QUICKSTART
Over 35 Years Of Technology Training

Cybersecurity Immersive Bootcamp

Complete Outline

About

Program Length:

24 Weeks

Instruction Format:

Mentor-led cohorts (online)

Program Overview:

The Cybersecurity Professional bootcamp is an immersive and accelerated training program with a focus on creating the next generation of cyber security professionals. You will attend courses, do hands on labs and apply your learning to successfully complete projects that address different cyber security topics. Throughout the program you will interact with experts who will guide you through the bootcamp, answer questions, and help with labs and project. The bootcamp will end with few capstone projects where you will apply your learnings to real life cyber security hallenges. This is a 6 months program and students are expected to spend 15 to 25 hours a week to master the material. Graduates of this program will learn critical skills for different cyber security careers and will have access to career services throughout the program.

Certifications Covered:

This bootcamp will cover the material needed for following certification:

- CompTIA ITF+
- CompTIA Network+
- CompTIA Security+
- CompTIA CySA+
- Certified Ethical Hacking
- CompTIA Pentest+

Learning Outcomes:

- **Computer/ Systems Fundamentals**
  - Hardware architecture
  - Operating Systems (windows, linux, CISCO)
  - Troubleshooting

- **Networking**
  - Network Management/ Troubleshooting
  - WAN
  - Virtualization Techniques
  - TCP/IP
  - Scanning / Sniffing (Wireshark Nmap, Etc.)
  - And More

- **Cyber Security**
  - System/Network Security
  - Security Threats (Social Engineering, Malware)
  - Vulnerability Assessment
  - Identity and Assess Management
  - Cryptography
  - And More

- **Security Analyst**
  - Managing And Remediating Vulnerabilities
  - Security and Software Development
  - Incidence Response
  - Forensic Tools
  - Cloud Security tools
  - And More

- **Penetration Testing**
  - OS Vulnerabilities Exploitation
  - Multi-level Pivoting
  - SQL Injection
  - Host-Based Application Exploits
  - XSFR
  - And More

- **Ethical Hacking**
  - Footprinting
  - Reconnaissance
  - Networks Scanning
  - Enumeration
  - Session Hijacking
  - Hacking Web Applications
  - loT Hacking
  - And More

- **Scripting**

- Python
- Hacking
- Automation
- Tooling
- Shell Scripting
- Data Analysis
-

Study Plan	Name
Week 1 & 2	Insight by Industry Leaders
	CompTIA ITF Fundamentals (ITF+)
Week 3 & 4	Networking Fundamentals (CompTIA Network+)
	Networking Fundamentals Assessment
Week 5-7	Security Fundamentals (CompTIA Security+)
	Security Fundamentals Assessment
Week 8 & 9	Information Security Bootcamp: Project A
Week 10 & 11	Python Programming Fundamentals
	Python Fundamentals Assessment
Week 12	Security Bootcamp: Project B
Week 12-16	Certified Ethical Hacking (CEHv11)
	Ethical Hacking Assessment
Week 17-19	Information Security Bootcamp: Project C (EH)
Week 20-22	CompTIA CySA+ Cybersecurity Analyst (CS0-002)
	Cybersecurity Analysis Assessment
Week 23 & 24	Information Security BootCamp: Final Capstone Project - CYSA+
Week 20-22	CompTIA Pentest+
	Penetration Testing Assessment
Week 23 & 24	Information Security BootCamp: Final Capstone Project - PENTEST+
	Time to Dive In! QuickStart - Provided Resources to Help You Get Hired

Courses & Modules

1. **Insight by Industry Leaders**

2. **CompTIA ITF Fundamentals**

- Module 1: Common Computing Devices
- Using a Workstation
- Using an OS
- Managing an OS
- Troubleshooting and Support
- Module 2: Using Apps and Databases
- Using Data Types and Units
- Using Apps
- Programming and App Development
- Using Databases
- Module 3: Using Computer Hardware
- Using Device Interfaces
- Using Peripheral Devices
- Using Storage Devices
- Using File Systems
- Module 4: Using Networks
- Networking Concepts
- Connecting to a Network
- Secure Web Browsing
- Using Shared Storage
- Using Mobile Devices
- Module 5: Security Concepts
- Security Concerns
- Using Best Practices
- Using Access Controls
- Behavioral Security Concepts
- Module 6: Infrastructure
- Cloud Fundamentals
- Waterfall vs. AgileDevOps

3. **Networking Fundamentals (CompTIA Network+)**

- Course Introduction
- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture
- Final Exam

4. **Networking Fundamentals Assessment**

5. **Security Fundamentals (CompTIA Security+)**

- Course Introduction
- Lesson 1: Comparing Security Roles and Security Controls
- Lesson 2: Explaining Threat Actors and Threat Intelligence
- Lesson 3: Performing Security Assessments
- Lesson 4: Identifying Social Engineering and Malware
- Lesson 5: Summarizing Basic Cryptographic Concepts
- Lesson 6: Implementing Public Key Infrastructure
- Lesson 7: Implementing Authentication Controls
- Lesson 8: Implementing Identity and Account Management Controls
- Lesson 9: Implementing Secure Network Designs
- Lesson 10: Implementing Network Security Appliances
- Lesson 11: Implementing Secure Network Protocols

- Lesson 12: Implementing Host Security Solutions
- Lesson 13: Implementing Secure Mobile Solutions
- Lesson 14: Summarizing Secure Application Concepts
- Lesson 15: Implementing Secure Cloud Solutions
- Lesson 16: Explaining Data Privacy and Protection Concepts
- Lesson 17: Performing Incident Response
- Lesson 18: Explaining Digital Forensics
- Lesson 19: Summarizing Risk Management Concepts
- Lesson 20: Implementing Cybersecurity Resilience
- Lesson 21: Explaining Physical Security
- Course Summary

6. Security Fundamentals Assessment

7. Information Security Bootcamp: Project A

8. Python Programming Fundamentals

- Course Introduction
- Module 1: Introduction to Python
- Module 2: Language Fundamentals
- Module 3: Functions
- Module 4: Exception Handling
- Module 5: Data Structures
- Module 6: Object Oriented Programming
- Module 7: Interacting with Files and Directories
- Module 8: Module and Packages
- Course Summary

9. Python Fundamentals Assessment

10. Security Bootcamp: Project B

11. Certified Ethical Hacking (CEHv11)

- Course Introduction
- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection
- Module 16: Hacking Wireless Networks
- Module 17: Hacking Mobile Platforms
- Module 18: IoT and OT Hacking
- Module 19: Cloud Computing
- Module 20: Cryptography
- Course Summary
- Final Exam

12. **Ethical Hacking Assessment**

13. **Information Security Bootcamp: Project C (EH)**

14. **CompTIA CySA+ Cybersecurity Analyst (CS0-002)**

- Course Introduction
- Lesson 1: Explaining the Importance of Security Controls and Security Intelligence
- Lesson 2: Utilizing Threat Data and Intelligence
- Lesson 3: Analyzing Security Monitoring Data
- Lesson 4: Collecting and Querying Security Monitoring Data
- Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques
- Lesson 6: Applying Incident Response Procedures
- Lesson 7: Applying Risk Mitigation and Security Frameworks
- Lesson 8: Performing Vulnerability Management
- Lesson 9: Applying Security Solutions for Infrastructure Management
- Lesson 10: Understanding Data Privacy and Protection
- Lesson 11: Applying Security Solutions for Software Assurance
- Lesson 12: Applying Security Solutions for Cloud and Automation
- Course Summary

15. **Cybersecurity Analysis Assessment**

16. **Information Security BootCamp: Final Capstone Project - CYSA+**

17. **CompTIA Pentest+**

- Course Introduction
- Lesson 1: Scoping Organizational/Customer Requirements
- Lesson 2: Defining the Rules of Engagement
- Lesson 3: Footprinting and Gathering Intelligence
- Lesson 4: Evaluating Human and Physical Vulnerabilities
- Lesson 5: Preparing the Vulnerability Scan
- Lesson 6: Scanning Logical Vulnerabilities
- Lesson 7: Analyzing Scanning Results
- Lesson 8: Avoiding Detection and Covering Tracks
- Lesson 9: Exploiting the LAN and Cloud
- Lesson 10: Testing Wireless Networks
- Lesson 11: Targeting Mobile Devices
- Lesson 12: Attacking Specialized Systems
- Lesson 13: Web Application-Based Attacks
- Lesson 14: Performing System Hacking
- Lesson 15: Scripting and Software Development
- Lesson 16: Leveraging the Attack: Pivot and Penetrate
- Lesson 17: Communicating During the PenTesting Process
- Lesson 18: Summarizing Report Components
- Lesson 19: Recommending Remediation
- Lesson 20: Performing Post-Report Delivery Activities

- Final Exam

18. Penetration Testing Assessment

19. Information Security BootCamp: Final Capstone Project - PENTEST+

20. Time to Dive In! QuickStart - Provided Resources to Help You Get Hired

- Lesson 1: Automating your Job Search: Huntr Edition
- Lesson 2: Huntr Tutorial: How to Use your Board
- Lesson 3: Huntr Tutorial: Goal Setting/Our Expectations of You
- Lesson 4: Länch, Powered by Pepelwerk
- Summary and Key Points