A black and white photo of a black background

AI-generated content may be incorrect.

**DAY PLAN**

**Week 7 Day 01**

Day 03 Generator - **Configuring SOHO Network Security**

Day Identifier and Context

* **Day Number**: Day 01
* **Week Number**: Week 07
* **Day Title**: Configuring SOHO Network Security
* **Following Day Preview**: Day 02 will focus on Mobile Security, Data Destruction, and Network Security. The morning session will cover mobile device security threats, hardening techniques, and data destruction methods, including secure disposal practices. Students will explore the threat landscape, apply mobile security configurations, and evaluate data disposal options. The afternoon session will include hands-on activities, focusing on implementing mobile security configurations and configuring secure SOHO networks. The day will conclude with an AI-powered certification prep session and a reflection activity to consolidate learning.

Certification Domains and Objectives

* **Primary Domain(s)**: Security 2.0, Software Troubleshooting 3.0
* **Specific Objectives**:
  + 2.5: Compare and contrast common social engineering attacks, threats, and vulnerabilities
* **Objective Weightings**: These objectives represent approximately 5% of the CompTIA A+ Core 2 exam
* **Key Terms**: Phishing, Spear-phishing, SQL Injection, XSS, Social Engineering, Password Attacks, Whaling, Vishing, Smishing, Evil Twin, and others.

Morning Session Details

* **Session Learning Objectives**:
  1. Understand phishing and its variants such as spear-phishing, whaling, vishing, smishing, and evil twin attacks.
  2. Learn about password attacks, including methods for intercepting and cracking passwords.
  3. Identify the differences between internal and external threats and understand their consequences.
  4. Understand SQL injection attacks, their methods, and how to prevent them.
  5. Explore the concept of cross-site scripting (XSS) attacks and methods for mitigating them.
  6. Recognize vulnerabilities in systems, including the risks posed by zero-day attacks, unpatched systems, and legacy software.
  7. Learn about social engineering techniques, such as impersonation, dumpster diving, shoulder surfing, and tailgating, and how to prevent them.

**Topic Breakdown**:

* **Session: Attacks, Threats, and Vulnerabilities – (90 minutes)**
* **Phishing and Evil Twins:**
* **Phishing Overview:** Phishing is a social engineering attack where attackers impersonate trusted entities to steal sensitive information, often through emails or fraudulent websites.
* **Phishing Variants:**
* Spear-phishing targets specific individuals with personalized information.
* Whaling targets high-level executives using more sophisticated methods.
* Vishing involves voice-based attacks like phone calls.
* Smishing uses SMS to trick users into clicking malicious links.
* Evil Twin Attacks involve rogue wireless networks set up to steal user data.
* **Password Attacks**
* Password attacks aim to break or guess user passwords to gain unauthorized access to systems.
* **Types of Password Attacks:**
* Brute-force attacks try all possible combinations until the correct one is found.
* Dictionary attacks use precompiled lists of common passwords to find matches.
* **Cryptographic Hashing:**
* Hashing turns passwords into fixed-length strings, which are difficult to reverse.
* This makes stored passwords more secure.
* **Prevention Methods:**
* Enforce strong password policies (e.g., length, complexity).
* Encourage the use of multi-factor authentication (MFA) to increase security.
* **Social Engineering**
* Social engineering exploits human trust to gain unauthorized access.
* **Techniques:**
* Impersonation: Attackers pretend to be someone the victim knows or trusts (e.g., IT support).
* Dumpster Diving: Attackers search through physical or digital trash to gather information.
* Shoulder Surfing: Observing someone to gather sensitive data, such as passwords or PINs.
* Tailgating: Following someone into a secure area without proper authorization.

1. **Attack Mitigation Strategies:**

* **Phishing Prevention:**
* Train employees to recognize phishing attempts.
* Implement email filtering and use digital certificates for secure communication.
* **Password Attack Prevention:**
* Enforce password complexity and use password managers.
* Utilize MFA for additional security.
* **Social Engineering Mitigation:**
* Conduct regular training to help employees recognize social engineering tactics.
* Implement strict security policies for physical and remote access.
* **Activity: Identifying Phishing and Social Engineering – (30 minutes)**
* **Objective:** Review real-life scenarios of phishing and social engineering attacks. Identify attack types and propose preventive measures.
* **MORNING BREAK – (15 minutes)**
* **Session 2: Attacks, Threats, and Vulnerabilities (cont’d) – (90 minutes)**
* **Session Overview:**
* This session will continue exploring cybersecurity threats and mitigation strategies, focusing on SQL injection and XSS attacks.
* **Content Breakdown:**

1. **SQL Injection Attacks**

* **Overview of SQL Injection:**
* Attackers exploit vulnerabilities in SQL queries by injecting malicious code into user input fields (e.g., search bars or login forms).
* **Impact of SQL Injection:**
* SQL injections can allow attackers to access, manipulate, or delete data from a database, leading to security breaches.
* **Prevention Techniques:**
* *Input sanitization:* Ensure that user inputs are cleaned and validated.
* *Parameterized queries* treat user input as data, not executable code.
* Regular patching and vulnerability scanning can prevent exploitation.

1. **Cross-Site Scripting (XSS) Attacks**

* **Overview of XSS Attacks:**
* XSS attacks inject malicious scripts into trusted websites, which are then executed by the victim’s browser.
* **Types of XSS:**
* *Persistent XSS* stores malicious code in a database, affecting all users.
* *Non-persistent XSS* involves inserting malicious code that executes during the victim’s session.
* **Prevention Methods:**
* **Input Validation and Output Encoding:** Ensure that user inputs are sanitized, and potentially harmful scripts are encoded.
* **Content Security Policies (CSP):** Implement CSP to restrict which scripts can run in the browser.

1. **Vulnerabilities in Systems**

* **Types of Vulnerabilities:**
* Misconfigured or outdated software, untested patches, and unsecured communication protocols can expose systems to attacks.
* **Non-compliant Systems** may drift from secure configurations, increasing the attack surface.
* **System Hardening:**
* Enforce secure configuration baselines and conduct regular security audits to identify and address vulnerabilities.
* **Unprotected Systems:**
* Lack of security controls such as firewalls or antivirus software increases the risk of system exploitation.

1. **Mitigation Strategies for XSS and SQL Injection:**

* **For XSS:**
* Use *Content Security Policies* to block malicious scripts.
* Apply proper input validation and avoid reflecting untrusted data in the browser.
* **For SQL Injection:**
* Apply parameterized queries and avoid direct user input in SQL commands.
* **Activity: Identifying and Preventing Cyber Threats – Real-World Scenarios – (45 minutes)**
* **Objective:** Review real-world scenarios, identify attack types (Phishing, Password Attacks, SQL Injection, etc.), and propose solutions.

Afternoon Session Details

* **Lab (135 MINUTES)**
* **AFTERNOON BREAK -** (15 MINUTES)
* **Session: AI CERTIFICATION PREP: Attacks, Threats, and Vulnerabilities - (75mins)** (Objective 2.5)
* **Phishing and Evil Twins – (20 MINUTES)**
* **Identify phishing tactics**
  + Spear-phishing, whaling, and vishing recognition
  + Identify scenarios where phishing tactics are used
* **Recognize evil twin Wi-Fi attacks**
  + Identifying rogue access points
  + Preventing credential theft through evil twin attacks
* **Scenario-based practice**
  + AI-driven scenarios to simulate phishing and evil twin situations
* **Password Attacks – (20 MINUTES)**
* **Recognize various password attacks**
  + Dictionary and brute-force attacks
  + Identifying methods for cracking passwords
* **Securing passwords**
  + Implementing password hashing
  + Using strong password policies and multi-factor authentication (MFA)
* **Scenario-based practice**
  + AI simulations with scenarios about plaintext password interception and securing passwords
* **Threat Types – (15 MINUTES)**
* **Differentiate between external and internal threats**
  + Recognizing external threat actors (e.g., hackers) vs. internal threats (e.g., employees, contractors)
* **Case studies on threats**
  + Supply chain attacks
  + Insider threats
  + Effective security policies for mitigating these threats
* **Prioritizing countermeasures**
  + AI questions will focus on selecting appropriate defensive actions based on the threat actor’s intent and capabilities
* **SQL Injection Attacks – (10 MINUTES)**
* **Recognize SQL injection attempts**
  + Identify SQL injection patterns in user inputs
* **Prevent SQL injection**
  + Using input sanitization and parameterized queries
* **Scenario-based practice**
  + AI-driven questions to help students identify and mitigate SQL injection vulnerabilities
* **Cross-site Scripting (XSS) Attacks – (10 MINUTES)**
* **Prevent XSS attacks**
  + Identify malicious scripts and mitigate them using input validation and output encoding
* **Persistent vs. Non-persistent XSS**
  + Differentiate between persistent and non-persistent XSS attacks
  + Solutions using Content Security Policies (CSP)
* **Scenario-based practice**
  + AI scenarios to simulate XSS prevention methods
* **Session: REFLECTION ACTIVITY: Day 1 Wrap-Up - (15 mins)**
* **Knowledge synthesis exercise** – *(5 MINUTES)*
  + Students reflect on how attacks like phishing or SQL injection impact an organization’s security posture.
  + Discuss how attackers might combine multiple techniques to launch a successful attack.
* **Question forum –** *(5 MINUTES)*
  + Open forum for questions on phishing, password attacks, SQL injection, social engineering, or any other topics discussed during the session.
  + Encourage peer responses when appropriate.
* **Preview of future learning** – *(5 MINUTES)*
  + Brief preview of upcoming cybersecurity topics, focusing on advanced defensive strategies and measures.
  + Students are encouraged to review password security and phishing concepts before the next session.
* **Certification Alignment:**
  + The content directly aligns with the certification objectives for CompTIA A+ Core 2 (Security 2.0).
  + The session covers essential cybersecurity principles, including threat identification, mitigation strategies, and scenario-based troubleshooting, preparing students for practical applications in network security.

**DAY PLAN**

**Day Identifier and Context**

* **Day Number:** Day 04
* **Week Number:** Week 07
* **Day Title:** Mobile & PC Security Essentials
* **Session Duration:** 4 hours
* **Target Certification Domains:** Security 2.0, Software Troubleshooting 3.0

**Next Week Preview:**  
Day 05 will focus on **advanced mobile OS troubleshooting** and explore **security frameworks** and **system hardening**, applying troubleshooting skills to more complex environments and scenarios.

**Certification Domains and Objectives**

* **Primary Domains:** Security 2.0, Software Troubleshooting 3.0
* **Specific Objectives:**
  + **Objective 3.2:** Troubleshoot common mobile OS and application issues
  + **Objective 3.3:** Troubleshoot common mobile OS and application security issues
* **Objective Weightings:** Represent approximately **5%** of the CompTIA A+ Core 2 exam
* **Key Terms:** Phishing, Spear-phishing, SQL Injection, XSS, Password Attacks, Whaling, Vishing, Smishing, Evil Twin, Social Engineering, Malware

**Morning Session Details**

**Session Learning Objectives:**

1. **Mobile OS Troubleshooting:**
   * Diagnose common mobile OS issues across **Android**, **iOS**, and **iPadOS**.
   * Use systematic troubleshooting methodologies to resolve **application-related problems** and device configuration errors.
2. **Mobile Application Troubleshooting:**
   * Identify and resolve **application launch failures**, **installation issues**, and **slow performance** in mobile apps.
   * Apply structured methods to troubleshoot **app crashes**, **update failures**, and **networking problems**.
3. **Mobile Device Performance and Connectivity:**
   * Optimize mobile device **battery life** and **system performance**.
   * Troubleshoot **connectivity challenges** including **Wi-Fi**, **Bluetooth**, and **NFC** issues.

**Session 1: Mobile Application Issues – (75 minutes)**

* **Application Launch Failures:**
  + **Types of Failures:**
    - Immediate crash
    - Freeze on launch
    - Black/white screen
    - Force close dialog
    - Silent failure
  + **Root Causes:**
    - Incompatible OS versions
    - Insufficient resources (low RAM, storage)
    - Corrupted application data (cache issues, damaged files)
  + **Troubleshooting Steps:**
    - **Force stop** the app and restart it.
    - **Clear cache** (Android: Settings > Apps > [App Name] > Storage > Clear Cache).
    - **Reinstall** the application completely if the app fails to launch after initial attempts.
    - **Check for updates** and ensure the app is compatible with the OS version.
* **Application Update and Installation Issues:**
  + **Common Causes:**
    - **Network Issues:** Instability, low bandwidth, VPN interference, cellular data restrictions.
    - **Storage Issues:** Device storage full, insufficient temporary space, system partition full.
    - **Marketplace Account Issues:** Expired payment methods, authentication errors.
  + **Resolution Methods:**
    - Check for **stable network** connection and disable VPN if needed.
    - Ensure **sufficient storage** (clear temporary files, remove unused apps).
    - **Verify account credentials** for app stores (Apple ID/Google Play).
    - **Install via alternative networks** if needed (Wi-Fi vs. mobile data).
* **Slow Application Response:**
  + **Causes:**
    - Unnecessary background apps consuming excessive resources.
    - Application cache build-up leading to delayed data retrieval.
    - Poor device performance (lack of RAM, outdated OS).
  + **Optimization Techniques:**
    - **Clear app cache** and reset application preferences if needed.
    - **Limit background apps** and use "Battery Saver" modes.
    - Ensure **system and app updates** are installed.
    - Enable **Adaptive Brightness** and **shorten screen timeout** settings for power efficiency.
* **Activity:** **Mobile Application Troubleshooting Decision Tree – (30 minutes)**
  + **Objective:**
    - Develop a logical decision tree for resolving common mobile app issues like app failure to launch or crash.
    - Identify root causes by systematically following a structured flowchart.

**Morning Break – (15 minutes)**

**Session 2: Device Performance and Connectivity – (90 minutes)**

* **Battery Life Issues:**
  + **Diagnosis:**
    - Check battery consumption via **settings menu** (Android: Battery Usage, iOS: Battery).
    - Identify apps with **high power usage** and background consumption.
    - Understand hardware vs. software battery drain (software issues often occur after OS update).
  + **Optimization Steps:**
    - Use **Battery Saver Mode** and **force stop** background apps that are not in use.
    - **Lower screen brightness** and enable **dark mode** for OLED screens.
    - **Disable non-essential services** like location, Bluetooth, or Wi-Fi when not needed.
* **Random Reboots and System Instability:**
  + **Common Causes:**
    - Software conflicts, insufficient resources, thermal shutdowns, system corruption.
  + **Systematic Troubleshooting:**
    - **Check system logs** (Samsung: \*#9900#), identify repeating error patterns.
    - **Safe mode testing** to isolate third-party app conflicts.
    - **Check thermal performance** and avoid using device while charging if overheating.
    - **Factory reset** as a last resort after data backup if instability persists.
* **Connectivity Issues (Wi-Fi, Bluetooth, NFC):**
  + **Wi-Fi Troubleshooting:**
    - Diagnose **authentication failures**, **signal issues**, and **IP conflicts**.
    - Steps: Forget network and reconnect, check router settings, ensure device is on the correct frequency band (2.4GHz vs. 5GHz).
  + **Bluetooth Troubleshooting:**
    - Pairing failures, connection dropouts, and device incompatibility.
    - Steps: Ensure both devices are in **pairing mode**, check **Bluetooth version compatibility**, restart **Bluetooth** on both devices.
  + **NFC Troubleshooting:**
    - Issues with **detection** or **communication** when trying to use NFC tags or payment systems.
    - Steps: Enable **NFC** in device settings, check for device interference (thick cases, faulty NFC chips).
* **Activity:** **Device Performance and Connectivity Troubleshooting Flowchart – (20 minutes)**
  + **Objective:**
    - Create a troubleshooting decision tree for battery drain, Wi-Fi drops, and Bluetooth connection failures.
    - Use the flowchart to develop a systematic process for resolving connectivity issues on mobile devices.

**Session 3: PC Security Troubleshooting – (60 minutes)**

* **PC Security Issue Indicators and Symptoms:**
  + Identify **unauthorized applications**, **malware behavior**, and **unusual network traffic** that could indicate a security breach.
  + Use **system logs** and **task manager** tools to identify suspicious processes.
* **Account Access and Permission Management:**
  + Implement **user permissions** to secure **workstations** and minimize security risks.
  + Apply **principle of least privilege** to ensure users have only necessary access rights.
* **Account Policies:**
  + **Login Time Restrictions**: Prevent users from logging in outside of working hours.
  + **Failed Attempt Lockout:** Limit the number of incorrect login attempts and lock accounts temporarily.
  + **Account Expiration:** Set expiration dates for temporary accounts to prevent unauthorized access after a specified period.
* **Managing AutoRun & AutoPlay Settings:**
  + **Security Risks** from automatic execution of potentially harmful files (USB drives, CDs).
  + **Disabling AutoRun** on Windows to prevent automatic malware execution from external media.
* **Activity:** **Account Access and Permission Management – 30 minutes**
  + **Scenario-Based Activity:**
    - Work in groups to solve **permission management** scenarios that include over-privileged users, conflicting permissions, and the risks of enabling guest accounts.

**Afternoon Session Details**

**Labs (135 minutes)**

* **Labs 1: SSL Certificate Binding to Website**
* **Labs 2: Jailbreaking an iPhone**
* **Labs 3: Configuring and Managing User Permissions in Windows**
* **Labs 4: Join a Workstation to a Domain**

**Afternoon Break – (15 minutes)**

**Session: AI Certification Prep: Mobile OS Troubleshooting – (60 minutes)**

* **Mobile OS Issue Identification (20 minutes):**
  + **Scenario Analysis:** Work through scenarios identifying common mobile OS issues and troubleshooting steps.
  + **Key Concepts:** Identify update failures, resource constraints, and OS-level issues.
* **Mobile Application Troubleshooting (20 minutes):**
  + **Application Issue Diagnosis:** Work through scenarios diagnosing app crashes, update issues, and installation failures.
  + **Key Concepts:** Identifying app-level issues and differentiating between application and system problems.
* **Mobile Security Threats (20 minutes):**
  + **Security Compromise Detection:** Learn to recognize signs of security breaches such as unauthorized apps, abnormal resource usage, and suspicious permissions.
  + **Key Concepts:** Security implications of rooting/jailbreaking and handling suspicious apps.

**Session: Reflection Activity: Week 7 Wrap-Up – (30 minutes)**

* **Knowledge Consolidation Exercise (10 minutes):**
  + Participants summarize their critical learnings on mobile OS and application troubleshooting.
* **Discussion Questions (10 minutes):**
  + Discuss the most valuable takeaways and insights from mobile troubleshooting.
* **Common Misconception Clarification (10 minutes):**
  + Address any lingering misconceptions and clarify the distinctions between mobile and desktop troubleshooting.

**Certification Alignment**

* This session directly aligns with the **CompTIA A+ Core 2** objectives:
  + **Objective 3.2:** Troubleshoot common mobile OS and application issues.
  + **Objective 3.3:** Troubleshoot common mobile OS and application security issues.

This material represents **5%** of the total exam content.