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!

CompTIA Authorized Partner DELIVERY PARTNER

Cisco Networking Academy

aws training and certification

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

Lab 1- Introduction to Digital Forensics
Lab 2 Pestudio - Malware Analysis
Lab 3- Autopsy - Digital Forensics Platform
Lab 4- FTKImager - Disk Imaging and Analysis
Lab 5 Sucuri - Website Security Analysis
Lab 7 PasswordSaveInvestigation - Password Analysis
Lab 8-Maltego - Threat Intelligence
Lab 9 Exploring CVEs - Vulnerability Analysis
Lab 10 Comprehensive Digital Forensics Case Study
Lab 11 Advanced Pestudio Malware Analysis
Lab 12- Autopsy File Carving and Recovery
Lab 13 FTKImager Advanced Disk Analysis
Lab 14 Sucuri - Web Malware Removal
Lab 15 Capstone - Integrated Digital Forensics and OSINT Investigation

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