Final Project

by:
Ahmed Said Zaghloul
Khairy ahmed mahmoud
Ali Khaled Shalby

Network Protocols and Port Numbers:

- FTP (File Transfer Protocol): Transfers files between systems. Port 21.
- SSH (Secure Shell): Secure remote login. Port 22.
- SMTP (Simple Mail Transfer Protocol): Sends emails. Port 25.
- DNS (Domain Name System): Translates domain names to IP addresses. Port 53.
- DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses automatically. Port 67/68.
- HTTP (Hypertext Transfer Protocol): Web traffic. Port 80.
- HTTPS (HTTP Secure): Secure web traffic. Port 443.
- SNMP (Simple Network Management Protocol): Manages network devices. Port 161.
- RDP (Remote Desktop Protocol): Remote desktop access. Port 3389.

Difference between HTTP and HTTPS

- HTTP (Hypertext Transfer Protocol):
  - Data transmitted in plaintext Vulnerable to interception , uses port 80.
  - No guarantee of data integrity,No identity verification .
- HTTPS (Hypertext Transfer Protocol Secure):
  - Uses SSL/TLS encryption , Secure data transmission , Uses port 443 .
  - Requires SSL/TLS certificate from a Certificate Authority (CA).
  - Ensures data has not been altered during transfer
  - Essential for secure online transactions, protecting sensitive data from interception and tampering.

DNS: When It Uses TCP vs. UDP

- The Domain Name System translates domain names into IP addres.
- Uses UDP :
  - Standard Queries: Quick requests like looking up an IP address.
  - Response Size:Typical responses are 512 bytes or less.
  - Faster response times,Lower overhead, making it efficient for small queries.
- Uses TCP :
  - TCP is used for larger responses or specific operations.Ensures all data packets are received in order and without loss.
  - Large Responses:Responses exceeding 512 bytes.
  - Zone Transfers: AXFR (full zone transfer) between DNS servers.

dns mechansim (process)

1. Query Initiation : A user types a domain name into a browser.
2. DNS Resolver:The local DNS resolver checks its cache for the IP address.
3. Root Server Query:If not cached, the resolver queries a root server.
4. TLD Server Query:The root server directs the resolver to the appropriate TLD server.
5. Authoritative Server Query:The TLD server directs the resolver to the authoritative name server.
6. Final Resolution:The authoritative server returns the IP address to the resolver, which caches it for future use.

DNS Records:

1. A: RecordMaps a domain to an IPv4 address (e.g., example.com → 192.0.2.1).
2. AAAA Record: Maps a domain to an IPv6 address (e.g., example.com → 2001:db8::1).
3. CNAME Record: Alias for another domain name (e.g., www.example.com → example.com).
4. MX Record: Specifies mail exchange servers for email delivery (e.g., example.com → mail.example.com with priority).
5. TXT Record: Holds text information for various purposes (e.g., SPF records for email verification).
6. NS Record Indicates the name servers for a domain (e.g., example.com → ns1.example.com).
7. SRV Record Specifies services available at specific ports (e.g., for VoIP or instant messaging).

DHCP Mechanism:

- DHCP (Dynamic Host Configuration Protocol) automates the assignment of IP addresses and other network configuration parameters to devices on a network.
- DHCP Process:
  1. DHCP Discover: Client broadcasts a request to find available DHCP servers.
  2. DHCP Offer: DHCP server responds with an available IP address and configuration details.
  3. DHCP Request: Client requests the offered IP address.
  4. DHCP Acknowledgment: Server confirms the assignment, and the client configures its network settings.

Proxy: Function and Types

- A proxy is a server that acts as an intermediary between the user and the internet, handling requests and responses.
- Types of Proxy:
  1. Forward Proxy: Acts as an intermediary between the client (user) and the internet.Used for filtering requests and content.
  2. Reverse Proxy: Sits in front of a server and receives requests from the internet.Used for load balancing, performance enhancement, and security.
  3. Transparent Proxy: Requires no configuration from the user. Commonly used in organizations for monitoring activity.
  4. Non-Transparent Proxy: Requires user configuration. Offers additional features like data encryption.
  5. SOCKS Proxy:Operates at a low level and handles multiple protocol types. Often used to bypass geographical restrictions.
  6. Web Proxy: Used for web browsing through a web interface.Provides ease of use for bypassing restrictions.

Firewall Types Overview

1. Packet-Filtering Firewall Inspects packets at the network layer. Allows or blocks traffic based on predefined rules (IP address, port, protocol).
2. Stateful Inspection Firewall Monitors the state of active connections. Makes decisions based on the context of traffic and connection states.
3. Proxy Firewall Acts as an intermediary between users and the internet. Inspects and filters traffic at the application layer, providing anonymity and additional security.
4. Next-Generation Firewall (NGFW) Combines traditional firewall features with advanced capabilities (e.g., intrusion prevention, application awareness). Provides deep packet inspection and threat intelligence.
5. Web Application Firewall (WAF) Protects web applications by filtering and monitoring HTTP traffic.Guards against attacks like SQL injection and cross-site scripting (XSS).
6. Cloud Firewall Offered as a service in cloud environments.Provides scalable protection for cloud-based applications and infrastructure.

IPS and IDS:

- IDS: Monitors network traffic for suspicious activity and alerts administrators.
  - Types:
    - Network-based IDS (NIDS): Analyzes traffic on the network.
    - Host-based IDS (HIDS): Monitors individual devices for anomalies.
  - Action: Alerts only; does not take action to block threats.
- IPS :Monitors network traffic and actively blocks or prevents identified threats.
  - Types:
    - Network-based IPS (NIPS): Protects network traffic in real-time.
    - Host-based IPS (HIPS): Protects individual devices by bloc

Firewall, IDS, and IPS in Network Architecture

- Firewall :
  - Location:
    - Typically positioned at the network perimeter (between internal network and external networks).
    - Can also be deployed at the gateway of a segment within the network.
  - Layer:
    - Operates mainly at Layer 3 (Network Layer) and Layer 4 (Transport Layer), but some firewalls (e.g., Next-Generation Firewalls) can also operate at Layer 7 (Application Layer).
  - Mechanism:
    - Uses rules and policies to allow or deny traffic based on IP addresses, ports, and protocols.
    - Can perform stateful inspection, packet filtering, or proxying.

Firewall, IDS, and IPS in Network Architecture

- Intrusion Detection System (IDS)
  - Location:
    - Can be placed inside the network (NIDS) to monitor traffic across segments or on individual hosts (HIDS).
  - Layer:
    - Primarily operates at Layer 3 (Network Layer) and Layer 7 (Application Layer) for analyzing traffic and payloads.
  - Mechanism:
    - Analyzes network traffic for patterns or signatures that indicate potential intrusions.
    - Generates alerts for suspicious activities but does not take action to block them.

Firewall, IDS, and IPS in Network Architecture

- Intrusion Prevention System (IPS)
  - Location:
    - Positioned inline with network traffic, often immediately behind firewalls or integrated into them.
  - Layer:
    - Functions at Layer 3 (Network Layer) and Layer 7 (Application Layer) for real-time monitoring and response.
  - Mechanism:
    - Monitors network traffic and uses rules or behavioral analysis to detect and block potential threats.
    - Can drop malicious packets, block IP addresses, and prevent unauthorized access in real-time.

Encoding, Encryption, Hashing, Obfuscation:

- Encoding: Transforming data to a different format (Base64).
- Encryption: Securing data using keys (AES, RSA).
- Hashing: Generating a fixed-size string from data (SHA-256).
- Obfuscation: Making code harder to understand (JavaScript obfuscation).

Symmetric vs. Asymmetric Encryption:

- Symmetric: Same key for encryption/decryption (AES).
- Asymmetric: Different keys for encryption/decryption (RSA).

Risk, Threat, Vulnerability, Exploit, Impact:

- Risk: Potential for loss/damage.
- Threat: Possible cause of an unwanted outcome.
- Vulnerability: Weakness that can be exploited.
- Exploit: Taking advantage of a vulnerability.
- Impact: Consequences of an exploit.

WAF (Web Application Firewall):

- Purpose: Protects web applications by filtering and monitoring HTTP traffic.
- Placement: In front of the web server.
- Comparison: Use WAF for web-specific attacks, IPS for broader network threats.

Antivirus

- Purpose: Detects and removes malware.
- Types: Signature-based, heuristic, behavior-based.

EPP (Endpoint Protection Platform):

- Purpose: Comprehensive security solution for endpoints.
- Features: Antivirus, anti-malware, firewall, intrusion prevention

EDR , XDR, NDR, MDR

- EDR: Detects and responds to threats at endpoints.
- XDR: Correlates data across multiple security layers.
- NDR: Detects and responds to network-based threats.
- MDR: Managed service that handles threat detection and response.

IOC, TTP

- ❖IOCs: Evidence of a potential breach (malicious IPs, file hashes).
- ❖TTPs: The behavior and methods used by attackers to achieve their objective
- ❖Components:
  - Tactics: High-level goals of an attacker (e.g., data exfiltration).
  - Techniques: The general means used to achieve tactics (e.g., phishing).
  - Procedures: Specific implementations of techniques (e.g., using a particular malware variant).

Payload

- a payload refers to the part of malware or a cyber attack that performs the malicious action after a successful exploit.
- Examples:
  - Malware Payload: Code that executes harmful activities, such as stealing data or encrypting files.
  - Network Payload: The actual data transmitted over a network packet, which can contain malicious content.

Brute-Force Attack:

- Mechanism: Attempting all possible combinations to guess passwords.
- Tools: Hydra, John the Ripper.
- Mitigation: Use complex passwords, rate-limiting, account lockout policies.

Hashing Attack Example ,Phishing Detection

- Mechanism: Cracking hashed passwords using tools like Hashcat.
- Phishing Detection:Email filtering, user education, anomalydetection.
- Phishing Mitigation:
  - Techniques: Multi-factor authentication, user training, email security solutions.

SPF, DKIM, DMARC:

- SPF (Sender Policy Framework): Validates email senders.
- DKIM (DomainKeys Identified Mail): Authenticates email content.
- DMARC (Domain-based Message Authentication, Reporting & Conformance): Aligns SPF and DKIM.

SQL Injection Attack:

- where an attacker inserts or "injects" malicious SQL code into query, allowing them to manipulate the database behind a web application.
- Types: Union-based, error-based, blind.
- Mitigation: Use prepared statements, input validation.

XSS Attack (Cross-Site Scripting)

- is a type of security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. This can lead to unauthorized actions and data theft.
- Types of XSS Attacks:
  1. Stored XSS: The malicious script is stored on the server (e.g., in a database) and delivered to users whenever they access the affected page.
  2. Reflected XSS: The malicious script is reflected off a web server, typically via a URL or request, and executed immediately when the link is clicked.
  3. DOM-based XSS: The attack occurs in the browser, where the malicious script manipulates the Document Object Model (DOM) to execute.
- Mitigation: Sanitize inputs, use Content Security Policy (CSP).

CSRF Attack (Cross-Site Request Forgery)

- is a type of attack where a malicious website tricks a user's browser into making unauthorized requests to a different website where the user is authenticated. This can lead to actions being performed on behalf of the user without their consent.
- Mitigation: Use anti-CSRF tokens, same-site cookies.

Cookie vs. Session:

- Cookie
  - Definition: A small piece of data stored on the user's browser by the web server.
  - Lifetime: Can persist beyond the session; expires based on set expiration time.
  - Storage: Stored on the client-side, accessible by both client and server.
  - Use: Often used for storing user preferences, login tokens, and tracking information.
- Session
  - Definition: A server-side storage mechanism that keeps track of user interactions during a session.
  - Lifetime: Exists as long as the user is active; typically expires after a period of inactivity.
  - Storage: Stored on the server, with a unique session ID sent to the client (usually in a cookie).
  - Use: Commonly used for managing user authentication and temporary data during a user's visit.

CSRF Token:

- Definition: A CSRF token is a unique, secret value generated by the server and included in web forms to prevent Cross-Site Request Forgery attacks.
- Purpose: It ensures that requests made to a web application come from authenticated users.

- How It Works:
  1. The server generates a token and includes it in forms.
  2. When the form is submitted, the token is sent with the request.
  3. The server verifies the token; if it matches, the request is processed.

SOC (Security Operations Center):

- Purpose: Monitors and responds to security incidents.
- Members: Analysts, incident responders, SOC managers.
- T1: Initial triage and monitoring.
- T2: Detailed analysis and response.
- T3: Advanced threat analysis and remediation.
- Manager: Oversees SOC operations.
- False Positive:
  - Definition: A false alarm indicating a threat where none exists.

SOP (Standard Operating Procedure) ,Runbook ,Playbook:

- ❖SOP: Documented procedures for operations.
- ❖Runbook: Steps to handle specific tasks.
- ❖Playbook: Detailed responses for specific incidents.

Alarm Incident vs. False Positive: When to Escalate

- Alarm Incident:
  - When to Escalate:
    - If the incident shows signs of being critical (e.g., data breach, system compromise).
    - If initial investigation indicates a real threat that could impact the organization.
- False Positive
  - When to Escalate:
    - Generally, no escalation is needed since it does not represent a real threat.
    - However, if false positives are frequent, escalate to review alerting rules or thresholds to improve accuracy.

SIEM (Security Information and Event Management):

- SIEM is a security solution that collects and analyzes log data from various sources to identify and respond to security threats in real-time.
- Key Functions:
  1. Data Collection: Gathers logs and events from servers, networks, and applications.
  2. Correlation: Analyzes data to identify patterns that may indicate security incidents.
  3. Alerting: Generates alerts for potential threats or anomalies.
  4. Reporting: Provides insights and reports for compliance and security monitoring.

Parsing, Normalization, Aggregation, Correlation:

- ❖Parsing: Extracting data from logs.
- ❖Normalization: Standardizing data formats.
- ❖Aggregation: Combining data points.
- ❖Correlation: Identifying related events.

Connecting Log Sources to SIEM

1. Agent-Based Collection
   - Description: Install an agent on servers or devices to collect data and send it to the SIEM.
   - Benefits: Collects detailed data and provides real-time support.
2. Syslog
   - Description: Use the Syslog protocol to send logs from devices to the SIEM.
   - Benefits: A common and easy method to connect various devices, such as network equipment and servers.
3. API Integration
   - Description: Use Application Programming Interfaces (APIs) to collect logs from applications or cloud services.
   - Benefits: Allows flexible data collection from multiple sources.
4. File-Based Collection
   - Description: Read logs from specific files on servers.
   - Benefits: Simple to implement, especially for local logs.

HTTP

- ❖HTTP Response Status Codes:
  - Examples: 200 (OK), 404 (Not Found), 500 (Internal Server Error).
- ❖HTTP Request Methods:

  Examples: GET, POST, PUT, DELETE.

DLP (Data Loss Prevention):

- is a security solution that helps prevent sensitive data from being lost, misused, or accessed by unauthorized users.
- Key Functions:
  1. Monitoring: Tracks data in use, in motion, and at rest.
  2. Policy Enforcement: Applies rules to control how sensitive data is handled and shared.
  3. Alerting: Notifies when data breaches or policy violations occur.

PAM && FIM

- ❖PAM (Privileged Access Management):
  - Purpose: Controls and monitors access to critical resources by privileged users.
  - Features: Just-in-time access, session recording, automated workflows.

- ❖FIM (File Integrity Monitoring):

  Purpose: Detects changes to files that may indicate a breach.

  Tools: Tripwire, OSSEC.

Threat Intelligence:

- Examples: Indicators of Compromise (IOCs), threat feeds, vulnerability databases.
- Purpose: Helps in identifying and mitigating threats.

Kerberos:

- is a network authentication protocol designed to provide secure communication over an insecure network. It uses tickets to allow nodes to prove their identity securely. Key components include:
  - Authentication Server (AS): Issues a Ticket Granting Ticket (TGT) after verifying the user's credentials.
  - Ticket Granting Server (TGS): Issues service tickets based on the TGT for access to specific services.
  - Client: Requests access to services by presenting the TGT and the service ticket.
  - Tickets: Time-limited credentials that allow users to access services without re-entering passwords.

NTLM (NT LAN Manager):

- Definition: Authentication protocol used in older Windows environments.
- Limitations: Vulnerable to certain attacks compared to Kerberos.

MBR && GPT

- ❖MBR (Master Boot Record):
  - Purpose: Contains boot loader and partition table for legacy BIOS systems.
  - Size: 512 bytes.
- ❖GPT (GUID Partition Table):
  - Purpose: Modern partitioning scheme for UEFI systems.
  - Advantages: Supports larger disks and more partitions than MBR.

File Systems:

- ❖NTFS: Advanced file system with support for large files, encryption.
- ❖FAT: Simple file system, widely compatible.
- ❖Btrfs: Modern file system with advanced features like snapshots.
- ❖OCFS: Cluster file system for shared disk access.

Malware, Detection, and Analysis:

- ❖Types: Virus, Worm, Trojan, Ransomware.
- ❖Detection: Signature-based, heuristic, behavior analysis.
- ❖Analysis: Static and dynamic analysis.

Virus, Worm, Trojan, Ransomware:

- Virus: Attaches to files and spreads.
- Worm: Self-replicates and spreads across networks.
- Trojan: Disguises as legitimate software.
- Ransomware: Encrypts files and demands ransom

Honeypot && Sandbox

- ❖Honeypot:
  - Purpose: Decoy system to attract and analyze attacks.
- ❖Sandbox:
  - Purpose: Isolated environment for safely running and analyzing suspicious code.
  - Examples: Cuckoo Sandbox, FireEye.

Text File && Port Scanning as Malware

- ❖Text File as Malware:
  - Mechanism: Exploits vulnerabilities in file parsing to execute code.
  - Analysis: Examine file structure, behavior analysis.
- ❖Port Scanning Mitigation:
  - Information: Identify source IP, frequency of scans.
  - Mitigation: Use firewalls, intrusion detection systems, rate limiting.

Digital Forensics:

- Definition: Investigates digital devices for evidence.
- Purpose: Supports legal cases, incident response.
- Types: Computer forensics, mobile device forensics, network forensics.
- Tools: EnCase, FTK, Autopsy.