UNIT 6

Hacking Wi-Fi and Bluetooth

1. **What Is a Wireless Network?**
   A wireless network uses radio waves instead of wires to connect devices. It enables communication between devices like computers, smartphones, and IoT devices over a wireless medium (e.g., Wi-Fi).
   Key Features:
   - Provides flexibility and mobility.
   - Common standards: IEEE 802.11 (Wi-Fi).
2. **A Close Examination of Threats**:
   Wireless networks face specific vulnerabilities:
   - **Eavesdropping**: Intercepting data sent over the network.
   - **Rogue Access Points**: Unauthorized devices mimicking legitimate access points.
   - **Deauthentication Attacks**: Disconnecting users from the network.
   - **Weak Encryption**: Exploiting outdated security protocols like WEP.
3. **Hacking Bluetooth**:
   Bluetooth vulnerabilities can be exploited to:
   - **Bluejacking**: Sending unsolicited messages.
   - **Bluesnarfing**: Unauthorized access to a device's information.
   - **Bluebugging**: Taking control of a device to make calls or access data.
4. **Introduction to SIEM and SOC Solutions**:
   - **SIEM (Security Information and Event Management)**: A tool for real-time monitoring and analysis of security logs.
     - Correlates events to identify threats.
   - **SOC (Security Operations Center)**: A centralized team monitoring an organization’s IT infrastructure to detect and respond to security incidents.

Mobile Device Security

1. **Mobile OS Models and Architectures**:
   Mobile operating systems manage hardware and software resources for smartphones.
   - **Common OS**: Android, iOS.
   - **Architectures**:
     - **Kernel Layer**: Manages core processes and memory.
     - **Application Layer**: Interfaces for user applications.
     - **Middleware Layer**: Facilitates communication between apps and OS.
2. **Goals of Mobile Security**:
   - **Confidentiality**: Protecting sensitive user data.
   - **Integrity**: Ensuring data isn't tampered with.
   - **Availability**: Preventing denial-of-service on devices.
3. **Device Security Models**:
   - **Sandboxing**: Isolating apps to prevent unauthorized data access.
   - **Encryption**: Protecting stored and transmitted data.
   - **Biometric Authentication**: Securing access with fingerprints or facial recognition.
4. **Countermeasures**:
   - **User Awareness**: Educating users about phishing and malware.
   - **Regular Updates**: Patching vulnerabilities in the OS and apps.
   - **Mobile Device Management (MDM)**: Centralized security for enterprise devices.
   - **App Permissions**: Limiting apps to necessary permissions only.

Important MCQ for Unit 6

Hacking Wi-Fi and Bluetooth

1. What standard is most commonly associated with wireless networks?
   a) IEEE 802.3
   b) IEEE 802.11
   c) IEEE 802.15
   d) IEEE 802.16
   Answer: b

2. Which attack disconnects users from a Wi-Fi network?
   a) ARP Poisoning
   b) Deauthentication Attack
   c) Evil Twin Attack
   d) Rogue Access Point
   Answer: b

3. What is the main vulnerability of WEP encryption?
   a) Weak key management
   b) Large key size
   c) Requires high processing power
   d) Uses multiple layers of encryption
   Answer: a

4. A rogue access point is:
   a) A legitimate Wi-Fi network with poor security
   b) An unauthorized device mimicking a legitimate network
   c) A tool used for encryption
   d) An access point that blocks other devices
   Answer: b

5. What is **Bluejacking** in Bluetooth hacking?
   a) Gaining full control of a Bluetooth device
   b) Intercepting data transfers
   c) Sending unsolicited messages to a Bluetooth device
   d) Exploiting weak encryption in Bluetooth connections
   Answer: c

6. What tool is often used for packet capturing in Wi-Fi networks?
   a) Wireshark
   b) Metasploit
   c) SQLmap
   d) Nmap
   Answer: a

7. Which type of attack involves stealing data from a Bluetooth device?
   a) Bluejacking
   b) Bluesnarfing
   c) Bluebugging
   d) Spoofing
   Answer: b

8. What is the purpose of WPA3 in Wi-Fi security?
   a) To improve data speed
   b) To enhance encryption and security features
   c) To increase range
   d) To allow more devices on a network
   Answer: b

9. What is the primary role of a Security Operations Center (SOC)?
   a) Designing software
   b) Performing daily backups
   c) Monitoring and responding to security incidents
   d) Managing hardware configurations
   Answer: c

10. Which of the following is NOT a Bluetooth vulnerability?
    a) Bluebugging
    b) Rogue Access Point
    c) Bluejacking
    d) Bluesnarfing
    Answer: b

Mobile Device Security

11. Which mobile operating system is open-source?
    a) iOS
    b) BlackBerry OS
    c) Android
    d) Windows Phone
    Answer: c

12. What is **sandboxing** in mobile device security?
    a) Encrypting all device data
    b) Isolating apps to prevent unauthorized access
    c) Securing communications over Bluetooth
    d) Allowing apps to access system files
    Answer: b

13. The main goal of mobile device management (MDM) is to:
    a) Enable data sharing between devices
    b) Centralize the security of enterprise devices
    c) Backup personal devices automatically
    d) Remove restrictions on app usage
    Answer: b

14. Biometric authentication includes:
    a) Passwords and PINs
    b) Fingerprint and facial recognition
    c) Two-factor authentication
    d) CAPTCHA tests
    Answer: b

15. Which layer in a mobile OS manages hardware?
    a) Kernel Layer
    b) Middleware Layer
    c) Application Layer
    d) Presentation Layer
    Answer: a

16. What is the primary goal of encryption in mobile security?
    a) Speeding up data processing
    b) Hiding network connectivity
    c) Protecting data confidentiality
    d) Preventing app installations
    Answer: c

17. What is the purpose of regular updates in mobile security?
    a) To improve the device's speed
    b) To patch vulnerabilities in the OS and apps
    c) To free up storage space
    d) To install new features
    Answer: b

18. Which attack can compromise mobile device security by exploiting malicious apps?
    a) Phishing
    b) Ransomware
    c) Trojan Malware
    d) Rootkit Installation
    Answer: c

19. What is the function of application permissions in mobile devices?
    a) To improve app performance
    b) To limit app access to specific resources
    c) To enable multi-user access
    d) To provide free features in paid apps
    Answer: b

20. What does the term "Bring Your Own Device (BYOD)" imply?
    a) Employees using personal devices for work purposes
    b) Companies issuing personal devices to employees
    c) Employees developing their own software
    d) Companies implementing uniform security policies
    Answer: a

General Security Concepts

21. Which of the following threats is unique to wireless networks?
    a) Eavesdropping
    b) Brute Force Attack
    c) SQL Injection
    d) Malware Infections
    Answer: a

22. What protocol encrypts communication in Wi-Fi networks?
    a) HTTPS
    b) WPA
    c) TCP/IP
    d) ARP
    Answer: b

23. What is the primary weakness of public Wi-Fi networks?
    a) Poor speed
    b) Limited connections
    c) Lack of encryption
    d) Inconsistent signal strength
    Answer: c

24. What is the goal of Mobile Device Management (MDM)?
    a) Securely manage enterprise mobile devices
    b) Improve device performance
    c) Increase device storage
    d) Replace user authentication systems
    Answer: a

25. Which is an example of a countermeasure against unauthorized app installation?
    a) Enabling app sandboxing
    b) Increasing CPU speed
    c) Decreasing app download size
    d) Allowing unrestricted app permissions
    Answer: a

SIEM and SOC

26. SIEM solutions focus on:
    a) Preventing app crashes
    b) Analyzing and correlating security events
    c) Increasing software usability
    d) Managing employee productivity
    Answer: b

27. What is the main output of SOC operations?
    a) Security incident reports and mitigations
    b) Improved hardware performance
    c) Faster application loading
    d) Automated app testing
    Answer: a

28. What type of analysis does SIEM perform?
    a) Real-time monitoring and log analysis
    b) File size reduction
    c) Application testing
    d) Encryption verification
    Answer: a

29. Why are threat intelligence feeds integrated with SIEM?
    a) To improve data storage
    b) To enable proactive detection of new threats
    c) To reduce system updates
    d) To enhance graphical interfaces
    Answer: b

30. What is one challenge faced by SOC teams?
    a) Limited log storage
    b) Overwhelming number of alerts
    c) Lack of secure communication protocols
    d) Outdated software versions
    Answer: b

---

10 More MCQs for Exam Preparation

Hacking Wi-Fi and Bluetooth

1. What is the primary function of WPA3 in wireless networks?
    a) Providing stronger encryption and password security
    b) Increasing Wi-Fi range
    c) Speeding up data transmission
    d) Reducing network latency
    Answer: a

2. Which Bluetooth attack involves controlling a device to make calls or access data?
    a) Bluejacking
    b) Bluesnarfing
    c) Bluebugging
    d) Bluetooth Spoofing
    Answer: c

3. A deauthentication attack primarily targets:
    a) The encryption algorithm
    b) The connected devices on a network
    c) The router's IP configuration
    d) The firewall settings
    Answer: b

4. SIEM is mainly used for:
    a) Conducting penetration testing
    b) Monitoring and analyzing security events
    c) Managing network devices
    d) Backing up system data
    Answer: b

Mobile Device Security

5. What is the primary goal of encryption in mobile communication?
   a) To ensure data is transmitted faster
   b) To protect the confidentiality and integrity of data
   c) To simplify network connectivity
   d) To increase app compatibility
   Answer: b

6. What feature in mobile devices isolates apps to prevent unauthorized data access?
   a) Encryption
   b) Sandboxing
   c) MDM
   d) Biometric authentication
   Answer: b

7. Which of these is a countermeasure for securing mobile devices?
   a) Disabling encryption
   b) Updating the OS and applications regularly
   c) Using outdated software versions
   d) Avoiding the use of strong passwords
   Answer: b

General Security Concepts

8. Rogue access points are commonly used for:
   a) Network testing
   b) Hiding legitimate traffic
   c) Capturing sensitive data from unsuspecting users
   d) Speeding up Wi-Fi connections
   Answer: c

9. What is the primary focus of a Security Operations Center (SOC)?
   a) Software development
   b) Real-time threat monitoring and response
   c) Network configuration
   d) Data analysis for business intelligence
   Answer: b

SIEM and SOC

10. Why is log correlation important in SIEM systems?
    a) To reduce network congestion
    b) To identify and analyze security threats across multiple sources
    c) To improve server performance
    d) To automate software updates
    Answer: b