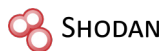# Cybersecurity Bootcamp

Fullstack Academy

Full-Time & Part-Time Syllabus

Prepare for a Cybersecurity Career in 13-21 Weeks:

Cybersecurity Essentials + Generative AI

Gain the essential skills you need to succeed in today's tech industry and stay ahead of future innovations.

Windows   ChatGPT   Linux   splunk>

metasploit   NMAP   WIRESHARK   Nessus

SHODAN   OWASP   NJ   B

crunch   ...and many more

CompTIA Authorized Partner | DELIVERY PARTNER

Exam preparation and voucher included.

APPLY NOW

Why Choose Fullstack Academy?

Learn to Apply Generative AI in Cybersecurity

Discover the cutting-edge applications of Generative AI in cybersecurity.

Dedicated Module & Exam Voucher for CompTIA Security+ Exam Preparation

As a CompTIA Authorized Delivery Partner, Fullstack Academy will prepare you for the CompTIA Security+ certification and provide an exam voucher at no extra cost.

Beginner-Friendly: Get Cybersecurity Career-Ready

Even without prior tech experience, our program will equip you with the skills to start a rewarding career in the high-demand field of cybersecurity.

Earn a Certificate of Completion

Upon bootcamp graduation, you'll earn a Fullstack Academy Certificate of Completion, validating your industry-ready skills.

Build a Solid Foundation in Core Cybersecurity Principles

Master the essentials of networking, governance, risk & compliance, cloud security, cyber threat intelligence, and cryptography principles—the bedrock of all cybersecurity expertise.

Get 1:1 Personalized Career Coaching and Job-Search Support

Receive tailored career coaching and job search support to help you secure a tech role.

Become a Well-Rounded Cybersecurity Professional

Become a versatile cybersecurity professional with skills in both offensive (Red Team) and defensive (Blue Team) cybersecurity.

Join a Powerful Alumni Network

Gain access to a vast network of 10,000+ supportive Fullstack Academy alumni who can help open doors to job opportunities.

Fullstack Academy Grads Get Hired

Throughout the bootcamp and beyond, the Fullstack Academy team is committed to helping you land the ideal tech role for you.

Proven Employment Outcomes

1,500+ companies across the U.S. have hired our grads—everywhere from large tech firms to mid-size companies and innovative start-ups.

Professional Career Coaching

Fullstack Academy grads have the competitive advantage of career coaching and practical experience to land a meaningful role.

A Built-In Network

You'll join our expansive network of alums—building lasting connections to support you throughout your career.

Perks of a Part-Time Bootcamp:

Learn at a balanced pace.

Maintain your job and other commitments.

Get the same immersive curriculum, covering in-demand tools and technologies, as our full-time program, with the added work-life balance of our part-time option.

Perks of a Full-Time Bootcamp:

Accelerate your skill development for expedited entry into the job market.

Explore the same comprehensive curriculum as the part-time option, but in a full-time format.

The Fullstack Academy Difference

Founded in 2012, Fullstack Academy is a pioneering and top-rated bootcamp provider that has helped over 10,000 graduates to launch or accelerate their careers in tech.

Fullstack Inclusion

Fullstack can help make your career goals possible, no matter your background. We're committed to providing a welcoming, diverse, and flexible learning environment.
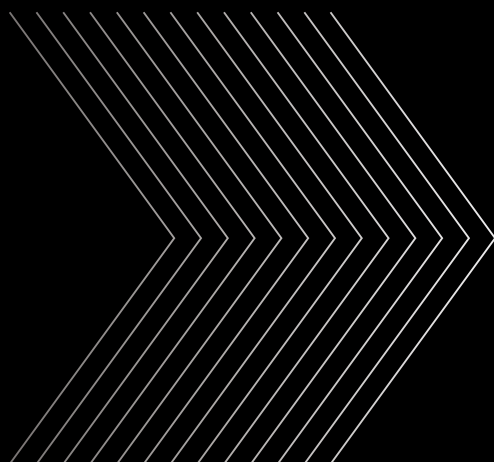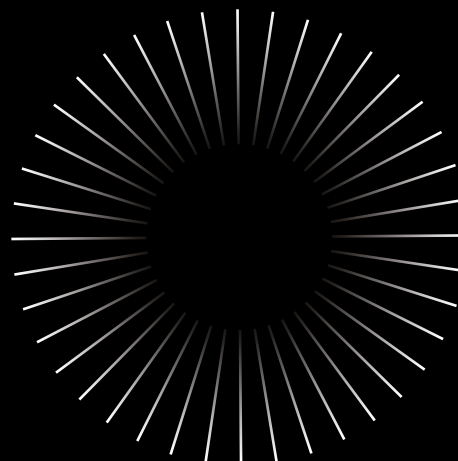
Fullstack Experience

Fullstack's rigorous curriculum focuses on the skills top-tier tech employers are seeking. Guided by passionate instructors and a caring career success team to assist with everything from interview prep to salary negotiations, you'll gain the confidence you need to build a fulfilling career.

Fullstack Outcomes

We're obsessed with helping our students succeed, and it shows: 1,500+ companies across the U.S. have hired our graduates—including notable companies like Google, Amazon, LinkedIn, Bloomberg, Spotify, and Etsy.
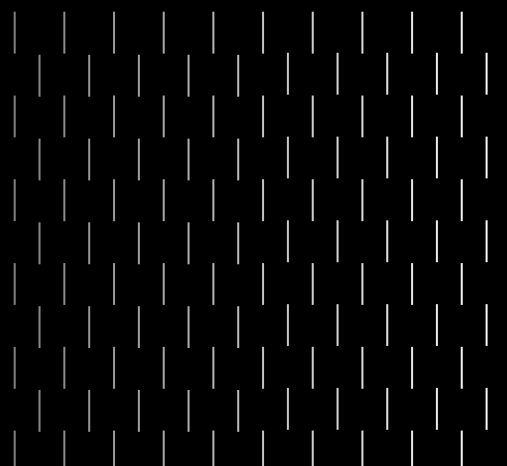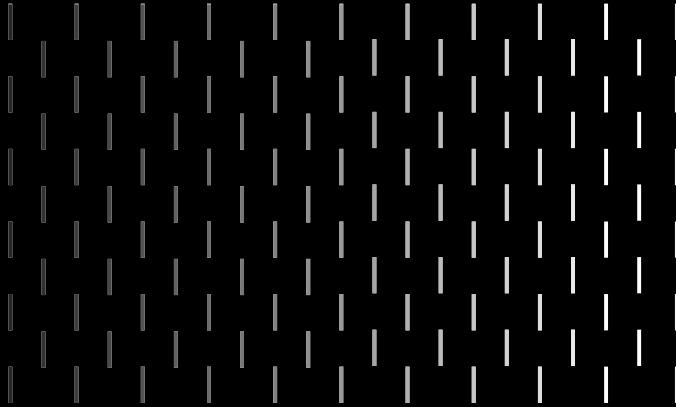
Curriculum Concepts

Fullstack Academy
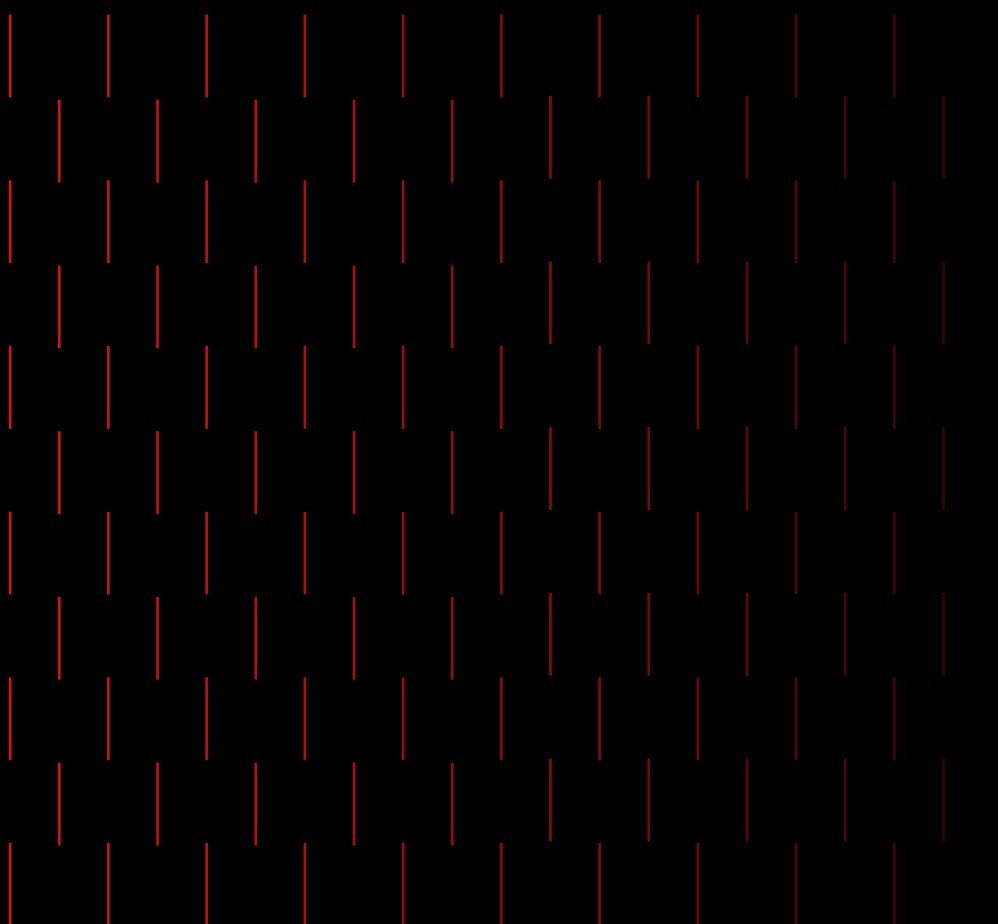
Unit 1
Operating Systems and Networking Essentials

Lay the groundwork for your cybersecurity journey. This unit introduces essential operating system (OS) concepts (Windows and Linux), fundamental networking principles, and an overview of cryptography and wireless security.

Key Learning Objectives

◆ Understand OS architecture

◆ Apply file system management techniques in Windows

◆ Demonstrate user and group account management

◆ Compare various network topologies

◆ List the layers and functions of the TCP/IP and OSI models

◆ Improve network efficiency and reliability

◆ Describe Public Key Infrastructure components

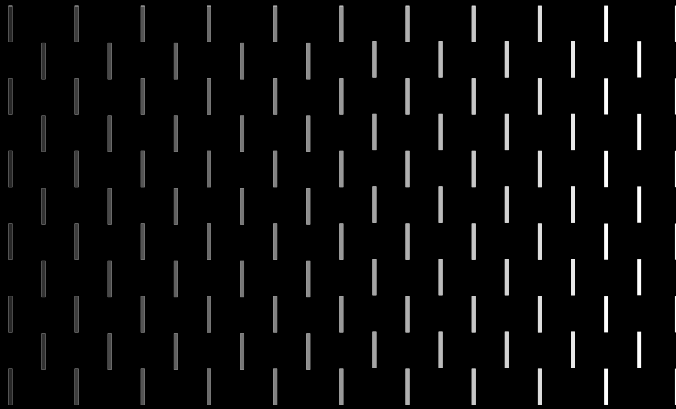◆ Apply wireless security measures to safeguard data

Key Skills

◆ Operating Systems

◆ Networking Concepts

◆ Network Topologies

◆ Cryptography Basics

◆ TCP/IP Model

◆ Public Key Infrastructure

◆ WLAN Security

Tools & Technologies

Windows   Linux

*Curriculum is subject to change.

Fullstack Academy

Unit 2
Enterprise Infrastructure Security

Understand the core facets of enterprise security. This unit covers fundamental security concepts, network defense mechanisms, Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), an overview of Zero Trust Network, and Identity and Access Management (IAM).

Key Learning Objectives

- Analyze key security concepts
- Evaluate network defense mechanisms
- Implement SOAR and SIEM tools
- Analyze log types, formats, and collection methods

- Configure SIEM components for data storage optimization
- Develop SIEM rules and use cases
- Manage alerts and incident response workflows
- Design secure authentication and access control strategies

Key Skills

- Security Fundamentals
- Network Security
- SIEM
- Log Management

- Incident Response Basics
- Identity & Access Management
- Zero Trust Concepts
- SOAR

Tools & Technologies

splunk>   Tor   Windows Server

*Curriculum is subject to change.

Fullstack Academy

Unit 3
Application Security and Cyber Resilience
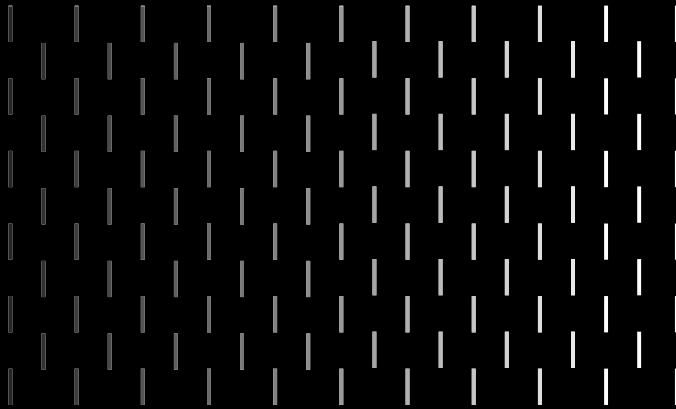
This unit explains the essentials of web application security. Learn core concepts like encryption and Public Key Infrastructure (PKI), address the OWASP Top 10 threats, and integrate security into development using threat modeling.

Key Learning Objectives

- Identify core principles of web application security

- Apply secure coding practices

- Integrate security measures into the software development life cycle

- Analyze threat modeling techniques

- Understand the role of cyber resilience in continuity, threat mitigation, and trust

Key Skills

- Web Application Security

- OWASP Top 10

- Server-Side Request Forgery
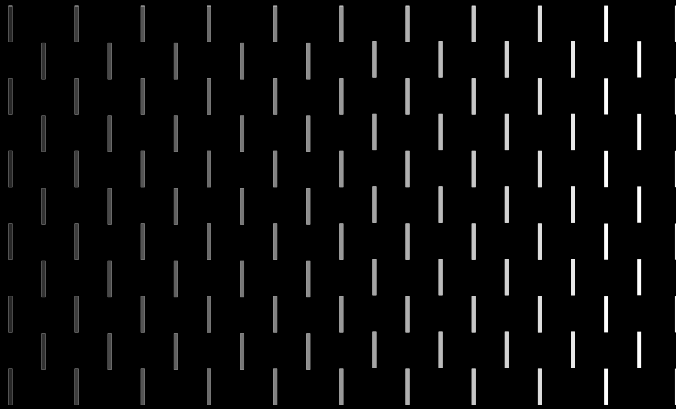
- Threat Modeling

- Cyber Resilience Concepts

Tools & Technologies

OWASP™

*Curriculum is subject to change.

Fullstack Academy

Unit 4
Web Application Vulnerabilities

Get hands-on experience with understanding and identifying weaknesses in web applications. This unit explores common application vulnerabilities and the techniques and tools used to find system vulnerabilities.

Key Learning Objectives

- ◆ Classify application vulnerabilities

- ◆ Analyze the security implications

- ◆ Analyze and demonstrate secure coding practices

- ◆ Integrate security measures for minimizing vulnerabilities

- ◆ Analyze the impact of regular updates

Key Skills

- ◆ Application Vulnerabilities
- ◆ Privilege Escalation
- ◆ Command Injection Attacks
- ◆ SQL Injection Attacks

- ◆ Cross-Site Scripting (XSS) Attacks
- ◆ Attack Vectors and Methods
- ◆ Vulnerability Identification Concepts

Tools & Technologies

metasploit®

*Curriculum is subject to change.

Fullstack Academy

Unit 5

Ransomware and Malware—Defense, Analysis, and Response
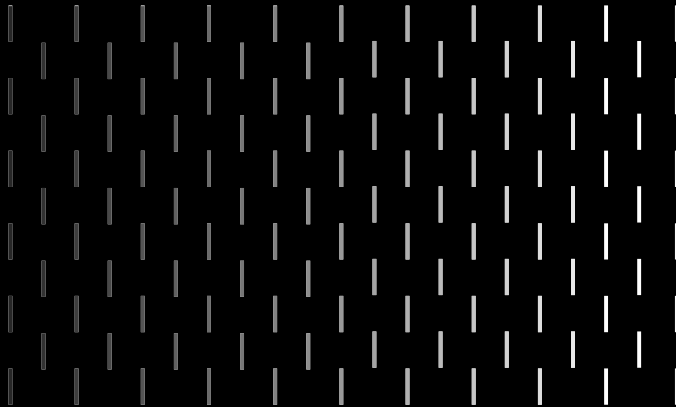
Learn techniques to combat modern malware threats. This unit introduces various types of malware, with a specific focus on ransomware, and covers malware analysis tools and techniques, digital forensics, and malware protection.

Key Learning Objectives

- Analyze different types of malware

- Implement digital forensics strategies

- Apply malware analysis techniques

- Examine ransomware attack campaigns and operators

- Evaluate malware naming conventions

Key Skills

- Malware Identification

- Incident Response Basics

- Ransomware Understanding and Mitigation

- Cyber Threat Intelligence

- Malware Analysis

- Static Analysis Techniques

- Digital Forensics

- Dynamic Analysis Techniques

Tools & Technologies

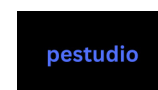7ZIP   Cmder   exterro FTK® Imager   HxD Hex Editor   njRAT   Noriben   pestudio   RanSim

*Curriculum is subject to change.

Fullstack Academy

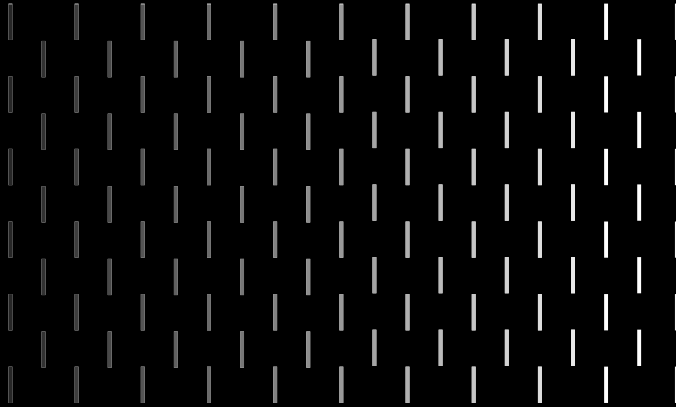**Unit 6**

Ethical Hacking: From Recon to Attack

Step into the shoes of an ethical hacker. This unit provides the foundation for ethical hacking, introduces the Cyber Kill Chain methodology, and covers essential reconnaissance and footprinting techniques used to gather information about target systems.

Key Learning Objectives

- Utilize Metasploit for user account enumeration

- Conduct active footprinting

- Perform DNS enumeration

- Apply advanced scanning techniques

- Implement network enumeration, mapping, and OS identification

- Explain the Cyber Kill Chain methodology and its stages

Key Skills

- Ethical Hacking & Reconnaissance

- Active Footprinting

- Cyber Kill Chain Methodology

- Active Reconnaissance

- Passive Reconnaissance

- Network Scanning

- Passive Footprinting

- DNS Enumeration

Tools & Technologies

*Curriculum is subject to change.

Fullstack Academy

Unit 7

Vulnerability Assessment and Penetration Testing (VAPT)
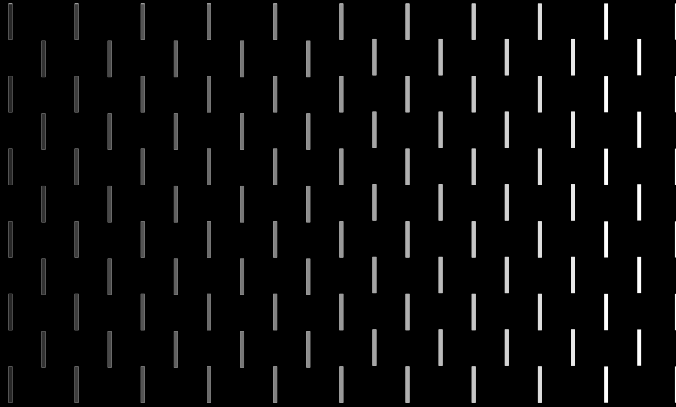
Develop the skills to identify and exploit vulnerabilities in systems and networks. This unit covers vulnerability analysis and assessment, penetration testing, security scanning, social engineering, and denial-of-service attacks. Cloud and container security are also discussed.

Key Learning Objectives

- Apply vulnerability assessment techniques
- Assess infrastructure and network-layer vulnerabilities
- Implement the vulnerability management lifecycle
- Conduct penetration testing activities
- Implement cloud and container security strategies
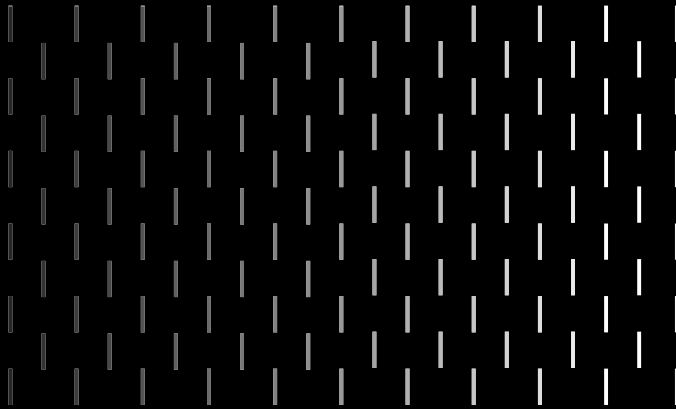- Evaluate social engineering and identity-based attack vectors

Key Skills

- Vulnerability Analysis
- Security Scanning
- Penetration Testing
- Social Engineering
- Denial of Service and DDoS Attacks
- Cloud Security
- Containerization
- Everything as a Service (XaaS)

Tools & Technologies

attify   aws   beebox SYSTEMS   crunch   metasploit   Nessus   NMAP   SHODAN   spiderfoot

*Curriculum is subject to change.

Fullstack Academy

Unit 8
Essentials of Generative AI

Explore the core concepts of Generative AI. This unit provides a fundamental understanding of Generative AI and Large Language Models (LLMs), focusing on prompt engineering and fine-tuning.

Key Learning Objectives

- Learn key concepts of generative AI and LLMs

- Utilize ChatGPT and domain-specific GPTs for practical use cases

- Demonstrate the ability to construct effective prompts

- Develop hands-on skills in leveraging multimodal capabilities and customized GPTs

Key Skills

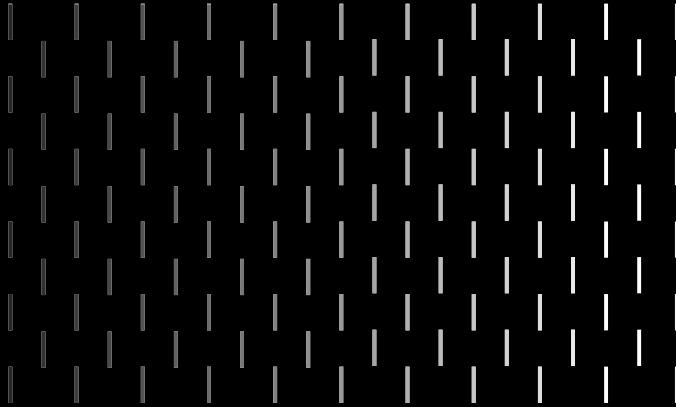- Generative AI Fundamentals
- Prompt Engineering
- Fine-tuning

Tools & Technologies

ChatGPT

*Curriculum is subject to change.

Fullstack Academy

Unit 9

Generative AI in Cybersecurity

Understand how AI and Generative AI are transforming cybersecurity. This unit explores the applications of GenAI in threat analysis, incident response, forensics, penetration testing, and defense, while also addressing the ethical implications of using GenAI in cybersecurity.

Key Learning Objectives

- Analyze the role of GenAI in cyber operations
- GenAI-driven defensive techniques
- Apply GenAI to real-world cyber scenarios
- Ethical implications of GenAI in cybersecurity

Key Skills

- Cybersecurity Analytics Using GenAI
- Introduction to Generative AI in Cybersecurity
- Risks and Vulnerabilities of GenAI in Cybersecurity
- Incident Response and Cyber Playbooks with GenAI

- Cybersecurity Triage Process with GenAI
- Guarding Against Risks in LLMs with GenAI
- Vulnerability Management with GenAI
- Defensive Techniques Using GenAI

- Penetration Testing Using GenAI
- Forensics Analysis with GenAI
- Threat Detection Using GenAI in SIEM
- GenAI-Driven SOAR

Tools & Technologies

ChatGPT

*Curriculum is subject to change.

Fullstack Academy

Unit 10

Capstone Project

Put your cybersecurity skills to the test! You'll create a comprehensive cybersecurity solution or analysis, applying the knowledge and skills gained throughout the bootcamp.

Key Learning Objectives

- Integrate knowledge from various units to solve a unique cybersecurity challenge

- Design a cybersecurity solution or analysis, and present your findings and recommendations
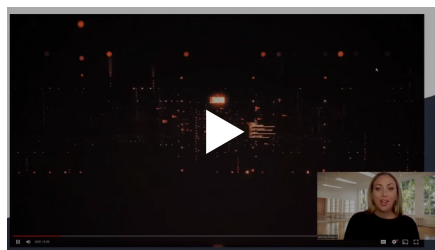
- Collaborate effectively in a team environment

Key Skills

- Problem-Solving in Cybersecurity

- Integration of Cybersecurity Concepts

- Teamwork and Collaboration

- Technical Presentation Skills

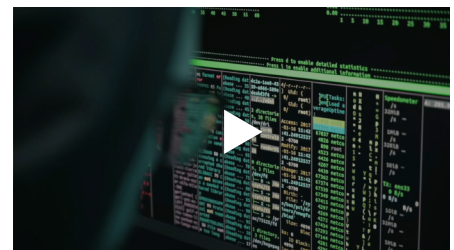## Watch Example Videos of Capstone Projects

Penetration Testing Simulation

Dance Studio Security Vulnerabilities

How to Use OSINT Tools

*Curriculum is subject to change.

CompTIA Security+ (Elective)

This optional elective unit will prepare you with essential knowledge and skills to take the CompTIA Security+ certification exam. The elective focuses on core security principles, risk management, incident response, cryptography, identity and access management, and securing networks, systems, and applications.

The CompTIA Security+ certification is a globally recognized credential that validates your foundational knowledge and skills in cybersecurity. The certification demonstrates competency in core concepts required for career advancement in cybersecurity.

Eligible students can receive a voucher for one CompTIA Security+ exam attempt at no additional cost.

Key Learning Objectives

- Understand and apply cybersecurity risk management concepts

- Understand compliance, governance, and security auditing principles

- Identify and mitigate common threats, vulnerabilities, and attacks

- Secure network architecture and endpoint systems

- Respond to security incidents and perform basic digital forensics

- Implement identity and access controls

Key Skills

- Threat Analysis and Vulnerability Assessment

- Basic Penetration Testing and Incident Response

- Network and Endpoint Security Configuration

- Identity and Access Management

- Secure Protocol Implementation

- Familiarity with Cloud and Mobile Security Best Practices

*Curriculum is subject to change.

Testimonials

Tyler Blocker
Technical Support Specialist

"The most helpful skills I learned were problem-solving, technical proficiency in cybersecurity tools, collaboration, and time management."

Read More

Kennedy Arnold
Fullstack Academy Cybersecurity Bootcamp Graduate

"I am leaving this bootcamp hungry for more information and excited about all the aspects of the cybersecurity industry that I could find myself a part of."

Read More

Korbin Lopez
Desktop Application Support

"I'm very glad to have taken the bootcamp, and it was a big plus on my resume to my current employer."

Read More

Xenisha Hawkins
Fullstack Academy Cybersecurity Bootcamp Graduate

"Now, I feel more confident about entering the workforce because I can bring the education I gained from the bootcamp."

Read More

Career Success Services

Starting in the bootcamp, you'll receive guidance and tools you'll need to power your job search.

Upon bootcamp graduation, and for a full year beyond, you'll have the opportunity to opt into the Fullstack Academy Career Success Program and access 1:1 personalized career coaching to help achieve your desired career outcome.

Interview Prep

◆   Mock Standard Interviews (Q&A)

Workshops

◆   How to Pitch Yourself

◆   Technical Resume Guidance

◆   LinkedIn Optimization

◆   Navigating the Job Search Process

◆   Job Application Best Practices

◆   Salary Negotiation

◆   Interview Answer Prep

◆   Leveraging Transferable Skills

*Curriculum is subject to change.

Make Your Move.

Fullstack Academy

APPLY NOW

fullstackacademy .com

Fullstack Academy