CYBERSECURITY INTERNSHIP

Introducing: Your Gateway to a Thriving Cybersecurity Career!

Embark on an immersive journey into the dynamic realm of Cybersecurity through our hands-on internship program designed specifically for beginners. Dive deep into transformative learning experiences that prioritize practical application and experiential learning.

Learn by case study, learn by projects, get experience learning. Welcome!

PARTNERS

CompTIA Authorized Partner | DELIVERY PARTNER

Networking cisco. Academy

aws training and certification

CLACACHI TECHNOLOGY LTD

PROJECTS

In this internship program we will be having about 4 Core Projects aside the over 200 Labs , this is to aid you become a better Cybersecurity analyst that doesn't just understand security concepts but can build, develop and advice team members and stakeholders on appropriate steps to aid a better security posture for any enterprise.

The following projects will be considered during the internship

1. Vulnerability Research, Fix and PenTest/Fix Report

Do you know that you have quiet a lot of vulnerable web applications all over the internet, these projects seeks to explore the bug bounty approach to searching out for vulnerable applications, proposing for fix and also doing same for interested stakeholder/project owners.
(This will be focused on web projects built by students and from sourced projects)

2. Python Scripts,PHP Scripts for Web, OSINT, Network Scanning

The goal here is to learn basic PHP and Python and see how to use it to create basic scripts adapted to Cybersecurity needs in Open source intelligence gathering, Network Scanning

1. URL Shorten Script
2. Inventory System/Cyber Incidence Report Alert System
3. Cybersecurity Analyst Appointment
4. Security Scanner Plugin-WordPress, PHP Applications
5. Use CVE API to create a web vulnerability assessment scanner- IP and URLs
6. Malware Analysis Sandbox
7. Mini Encryption Software based on choice algorithms
8. Web-Based Facial Authentication System
9. Network Log monitor and SIEM tool(Network Scanner)
10. Website Scraper - Google Map or any API or links
11. IP Tracker, WhoisTracker - RestAPI JS Project

3. Peer Review/Support/Analyst Role- Record Sheet for Tracking

Learning in a collaborative environment fosters growth, health competition and motivation for success, students are peered in group to help them better collaborate in small units taking turns to lead, support and assist their groups in presentation. These are skills needed in any workplace or in a consulting,freelance role (3 peer groups are **CyberPunk**, **Techie**, **Geeky**- each student will be added to one of the group during the course of the program)

4. NIST Framework for INCIDENCE Response Service for Interns

This will be peered to the project type 1 where the NIST framework will be adapted for incidence response.

HANDS-ON LABS

NETWORKING FOR CYBERSECUITY ANALYSTS

1Lab - Install Windows and security Features
2Lab - Install Third-Party Software in Windows -
3Lab - Install Wireshark - Configuration and Set up
4Lab - Use Wireshark to View Network Traffic -
5Lab - View Wired and Wireless NIC Information -
6Lab - Configure a Wireless Network -
7Lab - Configure Firewall Settings -
8Lab - Use Wireshark to Examine Ethernet Frames -
9 Lab - View Network Device MAC Addresses -
10 Lab - Research Laptop Screens -
11 Lab - Research Laptop Batteries -
12 Lab - Research Laptop Drives -
13Lab - View the Switch MAC Address Table -
14Lab - Install a Printer in Windows -
15 Lab - Share a Printer in Windows -
16 Lab - Install Linux in a Virtual Machine and Explore the GUI -
17 Lab - User Accounts -
18 Lab - Permissions -
19 Lab - Monitor and Manage System Resources -
20 Lab - Install Third-Party Software -
21 Lab - Work in the Windows Command Shell -
22 Lab - File System Commands -
23 Lab - Disk CLI Commands -
24 Lab - Task and System CLI Commands -
25 Lab - Share Resources -
26 Lab - Windows Remote Desktop and Assistance -
27 Lab - System Restore and Hard Drive Backup -
28 Lab - Troubleshoot Operating System Problems -
29 Lab - Operating System Security -
30 Lab - Bitlocker and Bitlocker To Go -
31 Lab - Use Ping and Traceroute to Test Network Connectivity -
32 Lab - Configure Windows Firewall -
33 Lab - Document Customer Information in a Work Order -
34 Lab - Investigate Breaches of PII PHI PCI -
35 Lab - Remote Technician - Fix a Hardware Problem -
36 Lab - Remote Technician - Fix an Operating System Problem -
37 Lab - Remote Technician - Fix a Network Problem -
38 Lab - Remote Technician - Fix a Security Problem -
39 Lab - Research Network Security Threats -
40 Lab - Design and Build a Small Network -

CISCO CYBEROPS

1 Class Activity - Top Hacker Shows Us How It is Done -
2 Lab - Installing the Virtual Machines -
3 Lab - Cybersecurity Case Studies -
4 Lab - Learning the Details of Attacks -
5 Lab - Visualizing the Black Hats -
6 Lab - Becoming a Defender -
7 Class Activity - Identify Running Processes -
8 Lab - Exploring Processes, Threads, Handles, and Windows Registry -
9 Lab - Create User Accounts -
10 Lab - Using Windows PowerShell -

11 Lab - Windows Task Manager -
12 Lab - Monitor and Manage System Resources in Windows -
13 Lab - Working with Text Files in the CLI -
14 Lab - Getting Familiar with the Linux Shell -
15 Lab - Linux Servers -
16 Lab - Navigating the Linux Filesystem and Permission Settings -
17 Lab - Tracing a Route -
18 Lab - Introduction to Wireshark -
19 Lab - Using Wireshark to Examine Ethernet Frames -
20 Lab - Using Wireshark to Observe the TCP 3-Way Handshake -
21 Lab - Exploring Nmap -
22 Lab - Using Wireshark to Examine a UDP DNS Capture -
23 Lab - Using Wireshark to Examine TCP and UDP Captures -
24 Lab - Using Wireshark to Examine HTTP and HTTPS Traffic -
25 Lab - Anatomy of Malware -
26 Lab - Social Engineering -
27 Class Activity - What's Going On -
28 Lab - Exploring DNS Traffic -
29 Lab - Attacking a mySQL Database -
30 Lab - Reading Server Logs -
31 Class Activity - Creating Codes -
32 Lab - Hashing Things Out -
33 Lab - Encrypting and Decrypting Data Using OpenSSL -
34 Lab - Encrypting and Decrypting Data Using a Hacker Tool -
35 Lab - Examining Telnet and SSH in Wireshark -
36 Lab - Certificate Authority Stores -
37 Lab - Snort and Firewall Rules -
38 Lab - Convert Data into a Universal Format -
39 Lab - Regular Expression Tutorial -
40 Lab - Extract an Executable from a PCAP -
41 Lab - Interpret HTTP and DNS Data to Isolate Threat Actor -
42 Lab - Isolate Compromised Host Using 5-Tuple -
43 Lab - Investigating a Malware Exploit -
44 Lab - Investigating an Attack on a Windows Host -
45 Lab - Incident Handling

WEB PROGRAMMING FOR SECURITY ANALYSTS

Lab 1- Introduction to HTML - Secure HTML Structure
Lab 2-Styling with CSS - CSS Security Implementation
Lab 3 -Responsive Design with Bootstrap - Security Considerations
Lab 4-PHP Basics - PHP Security Foundations
Lab 5- Server-Side Scripting with PHP - Secure Form Handling
Lab 6- Python Basics for security script writing via AI tools
Lab 7- Python for Cybersecurity - Scripting Secure File Operations
Lab 8- MySQL Database Basics - Secure Database Configuration
Lab 9- Integrating MySQL with PHP - Safe Database Connectivity
Lab 10- Input Validation and Sanitization - Robust Input Handling
Lab 11 Session Management and Authentication - Secure Authentication Implementation
Lab 12- Secure Data Storage - Encryption and Protection
Lab 13-Python for Cybersecurity - Network Security Scripting
Lab 14- Setting up AWS-GCP Account - Cloud Security Fundamentals
Lab 15- Deploying Web Applications to AWS-GCP - Secure Cloud Deployment
Lab 16- Network Security-File Security on Cloud Platforms - Access Control Strategies
Lab 18 CDN-Web Application Firewall (WAF) - WAF Configuration and Testing
Lab 19 Continuous Monitoring and Security Audits - Ongoing Security Assessments and Vulnerability Assessement
Lab 20- Capstone Project - Comprehensive Web Security Integration- Vulnerability and PenTest

DITIGAL FORENSICS, THREAT MANAGEMENT AND INCIDENCE RESPONSE

Lab 1 - Attack Analysis
Lab 2 - Create Your Personal Code of Ethical Conduct
Lab 3- Develop Cybersecurity Policies and Procedures
Lab 4- Evaluate Cybersecurity Reports
Lab 5 - Evaluate Vulnerabilities
Lab 6- Identify Relevant Threat Intelligence
Lab 7- Incident Handling
Lab 8- Recommend Disaster Recovery Measures
Lab 9- Recommend Security Measures to Meet Compliance Requirements
Lab 10- Risk Analysis
Lab 11- Introduction to Digital Forensics
Lab 12 Pestudio - Malware Analysis
Lab 13- Autopsy - Digital Forensics Platform
Lab 14- FTKImager - Disk Imaging and Analysis
Lab 15 Sucuri - Website Security Analysis
Lab 16- Risk Management
Lab 17 PasswordSaveInvestigation - Password Analysis
Lab 18-Maltego - Threat Intelligence
Lab 19 Exploring CVEs - Vulnerability Analysis
Lab 20 Comprehensive Digital Forensics Case Study
Lab 21 Advanced Pestudio Malware Analysis
Lab 22- Autopsy File Carving and Recovery
Lab 23 FTKImager Advanced Disk Analysis
Lab 24 Sucuri - Web Malware Removal
Lab 25 Capstone - Integrated Digital Forensics and OSINT Investigation
Lab 26- Security Controls Implementation
Lab 27- Use Wireshark to Compare Telnet and SSH Traffic
Lab 28 Investigate Disaster Recovery

CompTIA PEN TEST+

Lab 1 Embracing the Hackers Mindset
Lab 2- Applying the Cyber Kill Chain
Lab 3- Manual OSINT Techniques
Lab 4- Exploring Shodan for Reconnaissance
Lab 5- Network Enumeration and Scanning with Nmap
Lab 6- Installation and Operation of Vulnerability Scanners
Lab 7- Creating a PenTest Vulnerability Scanning Plan
Lab 8- Interpreting Vulnerability Scan Results
Lab 9- Developing a Penetration Testing Plan
Lab 10- Exploitation in Penetration Testing
Lab 11- Discovery Techniques
Lab 12- Pivoting in Penetration Testing
Lab 13- Hash Capture and Analysis
Lab 14- Brute-Forcing Services
Lab 15- Wireless Network Penetration Testing
Lab 16- Designing Physical Penetration Testing Scenarios
Lab 17- Using BeEF for Browser Exploitation
Lab 18- Application Security Testing Techniques
Lab 19- Utilizing ZAP Proxy for Web Application Security
Lab 20- Creating a Cross-Site Scripting (XSS) Vulnerability
Lab 21- SAM Dumping and Credential Cracking
Lab 22- Password Cracking Using Hashcat
Lab 23- Setting up Reverse and Bind Shells

Lab 24- Pentesting Remediation Strategies
Lab 25- Penetration Testing Report Writing
Lab 26- Reverse DNS Lookup for Reconnaissance
Lab 27- Network Traffic Analysis with Wireshark
Lab 28- Social Engineering Techniques- Pentesting Techniques
Lab 29- Advanced Persistent Threat Simulation
Lab 30- Cyber Threat Hunting and Incident Response for Web Applications

ETHICAL HACKER LABS

1. Deploy_a_Pre-Built_Kali_Linux_Virtual_Machine_(VM)
2. Investigate_Kali_Linux
3. Analyze_Exploit_Code
4. Analyze_Automation_Code
5. Compliance_Requirement_and_Local_Restrictions
6. Create_a_Pentesting_Agreement+
7. Pre-Engagement_Scope_and_Planning
8. Personal_Code_of_Conduct
9. Employee_Intelligence_Gathering
10. Finding_Information_from_SSL_Certificates
11. Finding_Out_About_the_Organization
12. Advanced_Searches
13. Using_OSINT_Tools
14. Network_Sniffing_with_Wireshark
15. Enumeration_with_Nmap
16. Packet_Crafting_with_Scapy
17. Vulnerability_Scanning_with-Kali_Tools
18. Investigate_Vulnerability_Information_Sources
19. Using_the_Browser_Exploitation_Framework_(BeEF)
20. Explore_the_Social_Engineer_Toolkit_(SET)
21. Using_the_Browser_Exploitation_Framework_(BeEF)
22. On-Path_Attacks_with_Ettercap
23. Scanning_for_SMB_Vulnerabilities_with_enum4linux
24. Web_Vulnerability_Scanning
25. Using_the_GVM_Vulnerability_Scanner
26. Use_the_OWASP_Web_Security_Testing_Guide
27. Injection_Attacks
28. Using_Password_Tools
29. Cross_Site_Scripting_
30. Explore_PenTest_Reports
31. Recommend_Remediation_Based_on_Findings

HAPPY LEARNING!!!