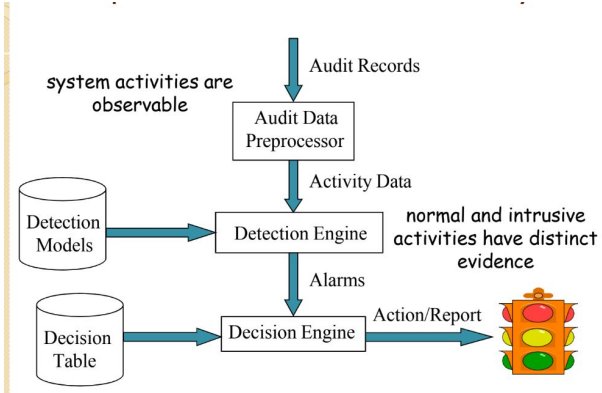


Network Layer Security Implementations

Intrusion Detection and Prevention System (IDPS)

- IDPS systems are designed to protect networks and systems from unauthorized access and malicious activity.
- They work by analyzing network traffic for patterns that indicate potential attacks, employing a combination of signature-based detection and anomaly-based detection techniques.
- **Signature-based detection** compares captured network traffic against a database of known attack signatures (patterns of malicious activity). If a match is found, an alert is triggered.
- Examples of IDS/IPS solutions include Snort, Zeek, Suricata, etc.

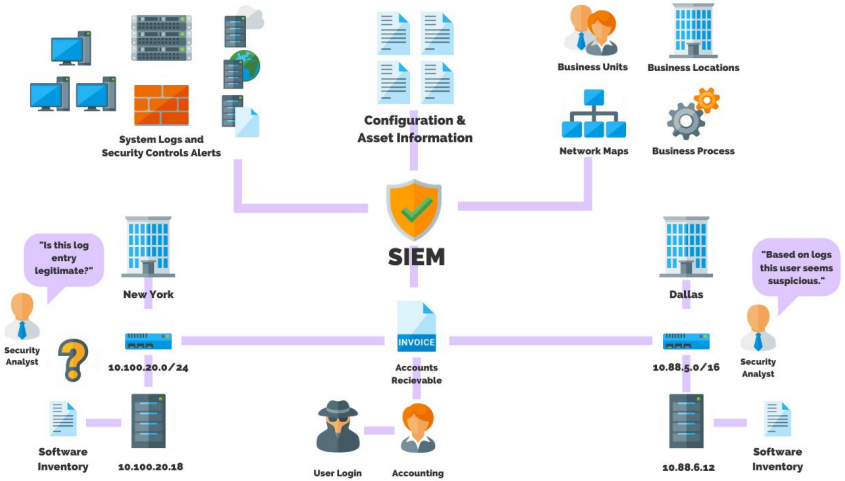
- **Anomaly-based detection** establishes a baseline of normal network behavior and detects deviations that could indicate malicious activity. Uses statistical analysis or machine learning techniques to identify anomalies. It can detect unknown threats.



Network Layer Security Implementations

Security Information and Event Management (SIEM)

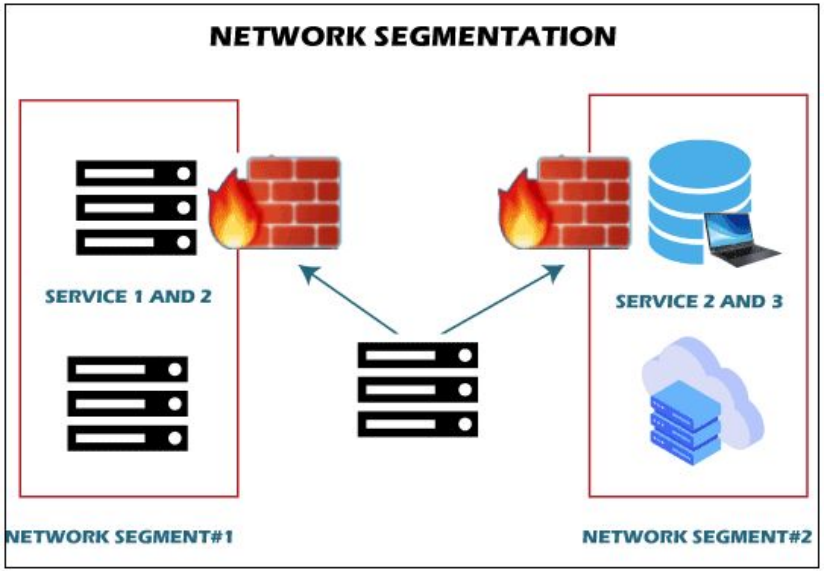
- A SIEM is a software solution that collects, analyzes, and correlates security events within an organization's IT infrastructure.
- Helps security teams identify and respond to potential threats promptly.
- Functions as a comprehensive security dashboard, detecting anomalies, investigating incidents, and ensuring compliance with regulations.
- Detects anomalies and risks, generates alerts if suspicious activity is detected.
- Provides insights into security trends and risks, aiding informed decisions for enhanced network protection.
- Examples of SIEM Solutions include Wazuh, Security Onion, Graylog, ELK Stack, etc.



Network Layer Security Implementations

Network Segmentation

Network segmentation is a security strategy that divides a network into isolated segments, limiting the spread of malware or threats. It can be achieved using VLANs, subnetting, router-based segmentation, firewall segmentation, VPN segmentation, or microsegmentation.



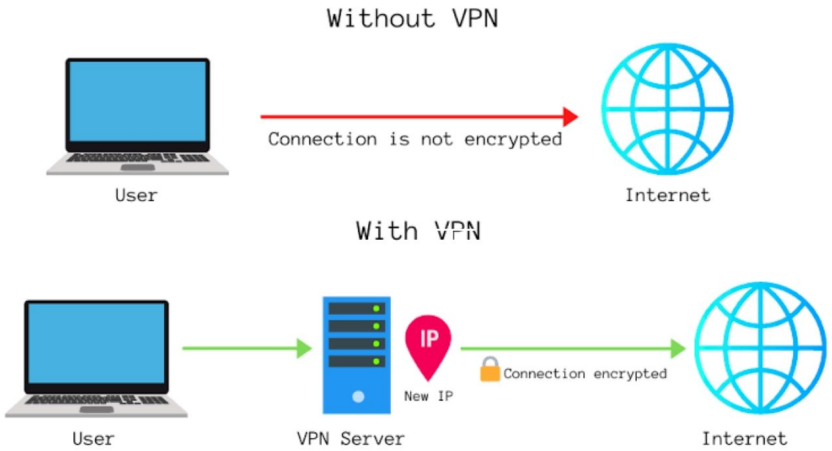
Access Control Lists (ACLs)

ACLs are crucial for network security as they offer a granular control over network access, preventing unauthorized access and protecting sensitive data. They are configured on network devices like routers, switches, and firewalls, based on criteria like Source IP Address, Destination IP Address, Source Port, Destination Port, and Protocol.

Network Layer Security Implementations

Virtual Private Network (VPN)
This is a technology that creates a secure, encrypted connection over a public network, such as the internet. This allows you to access the internet with a private IP address, protecting your online privacy and security.

VPNs come in various types: Remote Access VPNs allow individuals to connect to a corporate network remotely, Site-to-Site VPNs connect multiple offices over the internet, and Extranet VPNs provide business partners with secure access to critical information. These VPNs offer benefits like reduced costs, improved network connectivity, and enhanced security.



Data Link Layer

The Data Link Layer is the Second Layer of the OSI Model and is responsible for the transmission of data between devices on the same network, using physical addressing (MAC Addresses) to facilitate communication.

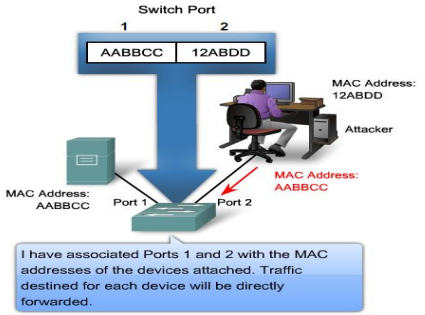
Security at this layer is crucial because it ensures data integrity and privacy as it moves between nodes on a local network. However, this layer is susceptible to a variety of attacks, which might compromise both network performance and security.

The data link layer is crucial for managing data transfer over physical connections like Ethernet or Wi-Fi, handling error detection, frame synchronization, and flow control. However, it can also be exploited by attackers to intercept, modify, or manipulate data.

Data Link Layer Attacks

MAC Address Spoofing

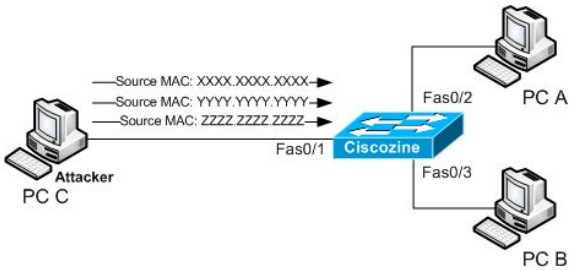
In a MAC address spoofing attack, an attacker alters the MAC address of their network device to impersonate another device on the network. This can allow the attacker to bypass access controls, monitor traffic intended for the legitimate device, or even gain unauthorized access to the network. Spoofing can also facilitate other attacks, such as man-in-the-middle (MitM) attacks, where the attacker intercepts and manipulates communications between two devices.



MAC Address Spoofing

MAC Flooding

MAC flooding is a network attack where an attacker sends a massive number of spoofed MAC addresses to a switch, overwhelming its MAC address table. When the table is full, the switch enters a fail-open mode, broadcasting all traffic to every port. This allows the attacker to capture sensitive data or disrupt network operations.

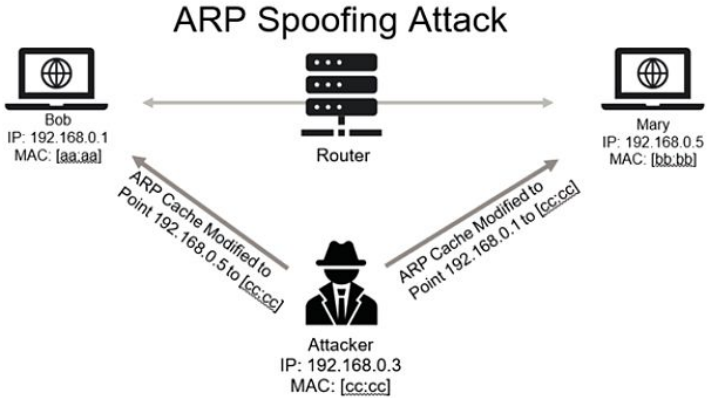


Mac Flooding

Data Link Layer Attacks

ARP Spoofing/Poisoning

In ARP spoofing, an attacker sends falsified ARP messages, tricking devices into associating the wrong MAC address with an IP address. This allows the attacker to intercept, modify, or disrupt network traffic, leading to attacks like session hijacking or denial of service (DoS). This can be done on Ettercap in Kali Linux.



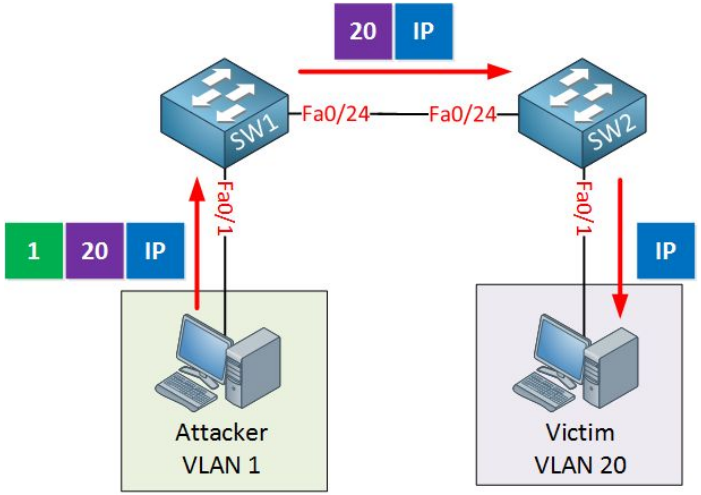
Switching Attacks

Switches, at the data link layer, direct traffic based on MAC addresses. Attackers can exploit vulnerabilities through MAC flooding, which overwhelms the switch's MAC address table, leading to a fail-open mode and sensitive data capture.

Data Link Layer Attacks

VLAN Hopping

Virtual Local Area Networks (VLANs) are used to segment network traffic for security and efficiency. However, an attacker can exploit misconfigurations in switches or VLANs to launch a VLAN hopping attack, allowing them to send traffic between different VLANs and gain unauthorized access to restricted areas of the network.



Wi-Fi Attacks

Wireless networks, which operate at the data link layer, are particularly vulnerable to attacks like Evil Twin attacks (where an attacker sets up a rogue access point to mimic a legitimate network) and Wi-Fi deauthentication attacks (which force devices to disconnect from the network, allowing attackers to intercept data during reconnection).

Data Link Layer Security Implementations

Port Security:
• Limits the number of MAC addresses associated with a specific port to prevent unauthorized devices from connecting.
• Automatically disables the port if an unauthorized MAC address is detected.

Dynamic ARP Inspection (DAI):
• Validates ARP requests and responses within a network.
• Prevents ARP spoofing attacks by ensuring only legitimate devices can communicate.

Encryption of Wireless Communications:
• Uses strong encryption standards like WPA3 to protect data transmitted over wireless networks.
• Uses Wireless Intrusion Prevention Systems (WIPS) to detect and prevent attacks.

MAC Address Filtering:
• Allows network administrators to control which devices are allowed to connect based on their MAC address.

802.1X Authentication:
• Enforces authentication at the data link layer before a device can access the network.
• Uses the Extensible Authentication Protocol (EAP) to authenticate devices.

VLAN Segmentation and Security:
• Proper VLAN configuration isolates sensitive network parts from general access.
• Uses access control lists (ACLs) and secure VLAN tagging to prevent unauthorized cross-VLAN communication.

Physical Layer

The physical layer of a network, responsible for transmitting data across cables, fibers, or wireless signals, is often overlooked in security discussions but is vulnerable to threats like cable tapping, denial-of-service attacks, and electromagnetic interference.

These attacks can disrupt network connections, eavesdrop on data, and degrade network performance, making data transmission difficult.

Physical Layer Security Implementations

To secure the physical layer, organizations should implement the following recommendations:

1. **Physical access controls**: Restrict access to network infrastructure like cables, routers, and switches by securing server rooms and wiring closets.
2. **Shielded cabling**: Use shielded twisted pair (STP) cables or fiber-optic cables, which are less susceptible to eavesdropping and interference than unshielded cables.
3. **Cable management**: Use conduits or cable locks to prevent unauthorized access and tampering.
4. **Environmental monitoring**: Deploy surveillance cameras, motion detectors, and alarms to monitor physical network infrastructure for tampering or damage.
5. **Wireless protection**: For wireless networks, use strong encryption and anti-jamming technologies to prevent signal interception and jamming attacks.

Defense in Depth

What is Defense in Depth?

Defense in Depth, often referred to as layered security, is a security strategy that employs multiple layers of protection to defend a system or network. The underlying principle is that if one layer fails, another can mitigate the risk. This approach helps to reduce the likelihood of a successful attack by making it more difficult for an attacker to penetrate all layers.

How is Defense in Depth Designed?

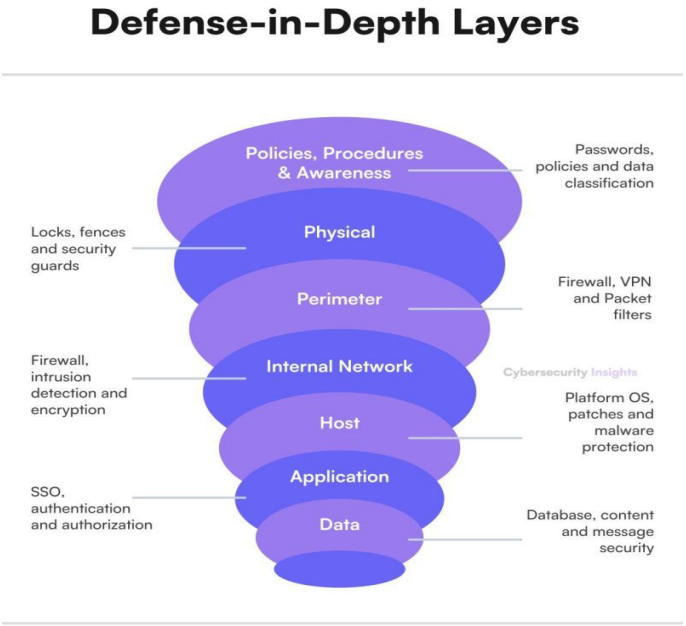
The design of a Defense in Depth strategy involves carefully considering various security controls and implementing them in a way that creates overlapping layers of protection. These layers can be physical, technical, or administrative.

Defense In Depth - Aim

- **Reduce vulnerability:** By implementing multiple layers of security, the overall vulnerability of a system is significantly reduced.
- **Contain breaches:** If a breach occurs, the layered approach can help to contain the damage by preventing the attacker from moving laterally within the system.
- **Improve resilience:** Defense in Depth makes a system more resilient to attacks, as it can recover more quickly from incidents.
- **Compliance:** Many regulatory frameworks require organizations to implement layered security controls to protect sensitive data.

AFRICAHACKON

Defense in Depth



Defense in Depth Security Control Types

"Defense in Depth" is a multi-layered security strategy integrating **administrative, technical, and physical controls** to ensure **if one fails, others protect.** By implementing multiple controls, organizations can protect against a variety of threats, from cyber-attacks to internal breaches, ensuring that critical systems and data remain secure.

Administrative Controls		Physical Controls		Technical Controls	
Admin controls manage user behavior and operations through policies, training, and audits.		Physical controls protect assets via locks, barriers, surveillance, and access management.		Technical controls safeguard IT via firewalls, encryption, antivirus, and access systems.	
Policies & Procedures Standards for organizational activities, including security guidelines.	**Personnel Security** Hiring and managing staff with security-focused processes.	**Environmental Controls** Systems to protect against fire, flood, and other hazards.	**Surveillance Systems & Security Guards** Cameras and monitoring for security and safety.	**Firewalls** Systems to block unauthorized network access.	**Intrusion Detection Systems** Monitoring networks for suspicious activities.
User Training & Awareness Educating staff on security best practices and potential threats.	**Audit and Monitoring** Regularly reviewing security practices for policy compliance.	**Secure Facility Access** Restricted access to buildings using keycards or biometrics.	**Physical Barriers** Fences, gates, and locks to prevent unauthorized entry.	**Encryption** Protecting data in transit and at rest.	**Antivirus Software & Patch Management** Protection against malware and viruses plus security updates.
Access Control Policies Defining roles for resource access based on organizational roles.	**Incident Response Plans** Handling security incidents from identification to recovery.	**Visitor Management** Processes to control and monitor visitor access.	**Secure Equipment Areas** Protected zones for sensitive or critical equipment.	**Data Backup** Regular backups of critical data for recovery purposes.	**Access Control Systems** Restricting user access to systems and data.

Defense in Depth - Components

1. **Physical security:** This layer involves protecting the physical infrastructure of the system, such as buildings, servers, and network devices. It includes measures like access controls, surveillance, and environmental monitoring.
2. **Network security:** This layer focuses on protecting the network infrastructure, including routers, switches, and firewalls. It involves techniques like network segmentation, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
3. **Application security:** This layer involves protecting applications and software from vulnerabilities. It includes measures like input validation, output encoding, and security code reviews.
4. **Data security:** This layer focuses on protecting sensitive data, including encryption, access controls, and data loss prevention (DLP).
5. **Identity and access management (IAM):** This layer involves managing user identities and access privileges. It includes authentication, authorization, and account management.
6. **User education and awareness:** This layer involves educating users about security best practices and raising awareness of potential threats.