5-Day Workshop Plan

Cybersecurity

Day 1: Introduction to Cybersecurity

Session Overview: The first day will focus on providing an understanding of the fundamentals of cybersecurity, including basic concepts, types of cyberattacks, and an introduction to the tools and techniques used in the field.

Schedule:

- **10:00 AM - 10:15 AM: Welcome & Introduction**
- **Overview of the workshop, objectives, and the importance of cybersecurity in today's digital world.**
- **10:15 AM - 11:15 AM: Fundamentals of Cybersecurity**
- **Introduction to key concepts like confidentiality, integrity, availability (CIA), risk management, threat actors, and common types of cyberattacks (phishing, malware, ransomware, DDoS).**
- **11:15 AM - 11:30 AM: Break**
- **11:30 AM - 1:00 PM: Network Security Basics**
- **Understanding network protocols, firewalls, and security measures to protect network infrastructure.**
- **2:00 PM - 2:15 PM: Recap and Q&A**
- **Open session for addressing any questions from participants.**
- **2:15 PM - 3:15 PM: Types of Cyberattacks**
- **Detailed discussion on different types of cyberattacks, including phishing, malware, ransomware, social engineering, and more.**
- **3:15 PM - 3:30 PM: Break**
- **3:30 PM - 5:00 PM: Introduction to Cybersecurity Tools**
- **Overview of basic cybersecurity tools such as antivirus software, firewalls, intrusion detection systems (IDS), and encryption tools.**

sltechhsolutions@gmail.com

91-8341475919

5-Day Workshop Plan

Cybersecurity

Day 2: Ethical Hacking and Penetration Testing

Session Overview: This day will dive into the world of ethical hacking and penetration testing. Participants will learn how security professionals test and assess the vulnerabilities in systems.

Schedule:

- **10:00 AM - 10:15 AM: Recap of Day 1**
- **Review and address any questions from Day 1.**
- **10:15 AM - 11:15 AM: Introduction to Ethical Hacking**
- **Understanding ethical hacking, its importance, and the role of ethical hackers in preventing cyberattacks.**
- **11:15 AM - 11:30 AM: Break**
- **11:30 AM - 1:00 PM: Penetration Testing Phases**
- **Overview of penetration testing phases: planning, scanning, exploitation, post-exploitation, and reporting.**
- **2:00 PM - 2:15 PM: Recap and Q&A**
- **Session for clarifying any doubts and questions from the day.**
- **2:15 PM - 3:15 PM: Hands-on: Reconnaissance and Scanning Tools**
- **Introduction to tools used for reconnaissance (Nmap, Netcat) and vulnerability scanning tools (Nessus, OpenVAS).**
- **3:15 PM - 3:30 PM: Break**
- **3:30 PM - 5:00 PM: Hands-on: Exploiting Vulnerabilities**
- **Practical demonstration of exploiting basic vulnerabilities using Metasploit and other tools.**

sltechhsolutions@gmail.com

91-8341475919

5-Day Workshop Plan

Cybersecurity

Day 3: Web Application Security and Common Vulnerabilities

Session Overview: This day will cover web application security, focusing on common vulnerabilities in web applications and methods for securing them.

Schedule:

- **10:00 AM - 10:15 AM: Recap of Day 2**
- **A quick review of ethical hacking and penetration testing concepts from Day 2.**
- **10:15 AM - 11:15 AM: Web Application Security Overview**
- **Introduction to web application security, OWASP Top 10, and common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).**
- **11:15 AM - 11:30 AM: Break**
- **11:30 AM - 1:00 PM: SQL Injection and XSS Attacks**
- **In-depth explanation of SQL Injection and XSS, how they work, and methods to defend against them.**
- **2:00 PM - 2:15 PM: Recap and Q&A**
- **Clarification of any doubts from the day's sessions.**
- **2:15 PM - 3:15 PM: Securing Web Applications**
- **Best practices for securing web applications, including input validation, secure coding practices, and using security headers.**
- **3:15 PM - 3:30 PM: Break**
- **3:30 PM - 5:00 PM: Hands-on: Testing for Vulnerabilities**
- **Practical session on using tools such as Burp Suite and OWASP ZAP for testing and exploiting common web application vulnerabilities.**

sltechhsolutions@gmail.com

91-8341475919

5-Day Workshop Plan

Cybersecurity

Day 4: Network Security and Defense Strategies

Session Overview: Day 4 will focus on securing network infrastructure by understanding common network security protocols, defense mechanisms, and incident response strategies.

Schedule:

- **10:00 AM - 10:15 AM: Recap of Day 3**
- **Review of web application security concepts from Day 3.**
- **10:15 AM - 11:15 AM: Network Security Protocols**
- **Detailed discussion on security protocols like HTTPS, SSH, IPsec, and VPNs, and their role in securing communications.**
- **11:15 AM - 11:30 AM: Break**
- **11:30 AM - 1:00 PM: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)**
- **Introduction to IDS/IPS, their functions, and how they help detect and prevent cyberattacks.**
- **2:00 PM - 2:15 PM: Recap and Q&A**
- **Time for addressing questions and clearing doubts.**
- **2:15 PM - 3:15 PM: Firewalls and Network Defense Mechanisms**
- **Overview of firewalls, their configuration, and other defense mechanisms like DMZs and access control lists (ACLs).**
- **3:15 PM - 3:30 PM: Break**
- **3:30 PM - 5:00 PM: Hands-on: Configuring Firewalls and IDS/IPS**
- **Practical demonstration of setting up firewalls and IDS/IPS systems to protect network infrastructure.**

sltechhsolutions@gmail.com

91-8341475919

5-Day Workshop Plan

Cybersecurity

Day 5: Incident Response and Cybersecurity Best Practices

Session Overview: The final day will cover the procedures for incident response, best practices for maintaining a secure system, and how organizations can prepare for and respond to cybersecurity incidents.

Schedule:

- **10:00 AM - 10:15 AM: Recap of Day 4**
- **Quick review of network security protocols and IDS/IPS from Day 4.**
- **10:15 AM - 11:15 AM: Incident Response Lifecycle**
- **Introduction to incident response planning, the stages of incident response (detection, containment, eradication, recovery, and lessons learned).**
- **11:15 AM - 11:30 AM: Break**
- **11:30 AM - 1:00 PM: Cybersecurity Best Practices**
- **Learn about key best practices for organizations to follow to secure their systems, including regular patching, user access control, and encryption.**
- **2:00 PM - 2:15 PM: Recap and Q&A**
- **Review the key points from the day's sessions and address questions.**
- **2:15 PM - 3:15 PM: Cybersecurity Tools for Monitoring & Defense**
- **Overview of cybersecurity tools such as SIEM (Security Information and Event Management) and endpoint protection tools.**
- **3:15 PM - 3:30 PM: Break**
- **3:30 PM - 5:00 PM: Hands-on: Incident Response Simulation**
- **Practical session simulating a cybersecurity incident where participants will apply incident response techniques.**

sltechhsolutions@gmail.com

91-8341475919