3-Month Internship Program

(12 Weeks): Cybersecurity Training

Week 1: Introduction to Cybersecurity

- **Topics:**
  - **Fundamentals of cybersecurity: CIA triad (Confidentiality, Integrity, Availability).**
  - **Types of cyber threats and attacks (malware, phishing, DDoS).**
  - **Overview of cybersecurity tools and career paths.**
- **Assignment:**
  - **Research and present case studies of recent cyberattacks.**

Week 2: Networking Basics for Cybersecurity

- **Topics:**
  - **OSI and TCP/IP models.**
  - **Common network protocols (HTTP, HTTPS, FTP, DNS, etc.).**
  - **Basics of firewalls, VPNs, and proxies.**
- **Assignment:**
  - **Set up and secure a small network environment.**

Week 3: Operating Systems and Command-Line Tools

- **Topics:**
  - **Fundamentals of Linux and Windows operating systems.**
  - **Command-line tools for cybersecurity (netstat, ping, traceroute, etc.).**
  - **Introduction to PowerShell and Bash scripting.**
- **Assignment:**
  - **Use command-line tools to monitor and analyze network traffic.**

Week 4: Introduction to Cryptography

- **Topics:**
  - **Basics of encryption and decryption.**
  - **Symmetric vs. asymmetric encryption (AES, RSA).**
  - **Hashing algorithms (MD5, SHA family).**
- **Assignment:**
  - **Implement encryption and decryption for secure file sharing.**

Week 5: Vulnerability Assessment

- **Topics:**
  - **Identifying vulnerabilities in systems and networks.**
  - **Common vulnerabilities: OWASP Top 10.**
  - **Introduction to vulnerability scanning tools (Nessus, OpenVAS).**
- **Assignment:**
  - **Perform a basic vulnerability scan and create a report.**

Week 6: Penetration Testing Basics

- **Topics:**
  - **Fundamentals of penetration testing: Planning, execution, and reporting.**
  - **Ethical hacking and legal considerations.**
  - **Tools for penetration testing: Metasploit, Nmap, and Burp Suite.**
- **Assignment:**
  - **Conduct a simulated penetration test on a controlled environment.**

Week 7: Web Application Security

- **Topics:**
  - **Common web application vulnerabilities (SQL injection, XSS, CSRF).**
  - **Securing web applications against attacks.**
  - **Testing tools for web security (OWASP ZAP, Burp Suite).**
- **Assignment:**
  - **Identify and mitigate vulnerabilities in a sample web application.**

Week 8: Malware Analysis

- **Topics:**
  - **Basics of malware analysis: Types and behaviors of malware.**
  - **Static vs. dynamic analysis techniques.**
  - **Tools for malware analysis (IDA Pro, Wireshark).**
- **Assignment:**
  - **Analyze and document the behavior of a malware sample in a sandbox environment.**

Week 9: Incident Response and Forensics

- **Topics:**
  - **Steps in the incident response lifecycle.**
  - **Collecting and analyzing digital evidence.**
  - **Tools for digital forensics (Autopsy, FTK Imager).**
- **Assignment:**
  - **Simulate an incident response and prepare a detailed report.**

Week 10: Security Policies and Compliance

- **Topics:**
  - **Developing security policies and best practices.**
  - **Understanding compliance standards (ISO 27001, GDPR, HIPAA).**
  - **Risk management and mitigation strategies.**
- **Assignment:**
  - **Create a basic security policy document for an organization.**

Week 11: Security Tools and Automation

- **Topics:**
  - **Introduction to SIEM tools (Splunk, ELK Stack).**
  - **Automating security tasks with Python.**
  - **Monitoring and responding to threats in real time.**
- **Assignment:**
  - **Develop a Python script for automating a security task (e.g., log monitoring).**

Week 12: Final Project

- **Topics:**
  - **Integration of all learned concepts into a real-world scenario.**
  - **Guidance and mentorship for project implementation.**
- **Assignment:**
  - **Build a comprehensive cybersecurity project (e.g., intrusion detection system,**
  - **secure web application) and prepare a final presentation.**

sltechhsolutions@gmail.com

91-8341475919