FUNDAMENTAL OF CYBERSECURITY

Protecting Yourself in the Digital World

Cyber security is a crucial aspect of modern technology that involves protecting computer systems, networks, and data from digital attacks, unauthorised access, and damage.

- **Protection of Information:** Ensures that sensitive data remains confidential and is not accessed or disclosed to unauthorised parties.

- **Integrity of Systems:** Maintains the accuracy and reliability of data and systems, preventing unauthorised modifications.

- **Availability of Resources:** Guarantees that information and systems are accessible to authorised users as needed, preventing disruptions caused by cyber-attacks.

IMPORTANCE OF CYBERSECURITY

- **Preventing Data Breaches:** Protects personal and financial information from being stolen or compromised, which can lead to identity theft and financial loss.

- **Securing Business Operations:** Ensures that businesses can operate smoothly without interruptions caused by cyber attacks, which can lead to damage of a business' finances and reputation.

- **Protecting National Security:** Safeguards critical infrastructure and government data from cyber espionage and attacks that could undermine national security and public safety.

- **Enhancing Consumer Trust:** Builds trust among consumers and clients through a commitment to protecting their data and privacy.

KEY ELEMENTS OF CYBERSECURITY

- **Firewalls and Intrusion Detection/Prevention Systems:** Act as barriers to block unauthorised access and monitor for suspicious activities within networks.

- **Encryption:** Ensures that data transmitted over networks or stored on devices is unreadable to unauthorised users.

- **Access Controls:** Manages who can access information and systems, ensuring that only authorised individuals have the necessary permissions.

- **Regular Updates and Patching:** Keeps software and systems up to date to protect against known vulnerabilities and exploits.

- **Security Awareness Training:** Educates users on how to recognise and respond to potential security threats.

TYPES OF CYBER THREATS

Cyber threats come in a variety of forms, each presenting unique challenges to security. Understanding these threats helps in developing effective defence strategies.

MALWARE

Malicious software that is designed to disrupt, damage, or gain unauthorised access to systems.

SOCIAL ENGINEERING

Manipulative tactics used to trick individuals into divulging confidential information

RANSOMWARE

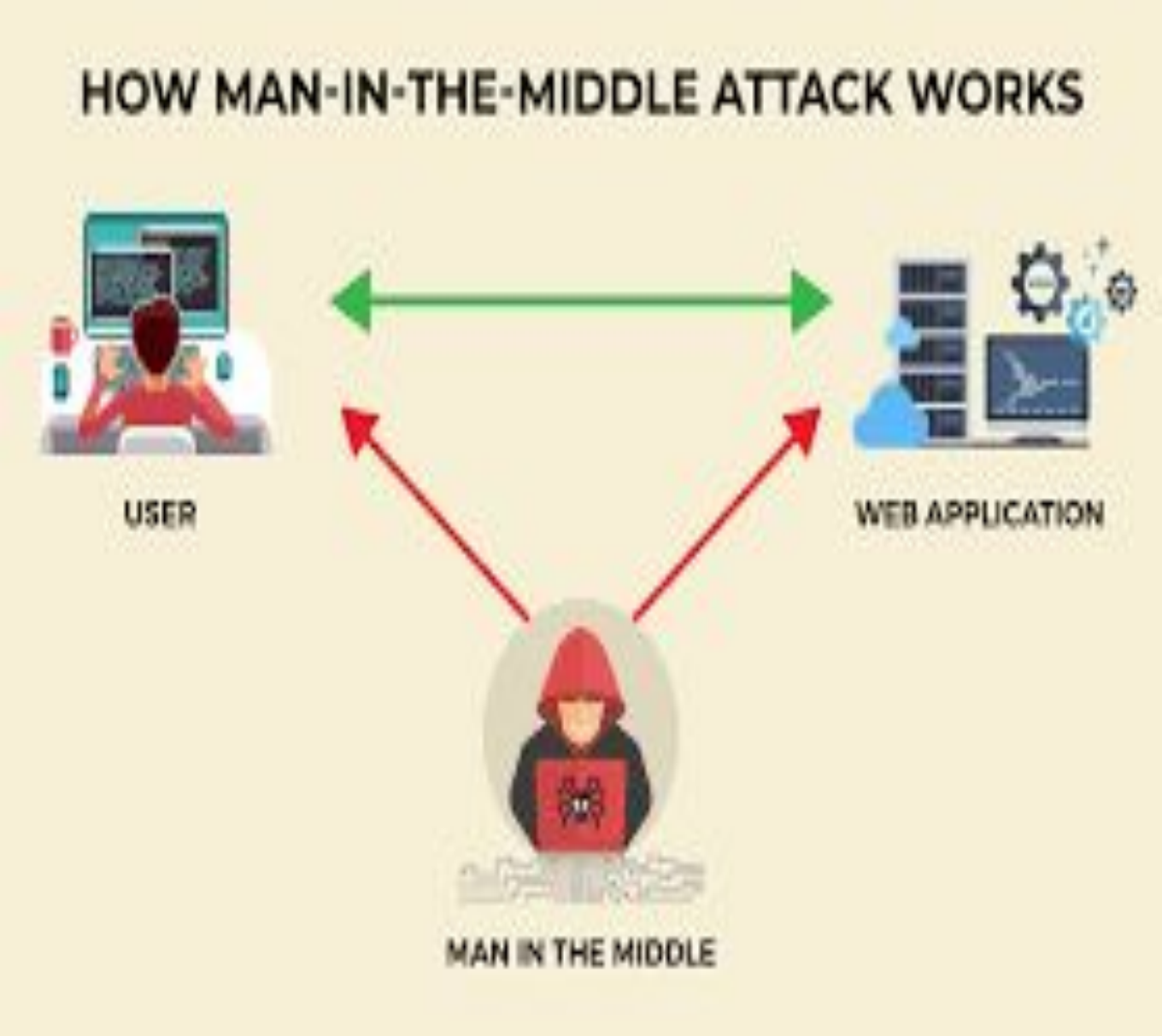
A type of malware that encrypts data and demands payment for the decryption key.

Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle attacks occur when an attacker intercepts and alters communication between two parties without their knowledge.

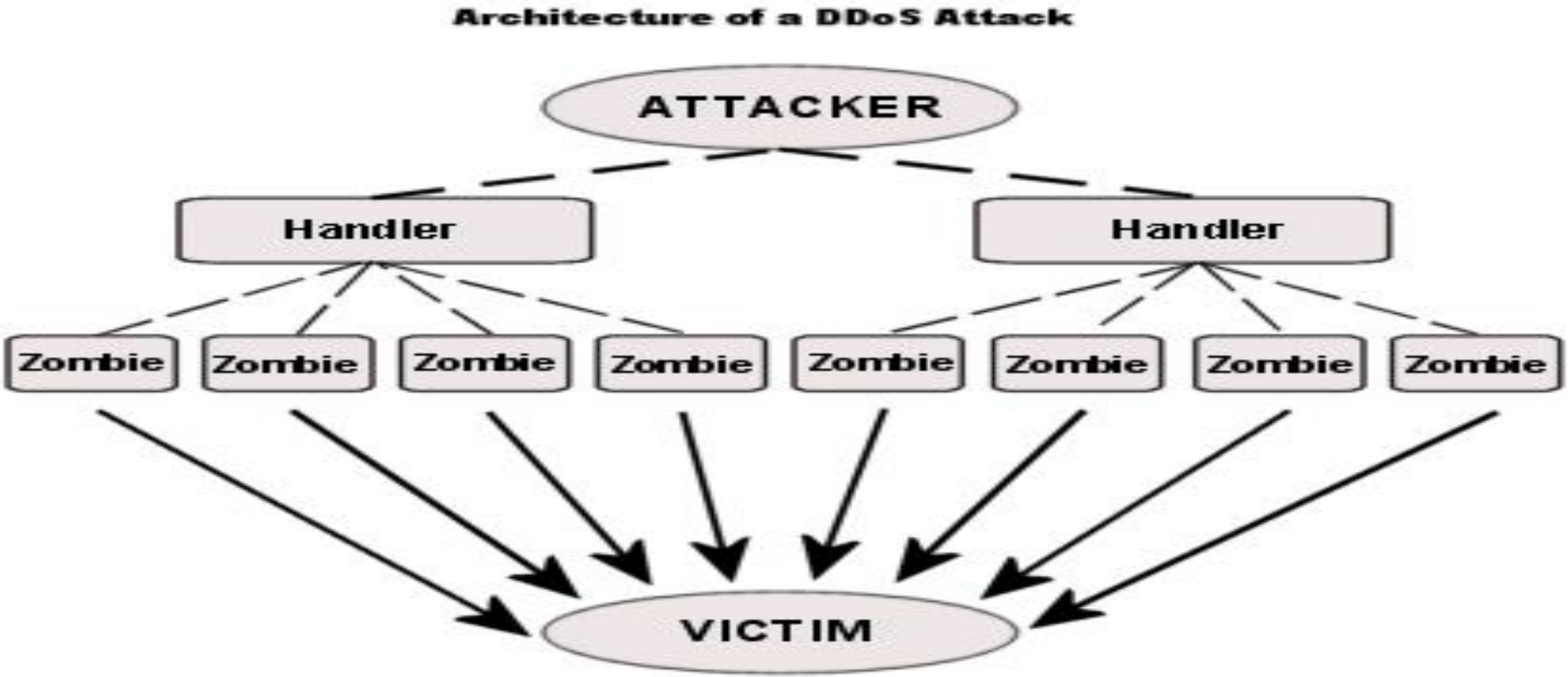
- **Eavesdropping:** The attacker intercepts private communications to steal sensitive information.

- **Session Hijacking:** The attacker takes control of a user's session, typically in a web application, to gain unauthorised access.



DDOS ATTACKS

Distributed Denial of Service (DDoS) attacks overload a system with traffic, rendering it unavailable to users.



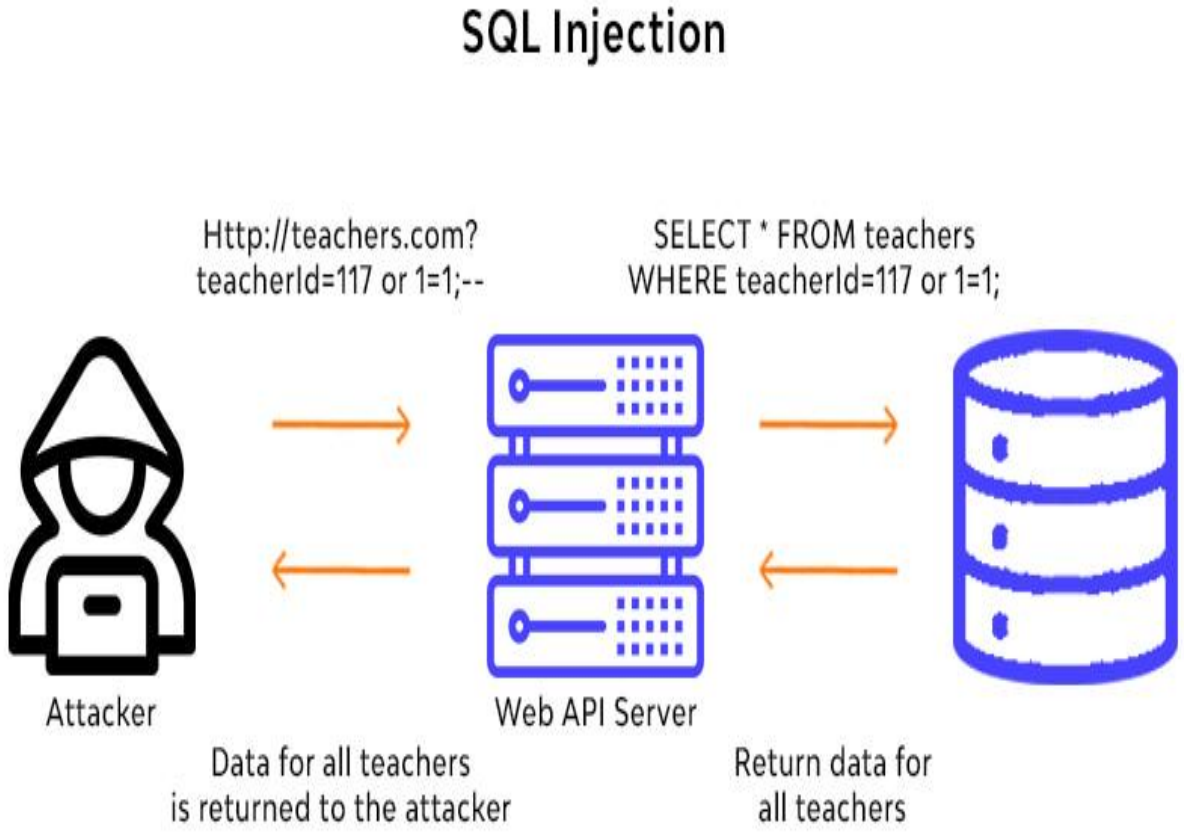
SQL INJECTION

SQL Injection involves inserting or "injecting" malicious SQL queries into a database input field, exploiting vulnerabilities in the software to execute arbitrary SQL commands

- **Error-based SQL Injection:** Exploits error messages returned by the database to gain information about the structure of the database.

- **Blind SQL Injection:** Exploits the database without any message from the server, making it harder to detect.

- **Union-based SQL Injection:** This technique leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result, allowing the attacker to retrieve data from other tables within the database.



PASSWORD ATTACKS

Password attacks aim to obtain an individual's password through various means.

Brute Force Attack: The attacker uses automated tools to guess passwords by trying every possible combination.

Dictionary Attack: The attacker uses a list of common passwords to attempt to gain access.

Credential Stuffing: The attacker uses stolen credentials from one site in an attempt to gain access to other sites.

Rainbow Table Attack: The attacker uses precomputed tables containing the hash values of common passwords. By comparing these hash values to the hashed password stored in the system, the attacker can quickly identify the original password.

ADVANCED PERSISTENT THREATS (APTS)

Advanced Persistent Threats involve prolonged and targeted cyber attacks during which an intruder gains access to a network and remains undetected for an extended period.

Surveillance and Data Exfiltration: The attacker monitors the network and gradually syphons off sensitive data.

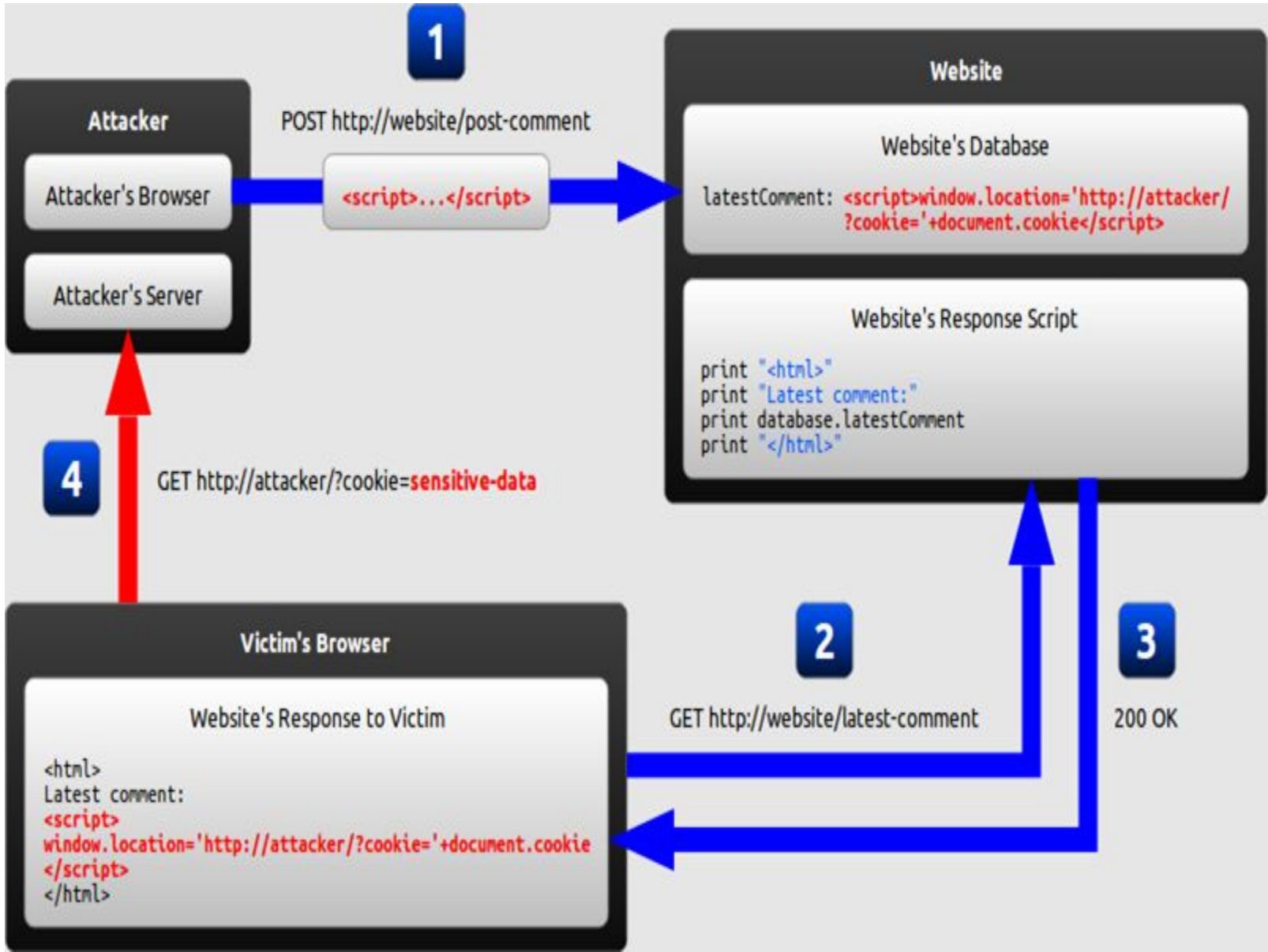
Command and Control (C2) Servers: The attacker establishes a backchannel to communicate with the compromised network.

CROSS-SITE SCRIPTING

Cross-Site Scripting is a type of injection attack where malicious scripts are inserted into normally harmless and trusted websites.

Stored XSS: The malicious script is permanently stored on the target server.

Reflected XSS: The malicious script is reflected off a web server, such as in a search result or error message.



INSIDER THREATS

Insider Threats involve malicious actions taken by individuals within an organisation who have authorised access to its systems and data.

Malicious Insiders: Employees or contractors who intentionally exploit their access for personal gain or to cause harm.

Unintentional Insiders: Employees who accidentally compromise security through

PHISHING

Phishing is a social engineering attack that aims to trick individuals into divulging sensitive information such as usernames, passwords, and credit card details.

- Email Phishing: Attackers send fraudulent emails that appear to come from a reputable source, prompting recipients to click on malicious links or download attachments.

- Spear Phishing: A more targeted form of phishing where attackers customise their messages to a specific individual or organisation, often using personal information to make the attack more convincing.

- Clone Phishing: Attackers create a nearly identical copy of a legitimate email previously sent by a trusted entity, replacing any links or attachments with malicious ones.

- Whaling: A type of phishing targeting high-profile individuals within an organisation, such as executives or senior management, often involving highly personalised messages.

ZERO-DAY EXPLOIT

Zero-Day Exploits take advantage of previously unknown vulnerabilities in software, which developers have had no opportunity to fix before they are discovered.

Zero-Day Attack: The attacker exploits the vulnerability before the software vendor releases a patch.

PRINCIPLES OF CYBERSECURITY

Fundamental to understanding cyber security are the concepts of confidentiality, integrity, and availability, often referred to as the CIA triad. These principles form the backbone of effective security measures.

CYBERSECURITY – INFOSEC CIA TRIAD

Safeguarding the accuracy and completeness of information and processing methods.

Includes the detection of alterations that occurred in storage, transit, process,...

Ensuring that information is accessible only to those authorized to have access.

Includes:

- Protection from unauthorized access and use;
- Protecting data on systems, in transit, in process,...

Ensuring that authorized users have access to information and associated assets when required.

Includes controls for:

Acceptable level of performance
Fault tolerance
Prevention of data loss and destruction
Reliable backups, redundancy,...

ACCESS CONTROL FUNDAMENTAL

Authentication, authorization, and accounting, often referred to as AAA, are fundamental concepts in cyber security for securing systems and managing access control.

Authentication

Authentication is the process of verifying the identity of a user, device, or system before granting access. It ensures that the entity requesting access is who it claims to be.

- **Password-Based Authentication:** Users provide a secret password that matches the one stored in the system. Strong, unique passwords enhance security.

- **Multi-Factor Authentication (MFA):** Requires two or more verification methods, typically something the user knows (password), something the user has (security token), or something the user has (biometric verification).

- **Biometric Authentication:** Uses unique biological characteristics, such as fingerprints or facial recognition, to verify identity.

- **Token-Based Authentication:** Involves the use of tokens, which can be physical (e.g., smart cards) or digital (e.g., software tokens), to authenticate users.

Authorisation

Authorization is the process of determining whether an authenticated user has permission to access a resource or perform an action. It ensures that all users have appropriate access levels.

- **Role-Based Access Control (RBAC):** Assigns access rights based on user roles within an organisation, limiting access to only those resources necessary for their role.

- **Access Control Lists (ACLs):** Define which users or system processes have access to specific resources and what operations they can perform.

- **Attribute-Based Access Control (ABAC):** Uses attributes (e.g., user attributes, resource attributes, environmental conditions) to grant access dynamically based on policies.

- **Policy-Based Access Control:** Establishes policies that specify conditions under which access is granted, often used in conjunction with ABAC and RBAC.

Accounting

Accounting, also known as auditing, involves tracking and recording user activities on a system. This helps monitor usage, detect anomalies, and ensure compliance with security policies.

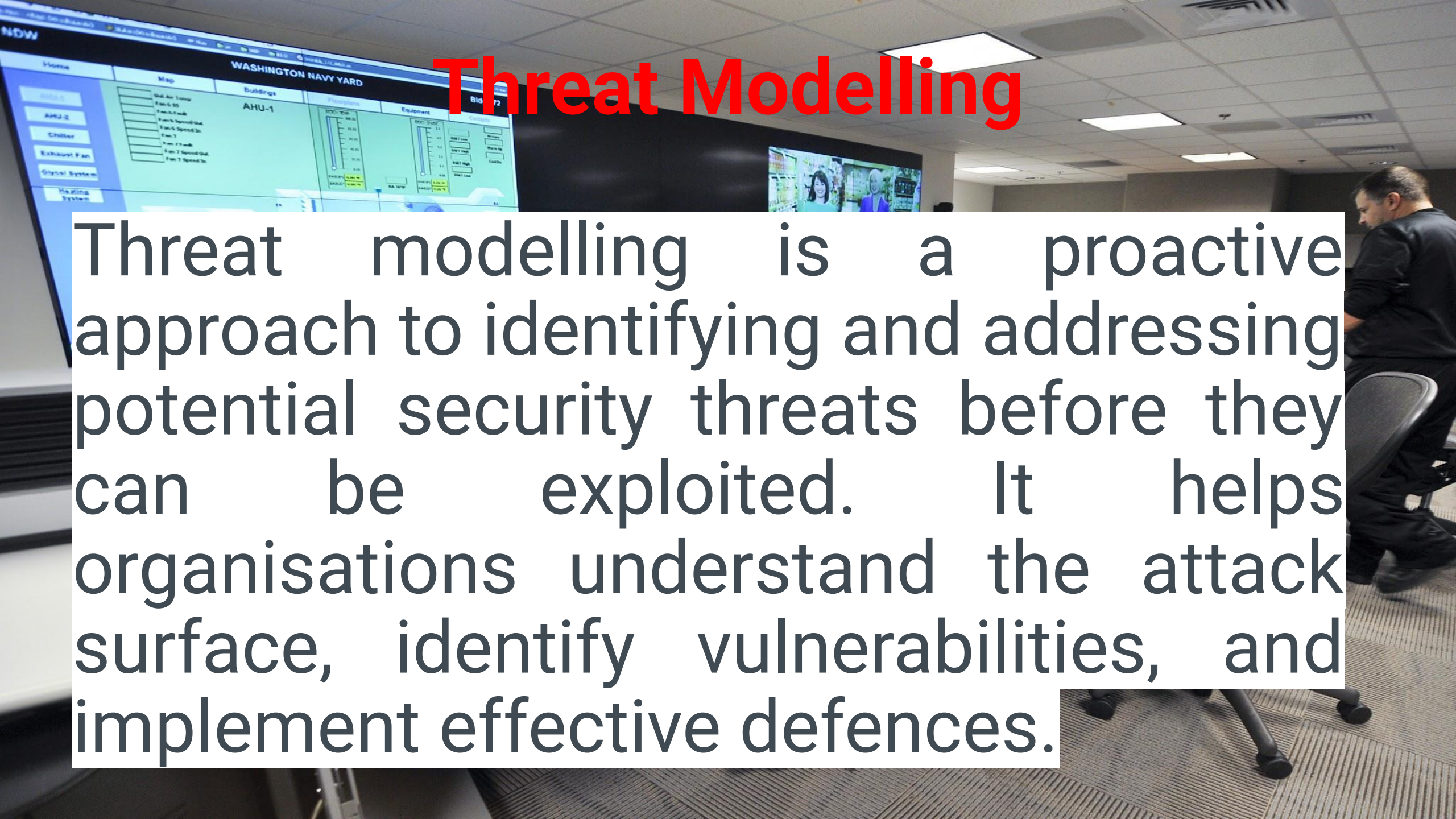
- **Log Management:** Collecting and managing logs that record user activities, system events, and access attempts. Logs are essential for auditing and forensic analysis.

- **Audit Trails:** Maintaining detailed records of system activities, which can be reviewed to ensure compliance with security policies and investigate incidents.

- **Usage Monitoring:** Continuously monitor system usage to detect unusual patterns or unauthorised activities that may indicate a security breach.

- **Reporting:** Generating reports from logs and audit trails to provide insights into user activities, access patterns, and potential security issues.

Threat Modelling



Threat modelling is a proactive approach to identifying and addressing potential security threats before they can be exploited. It helps organisations understand the attack surface, identify vulnerabilities, and implement effective defences.

The importance of threat modelling can be highlighted through the following points.

Systematic Identification of Threats: Provides a structured method to identify potential threats to an organisation's assets, considering various attack vectors and methods.

Understanding Attack Surface: Helps in understanding the different points at which an attacker could potentially exploit the system, allowing for a comprehensive security strategy.

Prioritising Security Efforts: Enables organisations to prioritise their security efforts by focusing on the most critical threats and vulnerabilities, ensuring resources are used efficiently.

Enhancing Security Design: Integrates security considerations into the design and development process of systems and applications, reducing the likelihood of vulnerabilities being introduced.

Facilitating Communication: Improves communication between different stakeholders, including security teams, developers, and management, ensuring a unified approach to addressing threats.

Continuous Improvement: Encourages ongoing evaluation and improvement of security measures as new threats emerge and systems evolve.

COMMON CYBERSECURITY STANDARDS

Cyber security standards provide structured guidelines and best practices to help organisations manage and reduce their cyber security risks. These standards are essential for establishing robust security policies, ensuring compliance with regulations, and protecting sensitive information. Below are some of the most common cyber security standards used today.

NIST cyber security Framework (CSF)

The National Institute of Standards and Technology (NIST) cyber security Framework is a comprehensive guide designed to help organisations manage and reduce their cyber security risk.

- **Identify:** Develop an understanding of how to manage cyber security risks to systems, assets, data, and capabilities.
- **Protect:** Implement appropriate safeguards to ensure the delivery of critical infrastructure services.
- **Detect:** Develop and implement activities to identify the occurrence of a cyber security event.
- **Respond:** Take action regarding a detected cyber security incident to contain its impact.
- **Recover:** Maintain plans for resilience and restore any capabilities or services that were impaired due to a cyber security incident.

ISO/IEC 27001

ISO/IEC 27001 is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

- **Context of the Organisation:** Understand the organisation's context and interested parties to ensure that the ISMS meets their needs.
- **Leadership:** Ensure top management commitment and define roles and responsibilities.
- **Planning:** Identify and assess information security risks and plan appropriate measures to address them.
- **Support:** Allocate resources, enhance competence, and ensure effective communication.
- **Operation:** Implement the necessary processes to meet the information security objectives.
- **Performance Evaluation:** Monitor, measure, analyse, and evaluate the performance of the ISMS.
- **Improvement:** Take corrective actions to improve the ISMS continually.

CIS Controls

The Centre for Internet Security (CIS) Controls are a set of best practices for securing IT systems and data against the most pervasive attacks.

- **Basic Controls**: Include essential practices like inventory and control of hardware and software assets, continuous vulnerability management, and controlled use of administrative privileges.
- **Foundational Controls:** Involve more advanced practices such as email and web browser protections, malware defences, and data recovery capabilities.
- **Organisational Controls:** Focus on broader organisational processes, including security awareness and skills training, application software security, and incident response management.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

- **Build and Maintain a Secure Network**: Implement strong access control measures and maintain a secure network architecture.
- **Protect Cardholder Data:** Ensure that cardholder data is protected and encrypted during storage and transmission.
- **Maintain a Vulnerability Management Program:** Regularly update and patch systems, and implement robust anti-virus measures.
- **Implement Strong Access Control Measures:** Restrict access to cardholder data to a need-to-know basis only.
- **Regularly Monitor and Test Networks:** Perform regular security testing and monitoring to identify and address vulnerabilities.
- **Maintain an Information Security Policy:** Develop and maintain a comprehensive information security policy.

FUNDAMENTAL OF NETWORKING

Networking is the backbone of modern communication, enabling devices to connect and share information efficiently. Understanding the fundamentals of networking is crucial for grasping the principles of network security. This overview provides a foundation for comprehending how networks function and their essential components

COMPONENTS OF NETWORK

Networks are composed of various elements that work together to facilitate communication and data transfer.

Devices: These include computers, smartphones, servers, and networking hardware such as routers, switches, and hubs.

Media: The physical pathways through which data travels. This can be wired (Ethernet cables, fibre optics) or wireless (Wi-Fi, Bluetooth).

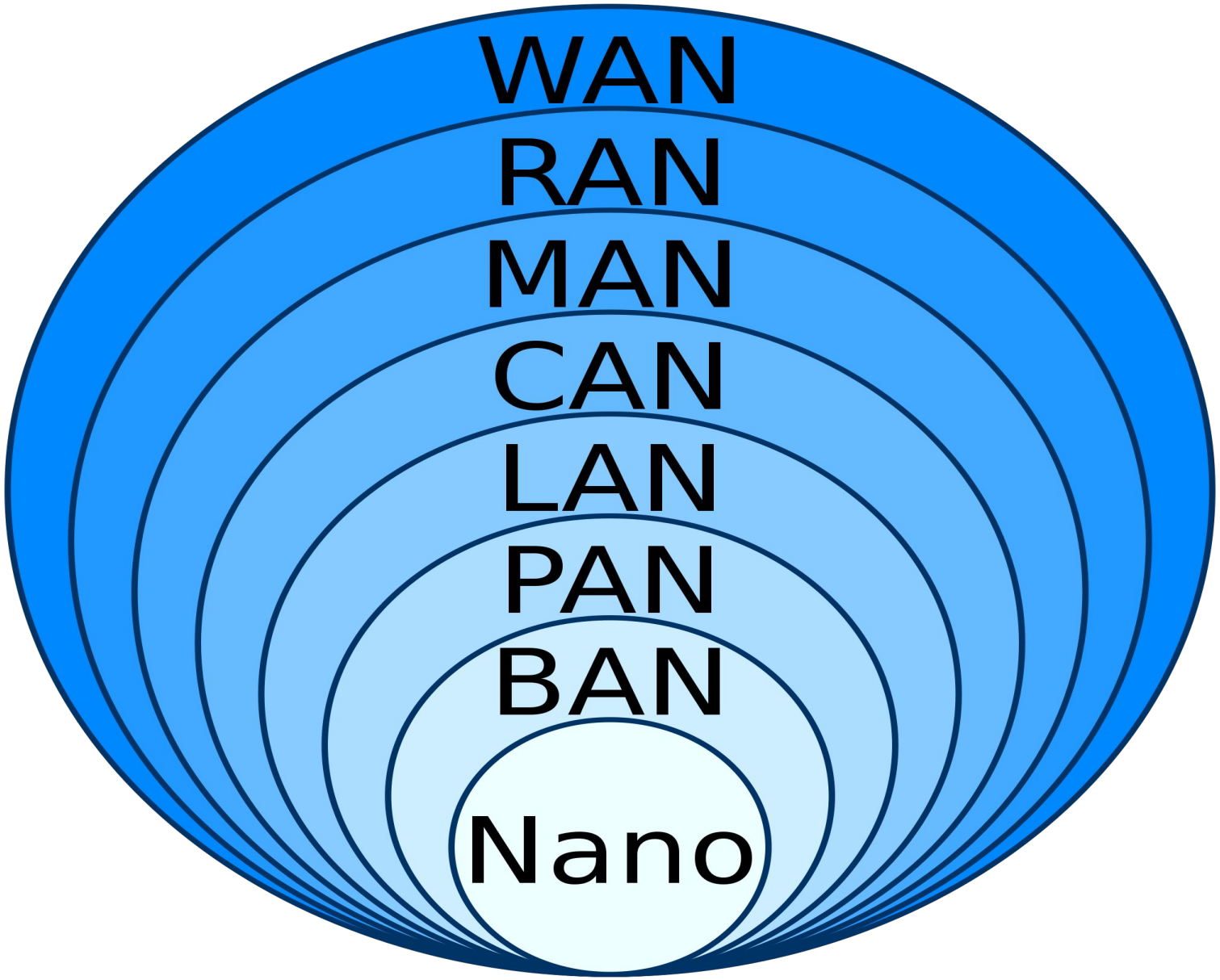
Protocols: Sets of rules that dictate how data is transmitted and received. Common protocols include TCP/IP, HTTP, FTP and SSH.

Network Interface Cards (NICs): Hardware components that connect devices to the network.

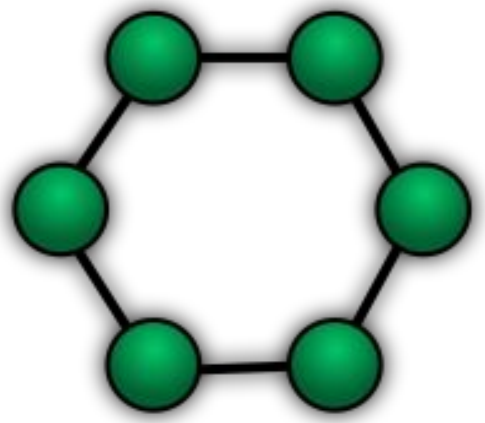
Software: Network operating systems and management software that control network functions and security.

TYPES OF NETWORK

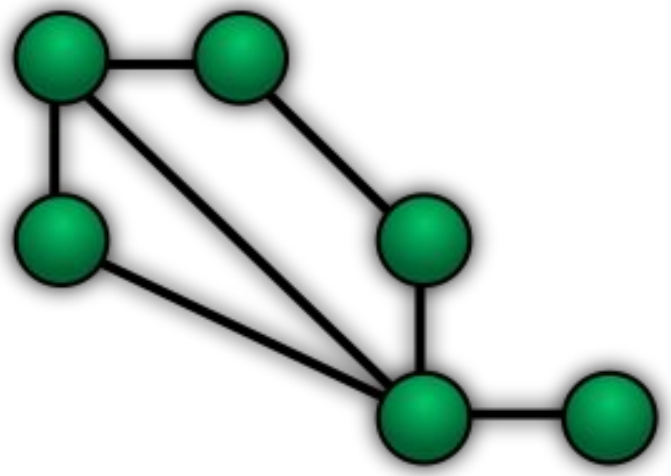
- Nano Network
- Body Area Network
- Personal Area Network
- Local Area Network
- Campus Area Network
- Metropolitan Area Network
- Radio Access Network
- Wide Area Network



NETWORK TOPOLOGY

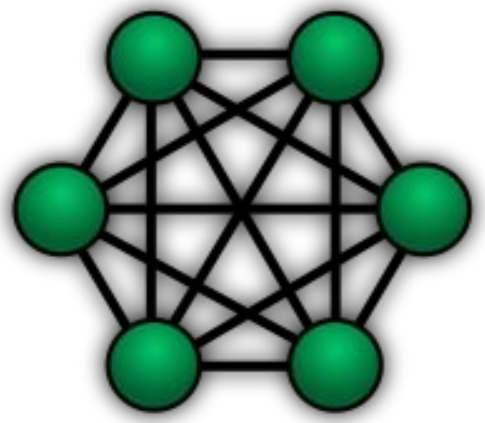


Ring

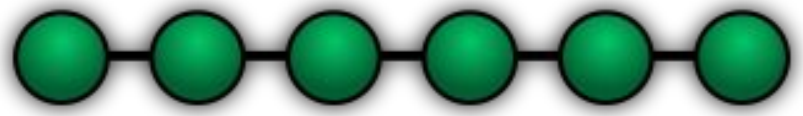


Mesh

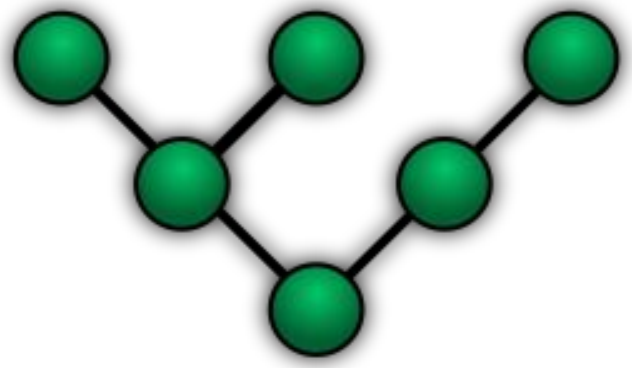
Star



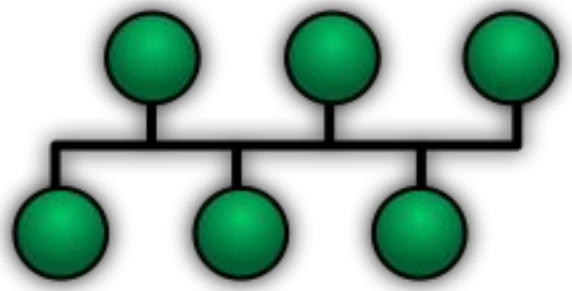
Fully Connected



Line



Tree



Bus

Network Addressing

Network addressing is crucial for identifying devices and ensuring accurate data delivery.

IP Addresses: Unique numerical labels assigned to each device on a network. IPv4 (e.g., 192.168.1.1) and IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334) are the two versions in use.

MAC Addresses: Hardware addresses unique to each NIC, used within LANs for addressing devices. A MAC address is a 48-bit identifier typically represented as six groups of two hexadecimal digits, separated by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E).

IP Addressing and Subnets

IP addressing and subnets are essential for efficient network management and data routing.

IPv4 Addressing: Consists of 32 bits divided into four octets.* It includes a network portion and a host portion, separated by a subnet mask (e.g., 255.255.255.0).

IPv6 Addressing: Utilises 128 bits, providing a significantly larger address space. It is represented in hexadecimal and separated by colons.

Subnets: Subdividing a network into smaller, manageable sections. This improves performance and security. Subnetting involves dividing an IP address into a network and host portion using a subnet mask.

Subnet Mask: Defines the network and host portions of an IP address. For example, a subnet mask of 255.255.255.0 indicates that the first three octets represent the network, and the last octet represents the host.

CIDR Notation: A shorthand for subnet masks, written as an IP address followed by a slash and the number of bits in the network portion (e.g., 192.168.1.0/24).
*An octet is an 8-bit section of an IPv4 address, allowing for values between 0 and 255.

Data Transmission

The process of moving data across a network involves several key concepts and techniques.

Packets: Data is broken into smaller units called packets for transmission. Each packet contains a portion of the data and control information.

Switching: Methods for directing packets to their destination. Includes circuit switching, packet switching, and message switching.

Routing: The process of selecting paths in a network along which to send data packets. Routers use algorithms and protocols (e.g., OSPF, BGP) to determine the best path.

Common Data Devices

Understanding the roles and functions of common network devices is essential for managing and securing a network effectively.

Key devices such as routers, switches, and firewalls play critical roles in ensuring data is transmitted efficiently and securely across the network.

Routers

Routers are pivotal in connecting multiple networks and directing data traffic between them.

Data Routing: Routers determine the best path for data to travel from one network to another using routing tables and protocols like OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).

Network Segmentation: They help segment networks into smaller, manageable sections, enhancing performance and security.

IP Address Management: Routers assign IP addresses to devices within a network using DHCP (Dynamic Host Configuration Protocol) and can also implement NAT (Network Address Translation) to allow multiple devices to share a single public IP address.

Connectivity: They enable different network types, such as LANs and WANs, to communicate with each other and support VPN (Virtual Private Network) connections for secure remote access.

Quality of Service (QoS): Routers can prioritise different types of traffic to ensure reliable performance for key applications.

Switches

Switches operate within a network to connect devices, ensuring efficient communication and data transfer.

Data Forwarding: Switches receive data packets and forward them to the appropriate device within the same network, using MAC addresses to identify devices.

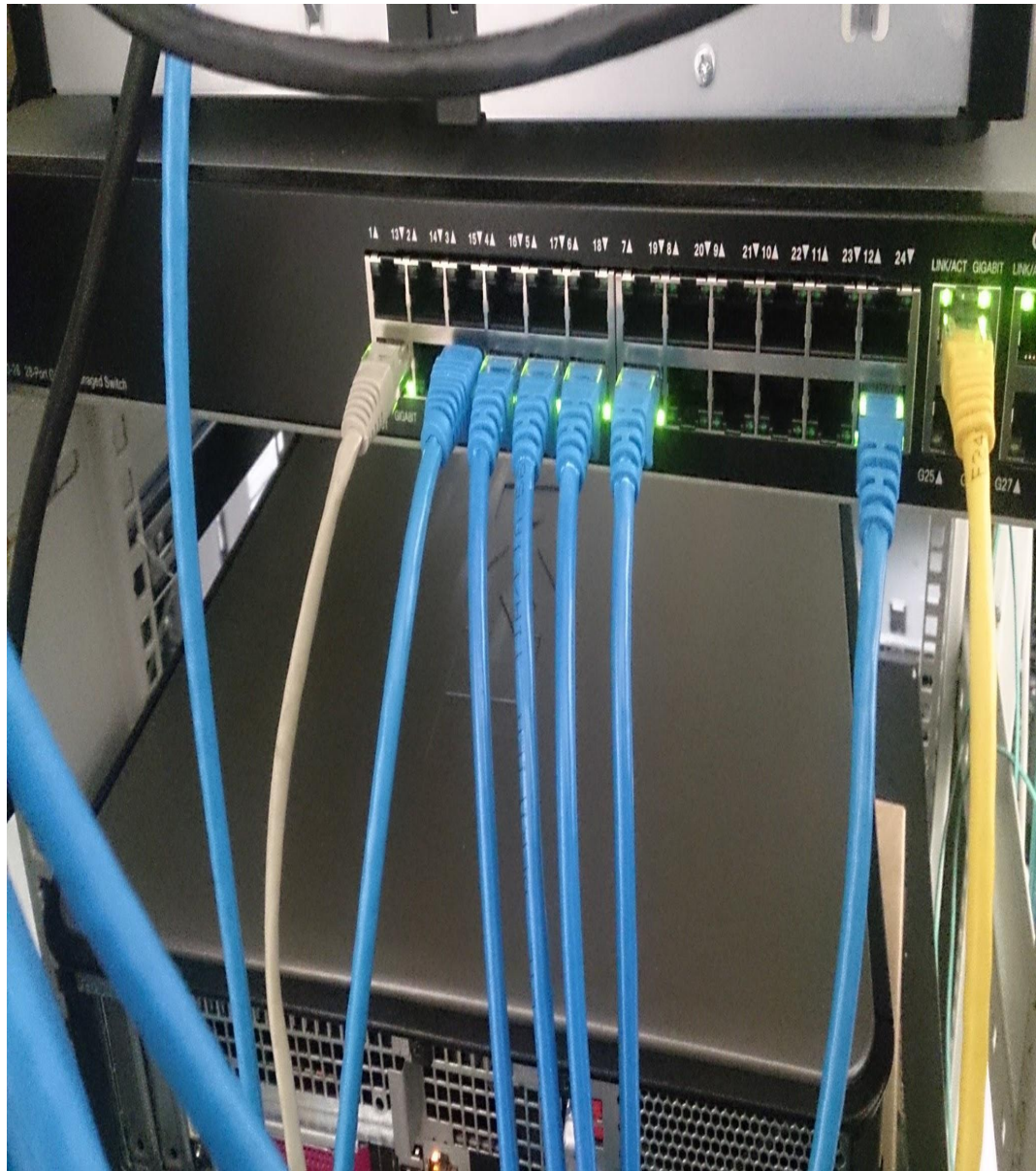
MAC Address Management: They use MAC addresses to identify devices and manage traffic efficiently, building a MAC address table to keep track of devices.

Network Segmentation: Switches can segment a network into VLANs (Virtual Local Area Networks), enhancing security and performance by isolating network traffic.

Bandwidth Management: They help manage and optimise network bandwidth by reducing collisions and controlling data flow, using features like link aggregation for increased bandwidth.

Layer 3 Switching: Some advanced switches can perform routing functions, making them capable of inter-VLAN routing and improving network efficiency.

CAM Tables: Content Addressable Memory (CAM) tables are used by switches to store and quickly reference MAC addresses. When a switch receives a data packet, it checks the CAM table to determine the correct port to forward the packet to, ensuring efficient data delivery.



HUBS

Hubs are basic networking devices that connect multiple Ethernet devices, making them act as a single network segment.

- **Data Broadcasting:** Hubs broadcast data packets to all devices on a network segment, regardless of the destination, which can lead to increased network traffic and collisions.

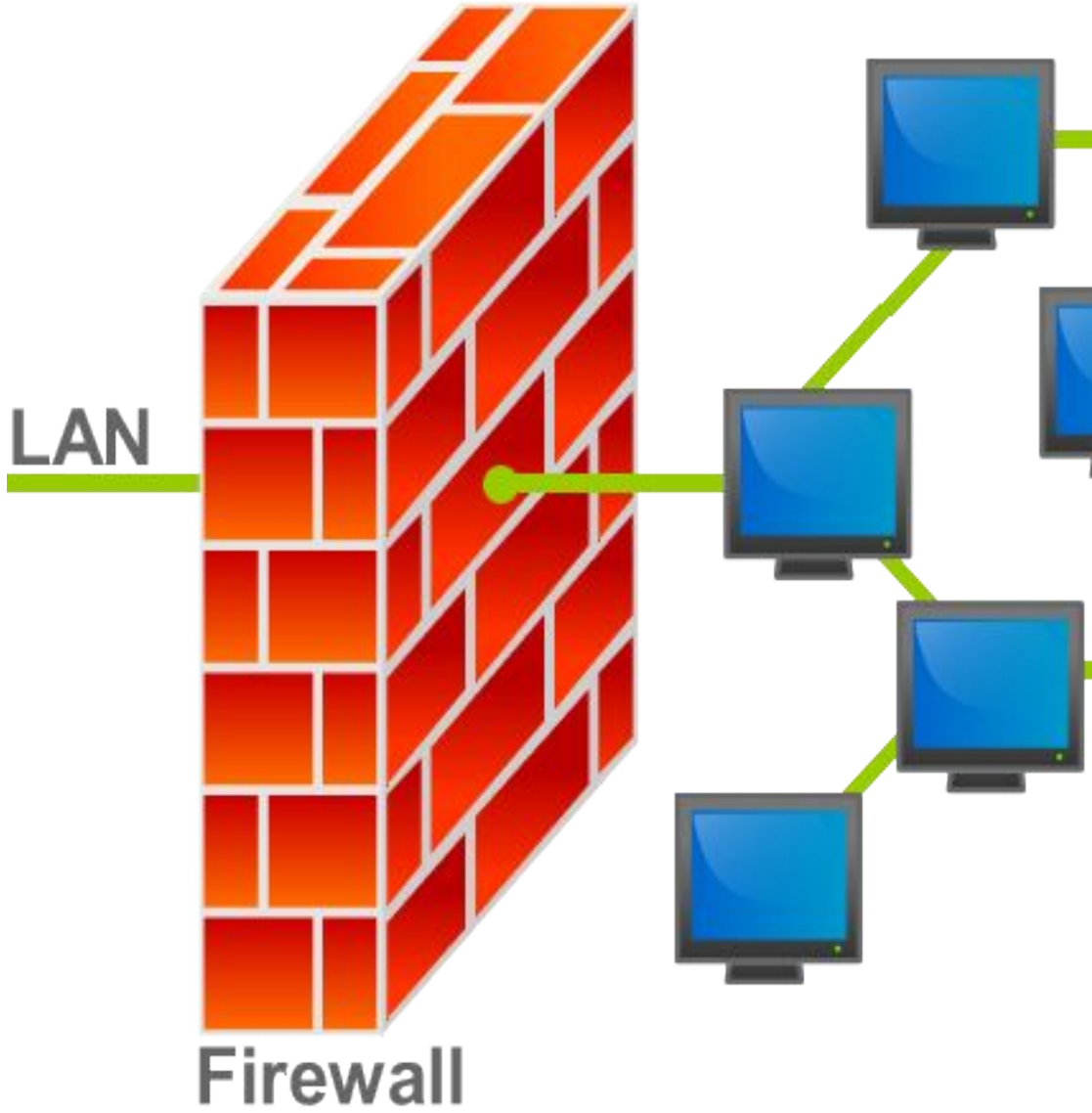
- **Simple Connectivity:** They provide a straightforward method to connect multiple devices in a network, but lack the intelligence to manage data traffic efficiently.

- **Limited Security:** Hubs do not differentiate between devices, leading to potential security vulnerabilities as data packets are accessible to all connected devices. Iit is preferable to use switches, which offer better security, efficiency, and network management capabilities.

Firewalls

Firewalls are critical for protecting a network by controlling incoming and outgoing traffic based on predetermined security rules.

- **Traffic Filtering:** Firewalls monitor and filter network traffic, allowing or blocking data packets based on security policies.
- **Access Control:** They enforce access control policies, ensuring only authorised users and devices can access the network, often integrating with authentication systems like RADIUS or LDAP.
- **Threat Prevention:** Firewalls protect against various cyber threats, including malware, viruses, and unauthorised access attempts, with advanced firewalls offering Intrusion Prevention Systems (IPS) for real-time threat detection.
- **Network Monitoring:** They provide logging and monitoring capabilities, helping identify and respond to suspicious activities, and can generate reports for security audits.
- **Types of Firewalls:** There are different types of firewalls, including hardware firewalls for enterprise networks, software firewalls for individual devices, and cloud-based firewalls for protecting cloud resources.



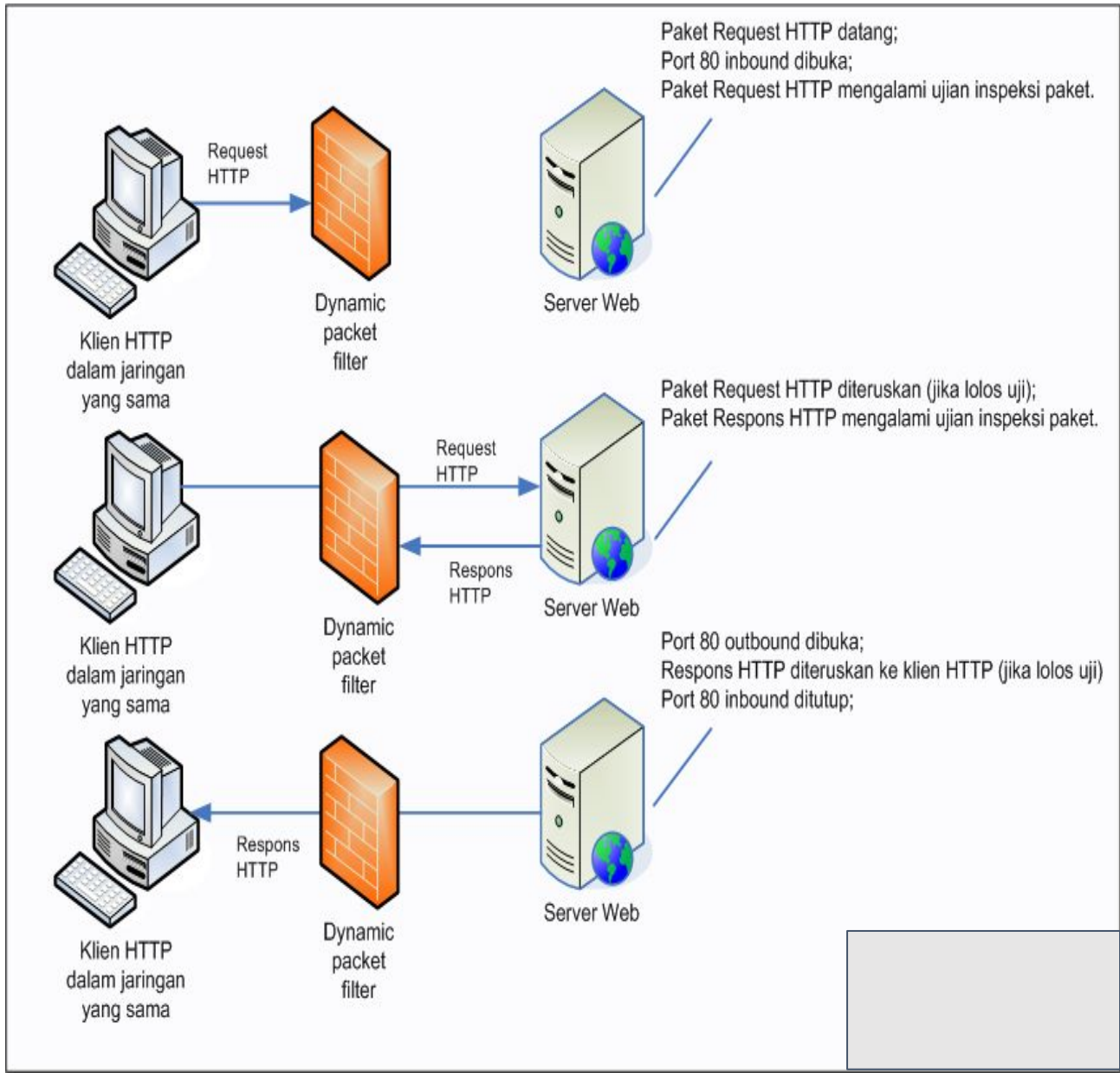
Packet-Filtering Firewalls

Type of Firewalls

Packet-filtering firewalls operate by inspecting packets in isolation. They apply a set of rules to each packet and decide to allow or block it based on the source and destination IP addresses, port numbers, and protocols.

Static Packet-Filtering: Uses fixed rules that do not change unless manually updated.

Dynamic Packet-Filtering: Adjusts rules based on ongoing communication, allowing more flexibility.

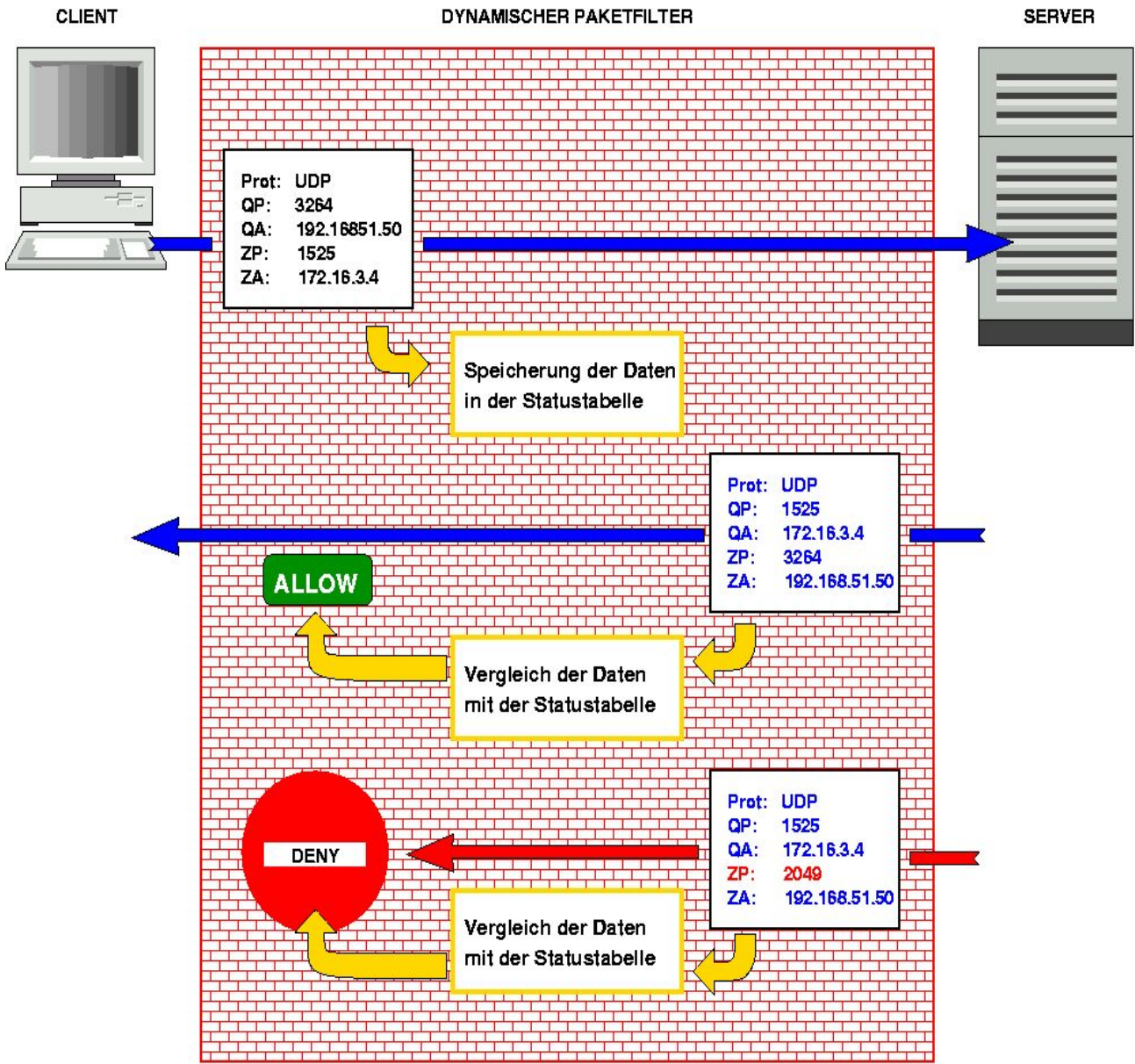


Stateful Inspection Firewalls

Stateful inspection firewalls, also known as dynamic packet-filtering firewalls, track the state of active connections and make decisions based on the traffic context.

Maintains State Information: Keeps track of the state of connections, allowing only packets that match an established connection.

Enhanced Security: Offers more robust protection compared to simple packet-filtering by considering the state and context of the traffic.



Network Security Principles

Network security is the practice of protecting a computer network from intruders, whether targeted attackers or opportunistic malware. Ensuring network security involves understanding the principles and implementing best practices to safeguard network integrity and confidentiality while maintaining availability.

Principles of Network Security

The core concepts of confidentiality, integrity, availability, authentication, and authorization play a crucial role in network security. Beyond these, several additional principles can be utilised to ensure robust network security.

Non-repudiation: Ensuring that a communication participant cannot deny the authenticity of their signature on a document or a sent message. Digital signatures and logging mechanisms help achieve non-repudiation.

Least Privilege: Granting users and systems the minimum level of necessary access to perform their functions, reducing the potential damage from compromised accounts.

Defence in Depth: Implementing multiple layers of security controls and defences throughout the network to protect against threats, ensuring that if one layer fails, others are still in place to maintain security.

Security by Design: Integrating security practices into the design and development of network systems and applications from the outset, rather than as an afterthought.

Best practices for Network Security

Implementing best practices is essential for creating a secure network environment.

Regular Updates and Patch Management: Keeping software and hardware up to date with patches protects against known vulnerabilities. This reduces the attack surface by eliminating exploitable weaknesses.

Network Segmentation: Dividing the network into segments to limit the spread of malware and restrict access to sensitive data. This can be achieved through VLANs, subnets, and firewalls.

Strong Password Policies: Enforcing the use of complex passwords and requiring regular changes to prevent unauthorised access. This includes using password managers and avoiding common or easily guessable passwords.

Multi-Factor Authentication (MFA): Adding an additional layer of security by requiring multiple types of verification before granting access. This mitigates the risk of compromised credentials.

Encryption: Encrypting data in transit and at rest to protect sensitive information from being intercepted or accessed by unauthorised parties. This includes using protocols like SSL/TLS for secure communication.

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): Using firewalls to block unauthorised access and IDS/IPS to monitor and respond to suspicious activities. These tools help detect and prevent potential breaches.

Regular Security Audits and Assessments: Conducting periodic reviews of network security measures to identify and address vulnerabilities. This involves penetration testing and vulnerability scanning.

User Training and Awareness: Educating employees about security policies, phishing attacks, and safe online practices to reduce human error. Regular training ensures that users are aware of current threats and best practices.

Incident Response Planning: Developing and maintaining an incident response plan to quickly address and mitigate the impact of security breaches. This includes defining roles, responsibilities, and procedures for handling incidents.

Access Control Lists (ACLs): Implementing ACLs to control which users and devices can access certain network resources, based on predefined policies. This helps enforce the principle of least privilege.

Backup and Recovery Procedures: Regularly backing up critical data and ensuring that recovery procedures are in place to restore information in case of data loss or corruption. This includes testing backups to ensure they can be restored effectively.

Zero Trust Architecture: Adopting a zero-trust approach where no user or device is trusted by default, even if they are within the network perimeter. Continuous verification and monitoring are essential components of this model.

Segregation of Duties: Ensuring that critical tasks and responsibilities are divided among different individuals or systems to reduce the risk of fraud or error.

User Training and Awareness: Educating employees about security policies, phishing attacks, and safe online practices to reduce human error. Regular training ensures that users are aware of current threats and best practices.

Incident Response Planning: Developing and maintaining an incident response plan to quickly address and mitigate the impact of security breaches. This includes defining roles, responsibilities, and procedures for handling incidents.

Access Control Lists (ACLs): Implementing ACLs to control which users and devices can access certain network resources, based on predefined policies. This helps enforce the principle of least privilege.

Backup and Recovery Procedures: Regularly backing up critical data and ensuring that recovery procedures are in place to restore information in case of data loss or corruption. This includes testing backups to ensure they can be restored effectively.

Zero Trust Architecture: Adopting a zero-trust approach where no user or device is trusted by default, even if they are within the network perimeter. Continuous verification and monitoring are essential components of this model.

Segregation of Duties: Ensuring that critical tasks and responsibilities are divided among different individuals or systems to reduce the risk of fraud or error.