Security Techniques

Objectives:

- 4.1 - Given a scenario, you must be able to apply common security techniques to computing resources
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Security Techniques**
    - *Security Techniques*
        - Protecting digital assets from evolving cyber threats
        - Scope
            - Traditional to advanced security techniques
    - Study Topics
        - Wireless Infrastructure Security
            - Significance of wireless networks
            - Challenges and security considerations
        - Wireless Security Settings
            - WPA3, AAA/RADIUS, Cryptographic protocols
            - Authentication protocols in wireless security
        - Application Security
            - Input validation, secure cookies
            - Static and dynamic code analysis
            - Code signing and sandboxing
        - Network Access Control (NAC)
            - Purpose and functionality of NAC

            - Policy enforcement on devices and users
        - Web and DNS Filtering
            - Agent-based web filters, centralized proxy
            - URL scanning, content categorization, block rules
            - Reputation-based filtering
        - Email Security
            - DMARC, DKIM, SPF protocols
            - Gateway protocol and spam filtering techniques
        - Endpoint Detection and Response (EDR)
            - Continuous monitoring of endpoint devices
            - Identifying, investigating, and preventing cyber threats
        - User Behavior Analytics (UBA)
            - Leveraging machine learning and data analytics
            - Identifying potentially harmful activities
            - Detection of anomalies or deviations
        - Selecting Secure Protocols
            - Protocol selection, port selection
            - Transport method selection

- **Wireless Infrastructure Security**
    - *Wireless Infrastructure Security*
        - Crucial for securing wireless networks in organizations
        - Placement of Wireless Access Points (WAPs) impacts network performance and security
    - *Wireless Access Point Placement*
        - WAPs allow wireless devices to connect to a wired network using Wi-Fi standards

- Placement influences
  - Network range
  - Coverage
  - Security
- Proper placement prevents unauthorized access by limiting signal leakage or dead zones
- Is a huge concern in terms of the security of the wireless network

- Placement Considerations
  - Avoid placing WAPs near external walls or windows to prevent signal leakage
  - Place WAPs in central locations for optimal coverage
  - Use unidirectional antennas when WAPs are near external walls
  - Mount WAPs on higher locations, such as ceilings, for better coverage
- *Extended Service Set (ESS)*
  - Multiple WAPs work together to provide seamless network coverage
  - Important for large buildings where a single WAP is insufficient
- *Wireless Access Point Interference*
  - Interference occurs when multiple WAPs use the same channels or overlapping frequencies
  - Types
    - Co-Channel Interference
    - Adjacent Channel Interference
  - In the 2.4 GHz band, select Channels 1, 6, and 11 to avoid overlap
- Tools for ensuring good Wireless Access Point Coverage
  - *Site Surveys*
    - Essential for planning and designing wireless networks
    - Involves a site visit to test for radio frequency interference and identify

optimal WAP installation locations

- *Heat Maps*
    - Graphical representations of
        - Wireless coverage
        - Signal strength
        - Frequency utilization
    - Useful for troubleshooting
        - Coverage issues
        - Dead zones
        - Signal leakage
    - Aid in visualizing the effectiveness of WAP placement and configuration

- **Wireless Security Settings**
    - *Wireless Security Settings*
        - Crucial for securing wireless networks due to increasing usage
    - *Wireless Encryption*
        - Wireless encryption is essential for data confidentiality in wireless networks
    - *WEP (Wired Equivalent Privacy)*
        - Introduced in 1999 as part of IEEE 802.11
        - Utilizes a static encryption key system
        - Considered insecure due to its weak 24-bit initialization vector
    - *WPA (Wi-Fi Protected Access)*
        - Introduced in 2003 as an improvement over WEP
        - Implemented TKIP for dynamic key generation
        - Inherited some vulnerabilities from WEP
        - Due to TKIP vulnerabilities, it was susceptible to cryptographic attacks

  - Insecure due to insufficient data integrity checks in the TKIP implementation
- *WPA2 (Wi-Fi Protected Access 2)*
  - Introduced in 2004, replacing WPA.
  - Uses AES protocol and CCMP protocol for stronger encryption
    - AES - Advanced Encryption Standard
    - CCMP - Counter Cipher Mode with Block Chaining Message Authentication Code
  - Introduced Message Integrity Code (MIC) for integrity checking
- *WPA3 (Wi-Fi Protected Access 3)*
  - The latest and most secure wireless security protocol.
  - Uses AES for encryption and introduces new features.
  - Features
    - *Simultaneous Authentication of Equals (SAE)*
      - Replaces the 4-way handshake with a Diffie-Hellman key agreement
      - Protects against offline dictionary attacks
    - *Enhanced Open (Opportunistic Wireless Encryption)*
      - Provides individualized data encryption even in open networks
      - Improves privacy and security in open Wi-Fi scenarios
    - *Updated Cryptographic Protocols*
      - AES GCMP replaces AES CCMP used in WPA2
      - Supports both 128-bit and 192-bit AES for enhanced security
    - *Management Frame Protection*
      - Ensures the integrity of network management traffic
      - Prevents eavesdropping, forging, and tampering with management frames

- *AAA Protocols*
    - Important for centralized user authentication and access control
    - Examples
        - *RADIUS (Remote Authentication Dial-In User Service)*
            - Offers Authentication, Authorization, and Accounting services
            - Widely used for secure access to network resources
        - *TACACS+ (Terminal Access Controller Access-Control System Plus)*
            - Separates Authentication, Authorization, and Accounting functions
            - More granular control
            - Encrypts the authentication process using TCP for enhanced security
- *Authentication Protocols*
    - Used to verify user identity and control network access
    - *EAP (Extensible Authentication Protocol)*
        - Authentication framework supporting multiple methods
        - Provides common functions and negotiation of authentication protocols
    - *PEAP (Protected Extensible Authentication Protocol)*
        - Encapsulates EAP within an encrypted TLS tunnel
        - Developed jointly by Cisco Systems, Microsoft, and RSA Security
    - *EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)*
        - Extends TLS support across platforms
        - Requires server-side certificates for security
    - *EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)*
        - Developed by Cisco Systems for secure re-authentication

            - Uses a Protected Access Credential and TLS tunnel

- **Application Security**
    - *Application Security*
        - Focuses on building secure applications
        - Aims to prevent, detect, and remediate security vulnerabilities
    - Six Key Areas in Application Security
        - *Input Validation*
            - Ensures that applications process well-defined, secure data
            - Guards against attacks exploiting data input vulnerabilities (e.g., SQL injection, XSS, buffer overflows)
            - Serves as a kind of quality control for data to ensure that every piece of information is valid, secure, and correctly formatted
            - *Validation Rules*
                - Delineate acceptable and unacceptable inputs
            - Validates data early in the process (front-end validation)
            - Used with additional tools for defense in-depth
                - Secure communication protocols
                - Regular security auditing
                - Implementing proper error handling
        - *Cookies*
            - Small data pieces stored by web browsers
            - Maintain stateful information between the server and client
            - *Secure Cookies*
                - Secure cookies are transmitted over HTTPS for enhanced security

        - Best practices
            - Refraining from persistent cookies for session verification
            - Enabling the Secure attribute
            - Enabling HttpOnly attribute
            - Configuring the SameSite attribute
    - *Static Code Analysis (SAST)*
        - A method of debugging an application by reviewing and examining its source code before running the program
        - Identifies issues like buffer overflows, SQL injection, and XSS
        - Important for proper input validation in both front-end and back-end code
    - *Dynamic Code Analysis (DAST)*
        - Analyzes applications while they run
        - Common methods of DAST
            - *Fuzzing (Fuzz Testing)*
                - Inputs random data to provoke crashes or exceptions
                - Helps uncover security flaws and weaknesses
            - *Stress Testing*
                - Evaluates system stability and reliability under extreme conditions
                - Reveals bottlenecks and assesses system recovery
    - *Code Signing*
        - Confirms the software author's identity and integrity
        - Utilizes digital signatures to verify code authenticity
        - Protects against code tampering but doesn't guarantee absence of vulnerabilities

            - *Sandboxing*
                - Isolates running programs, limiting their access to resources
                - Prevents harmful actions on the host device or network
                - Used to execute untrusted or untested programs securely

- **Network Access Control (NAC)**
    - *Network Access Control (NAC)*
        - Used to protect networks from both known and unknown devices by scanning devices to assess their security status before granting network access
        - Can be applied to devices within the internal network or those connecting remotely via VPN
        - NAC can be implemented as a hardware or software solution
    - NAC Process
        - When a device attempts to connect, it is placed in a virtual holding area for scanning
        - Scanning checks various factors, including antivirus definitions, security patching, and potential security threats
        - If a device passes inspection, it is allowed network access
        - If a device fails inspection, it is placed in a digital quarantine area for remediation
    - NAC Agent Types
        - *Persistent Agents*
            - Installed on devices in a corporate environment where the organization owns and controls device software
        - *Non-Persistent Agents*
            - Common in environments with personal devices (e.g., college campuses); users connect, access a web-based captive portal, download an agent for

scanning, and delete itself after inspection

- *802.1x Standard*
    - Port-based Network Access Control mechanism based on the IEEE 802.1x standard
    - Modern NAC solutions build on 802.1x, enhancing features and capabilities
- *Rule-Based Access Control*
    - In addition to health policy, NAC can use rule-based methods for access control
        - *Time-Based Factors*
            - Define access periods based on time schedules; may block access during non-working hours
        - *Location-Based Factors*
            - Evaluate the endpoint's location using geolocation data to detect unusual login locations
        - *Role-Based Factors*
            - Reevaluate device authorization based on its role (adaptive NAC)
        - *Rule-Based Factors*
            - Implement complex admission policies with logical statements to determine access based on conditions

- **Web and DNS Filtering**
    - *Web Filtering*
        - Web filtering or content filtering is used to control or restrict the content users can access on the internet
        - Crucial for businesses, educational institutions, and parents to ensure safe and productive internet use

- Different types of web filtering techniques
  - *Agent-Based Web Filtering*
    - Involves installing an agent on each device
    - Monitors and enforces web usage policies
    - Effective for remote and mobile workers
  - *Centralized Proxy*
    - Uses a proxy server as an intermediary between an organization's end users and the Internet
    - Evaluates and controls web requests based on policies
    - If the request does not conform with the policies, the request is simply blocked or denied
  - *URL Scanning*
    - Analyzes website URLs to check for matches in a database of known malicious websites
  - *Content Categorization*
    - Classifies websites into categories (e.g., social media, adult content) and blocks or allows categories based on policies
  - *Block Rules*
    - Specific guidelines set by organizations to prevent access to certain websites or categories, often used to address security threats
  - *Reputation-Based Filtering*
    - Blocks or allows websites based on a reputation score determined by third-party services, considering factors like hosting malware or phishing
- *DNS Filtering*
  - DNS filtering (Domain Name System filtering) blocks access to specific websites by preventing the translation of domain names to their IP addresses

        - Users' devices request domain name translation from DNS servers; if the domain is on the block list, the server withholds the IP address to prevent access
        - Commonly used to enforce internet usage policies, block inappropriate content, and protect against malicious websites
        - Often employed by schools, universities, and organizations to ensure safe and educational internet usage

- **Email Security**
    - *Email Security*
        - Encompasses techniques and protocols to protect email content, accounts, and infrastructure from unauthorized access, loss, or compromise
    - Key email security techniques
        - *DKIM (DomainKeys Identified Mail)*
            - Allows the receiver to verify the source and integrity of an email by adding a digital signature to the email headers
            - The recipient server validates the DKIM signature using the sender's public cryptographic key in the domain's DNS records
            - Benefits
                - Email authentication
                - Protection against email spoofing
                - Improved email deliverability
                - Enhanced reputation score
        - *SPF (Sender Policy Framework)*
            - Prevents sender address forgery by verifying the sender's IP against authorized IPs listed in the sender's domain DNS records
            - A receiving server checks if the sender's IP is authorized in the SPF record

        before accepting the email
    - Benefits
        - Preventing email spoofing
        - Improving email deliverability
        - Enhancing the domain's reputation
- *DMARC (Domain-based Message Authentication, Reporting and Conformance)*
    - DMARC detects and prevents email spoofing by setting policies for email sending and handling failures
    - DMARC can work with DKIM, SPF, or both
    - Implementation helps protect against
        - Business email compromise attacks
        - Phishing
        - Scams
        - Cyber threats
- *Email Gateway Protocol Configuration*
    - Email gateways serve as entry and exit points for emails, facilitating secure and efficient email transmission
    - They use SMTP (Simple Mail Transfer Protocol) to send and receive emails
    - Email gateways handle email routing, email security, policy enforcement, and email encryption
    - Email Gateway Deployment Options
        - *On-Premises Email Gateway*
            - A physical server located within an organization's premises, offering full control but requiring maintenance and updates

        - *Cloud-Based Email Gateway*
            - Hosted by third-party cloud service providers, providing scalability but limited control over configurations
        - *Hybrid Email Gateway*
            - Combines on-premises and cloud-based gateways for a balance between control and convenience
    - *Spam Filtering*
        - Spam filtering detects and prevents unwanted and unsolicited emails from reaching users' inboxes
        - Techniques
            - Content analysis
            - Bayesian filtering
            - DNS-based sinkhole list
            - Email filtering rules
        - Emails with spam-like keywords are flagged and often moved to the spam folder

- **Endpoint Detection and Response**
    - *Endpoint Detection and Response (EDR)*
        - Category of security tools that monitor endpoint and network events and record the information in a central database
        - Continuously monitoring and response to advanced threats
        - Monitors endpoint and network events, providing data for the following
            - Analysis
            - Detection
            - Investigation
            - Reporting

                - Alerting
            - Focuses on incident data for enhancing security monitoring, incident response, and forensic investigations
        - How EDR Works
            - *Data Collection*
                - Collects data from endpoints (devices that are physically on the endpoint of a network)
                    - System processes
                    - Registry changes
                    - Memory usage
                    - Network traffic patterns
            - *Data Consolidation*
                - Sends collected data to a centralized security solution or database
            - *Threat Detection*
                - Analyzes data using techniques like signature-based and behavioral-based detection to identify threats
            - *Alerts and Threat Response*
                - Takes actions such as creating alerts or performing threat response actions when threats are detected
            - *Threat Investigation*
                - Provides tools for security teams to investigate threats, including detailed timelines and forensic data
            - *Remediation*
                - Removing malicious files
                - Reversing changes
                - Restoring systems to their normal state

- *File Integrity Monitoring (FIM)*
    - Validates the integrity of operating system and application software files by comparing their current state with a known, good baseline
    - Identifies changes to
        - Binary files
        - System and Application Files
        - Configuration and Parameter Files
    - Monitors critical system files for changes using agents and hash digests, triggering alerts when unauthorized changes occur
- *Extended Detection and Response (XDR)*
    - Security strategy that integrates multiple protection technologies into a single platform
    - Improves detection accuracy and simplified incident response
    - Correlates data across multiple security layers to detect threats faster, including
        - email
        - endpoint
        - server
        - cloud workloads
        - network
- Difference between EDR and XDR
    - EDR is focused on the endpoints to detect and respond to potential threats
    - XDR is more comprehensive solution because it focuses on endpoints, but also on networks, cloud, and email to detect and respond to potential threats
        - It integrates multiple protection technologies

- **User Behavior Analytics**
  - *User Behavior Analytics (UBA)*
    - Advanced cybersecurity strategy that uses big data and machine learning to analyze user behaviors for detecting security threats
    - Focuses on understanding user behavior within systems and networks to identify patterns and anomalies
  - *User and Entity Behavior Analytics (UEBA)*
    - Technology similar to UBA but extends the monitoring of entities like routers, servers, and endpoints in addition to user accounts
    - Enhances security by analyzing both user and entity behavior to detect anomalies
  - Key Aspects of UBA and UEBA
    - UBA leverages data analytics to collect and analyze user behavior data to establish normal behavior baselines
      - Knowing the baseline makes it easier to spot anomalies
    - Machine learning algorithms are used to identify deviations from normal behavior, which may indicate security threats
    - UBA systems process data from various sources
      - Network traffic
      - User devices
      - Application logs
    - Alerts are generated when anomalies are detected, which are then investigated by the security team
  - Benefits of UBA and UEBA
    - Early Detection of Threats
      - UBA tools can identify potential threats before significant damage occurs,

allowing for quicker and more effective responses

    - Insider Threat Detection
        - Effective at identifying insider threats by detecting suspicious activities that deviate from typical behavior
    - Improved Incident Response
        - Provides detailed information about user behavior, helping security teams respond effectively to incidents, such as compromised credentials or unauthorized actions

- **Selecting Secure Protocols**
    - *Secure Protocols*
        - Choose secure protocols to protect data in transit from unauthorized access
            - Examples include HTTP vs. HTTPS, FTP vs. SFTP, Telnet vs. SSH
        - Secure protocols use encryption to safeguard data during transmission
        - *Telnet*
            - Application layer protocol that allows a user on one computer to log onto another computer that is part of the same network
            - Transmits in plaintext
            - Use SSH instead
        - Always use the encrypted version of the protocol
            - Examples
                - HTTPS
                - SFTP
                - SSH
                - IMAPS
                - POP3S

        - SMTPS
        - SNMPS
- Port Selection
    - Ports are logical constructs used to identify processes or services on a system
    - Categorized into the following
        - Well-known ports (0-1023)
        - Registered ports (1024-49151)
        - Dynamic/private ports (49152-65535)
    - Default port numbers often indicate whether a protocol is secure (e.g., HTTP on port 80 vs. HTTPS on port 443)
    - Additional security considerations
        - Follow the principle of least privilege by opening only necessary ports to minimize the attack surface
        - Changing port numbers can add a layer of obscurity but should not replace robust security measures
- Transport Methods
    - Choose a transport method (TCP or UDP) based on the application's needs
    - *TCP (Transmission Control Protocol)*
        - Connection-oriented, ensuring data delivery without errors
        - Ideal for applications where data accuracy is crucial, like web and email servers
        - Uses acknowledgments, retransmission, and sequencing for data integrity
    - *UDP (User Datagram Protocol)*
        - Connectionless and faster, but doesn't guarantee data delivery
        - Suitable for applications prioritizing speed over accuracy, like streaming video or gaming