Part-Time Online Cybersecurity Bootcamp

24 Weeks to a Cyber Career

Part-Time class commitment
Career Services Included
Learn by Doing 50-75% Lab Work

Over 8,000 alumni, hired by tech companies worldwide

*As of 2020 alumni data
Overview

The importance of cybersecurity today cannot be overstated. As our reliance on technology grows, there’s a corresponding need to secure and defend networks and data against leaks, theft, and attacks. That’s good news for cybersecurity specialists - the U.S. Bureau of Labor Statistics projects cybersecurity jobs will grow 31% through 2029. In short, there’s job security in cybersecurity.

What You’ll Get

- **Top Industry Certifications**
  Learn skills applicable to certifications such as the Network+, Linux+, Server+, Cloud+, and certified Ethical Hacker (CEH), and receive vouchers for CompTIA Security+ and CySA+.

- **Learn By Doing**
  Gain hands-on experience with a host of popular tools such as Wireshark, Kali Linux, Metasploit, and more within a sandbox environment.

- **Cyber-Specific Career Services**
  Receive personalized career support from a dedicated cybersecurity career services manager, and keep your career service access for life.

- **End-to-End, Extensive Curriculum**
  Cover the latest real-world deployment of cybersecurity management practices, including defensive and offensive tactics, NIST Cybersecurity Framework, and event & incident management.
A Professional-Grade Curriculum

From CompTIA Security+ to CySA+ certifications and beyond, our Cybersecurity program teaches students critical skills to assist in the identification, assessment, reporting, and mitigation of technology and information security risks.

This professional-grade program provides information, strategies, and tactics to identify and manage information system vulnerabilities, create effective defenses and preventative measures, and deploy countermeasures against attackers.

After completing Coding Dojo’s Cybersecurity program, students are mission-ready to identify, assess, report, and mitigate technology and information security risks.

Your Progression Plan
Week-By-Week Curriculum
Curriculum is subject to change

WEEK 1
Fundamentals
Dive right in with broad exposure to cybersecurity including: Controls, Frameworks, Benchmarks, Virtual Machines, Threats, Vulnerabilities, Defenses, Secure Software, Testing, Cryptography

Labs:
• VM Setup
• Windows & Mac Directions
• Network Settings
• Scanning Networks
• Packet Sniffing

WEEK 2
Kali Linux Introduction
Continuing the broad exposure adding more major cybersecurity elements. Build out your Kali Linux machine while also learning about networking and data security.

Labs:
• Nessus installation
• Password Cracking

WEEK 3
Networking & Security
Learn about network configurations and data security, including Network Design, Firewall Configuration, Access Control.

Labs:
• Basic ACL
• Firewall Configuration Kali
• Secure Network Design

WEEK 4
Malware & Intrusion Detection
Viruses and Ransomware, intrusion detection, useful tools, introduction to embedded (control) systems, secure shell, mobile & endpoint security.

Labs:
• Snort Installation
• SSH
• Endpoint Protection

WEEK 5
Virtual Machines
Learn more about Virtual Machines, malicious code, Disaster Recovery, and Powershell

Labs:
• Malicious Code
• Powershell Security

WEEK 6
Incident Response & Forensics
Identifying and responding to incidents, technical and legal elements of forensics

Labs:
• Configuring an Intrusion Detection System
• Incident Response
• Digital Forensics

WEEK 7
Resiliency & Automation
Learn how resiliency, automation, and backups provide essential and fundamental protection

Labs:
• Backup

WEEK 8
Cyber Career Prep
Tabletop exercises are effective for learning, preparing, and solving problems before they happen

Labs:
• Tabletop Exercise
• Career Preparation
• Belt Exam Sec+
Week-By-Week Curriculum
Curriculum is subject to change

WEEK 9

Threat Assessments
Understand roles and responsibilities, security controls, indicators of compromise, understanding threats, attack tools, monitoring networks

Labs:
- IoC Investigation
- Network Group Assignment

WEEK 10

Network Access Control
Protect networks, monitor and analyze various services for signs of compromise, run scripts, understand and use SIEM (Security Information and Event Management)

Labs:
- Wireshark Analysis
- Log Analysis
- Windows Security Logs
- Analyzing Email Headers
- SIEM Group Assignment

WEEK 11

Intermediate Forensics
Examining forensic tools and techniques, digging into indicators of compromise, understanding detection and containment, learning digital evidence collection, understanding frameworks, policies and procedures, exploring attacker lateral movement and pivoting.

Lab: Digital Evidence Collection (2 day lab)

WEEK 12

Intermediate Incident Response
Review of the phases of IR for further in depth work, participate in extended lab exercise, as well as understand the critical importance of effective recovery.

Lab: IR Writing Assignment (2 day lab)

WEEK 13

Risk Analysis
Understanding and managing risk is a key to security professional and program success; enumeration, credential security, and vulnerability assessment are key to effectiveness of security professionals and programs.

Labs:
- Risk Management
- Nmap Formatting
- Credential Security

WEEK 14

Regulation
Wireshark, Regulations, IAM, Network segmentation and other protections, Linux auditing, hardware assurance, specialized technologies

Labs:
- Another Wireshark
- Research Assignment (Regulations)
- Linux Audit

WEEK 15

Share Permissions
Learn technical and non-technical controls, various related regulations, the relationship of security and privacy, how to configure and analyze share permissions, and mitigate attacks

Lab: Configuring and Analyzing Share Permission

WEEK 16

Cloud Access with OWASP
Learn cloud technologies and how to protect your cloud-based solutions.

Labs:
- OWASP Research
- Web Assessment
- Belt Exam CySA+
**Week-By-Week Curriculum**

Curriculum is subject to change

---

**WEEK 17**

**Ethical Hacking**
Discuss the ethics of hacking while learning penetration testing, Metasploitable2 and Eternal Blue.

**Labs:**
- Metasploitable3 & Good Gone Bad
- Eternal Blue

---

**WEEK 18**

**Footprinting**
Understanding the underlying capabilities of search engines, WHOIS, DNS, nmap, dirbuster and gobuster, nikto, social engineering, specialized scanners, SNB enumeration.

**Labs:**
- Footprinting Assignment
- Specialized Scanners
- SMB Enumeration

---

**WEEK 19**

**Proactive Threat Hunting**
Become proactive in your approach to cybersecurity by seeking threats.

**Labs:**
- Vulnerability Scanning 1 of 2
- Vulnerability Scanning 2
- BurpSuite Setup

---

**WEEK 20**

**Mobile Pen Testing**
Learning Local File Inclusion and Remote File Inclusion, SQL injection techniques and defences, hacking and testing mobile devices.

**Labs:**
- LFI/RFI
- SQL Injection

---

**WEEK 21**

**Buffer Overflow**
Learn to counter and create a buffer overflow attack on Windows / Linux.

**Labs:**
- Windows BOF
- Analyzing Output from Web Application Assessment Tools

---

**WEEK 22**

**Advanced Malware**
Add to your malware knowledge with advanced techniques and tools.

**Lab:** Malware Analysis

---

**WEEK 23**

**File Transfers**
Learn to elevate privilege to fully exploit the platform, monitor the network, or access other systems during an attack.

**Labs:**
- Linux Privesc
- Windows Privesc

---

**WEEK 24**

**Exploits & Password Attacks**
Learn various sources for exploits and how to use them, the use of Shells, password attacks. With great power comes great responsibility!

**Labs:**
- How Many Shells?
- Password Attacks
How to Enroll

1. **Explore**
   - Schedule a Q&A call with Admissions to get quick answers about the bootcamp or join the next open house.

2. **Apply**
   - Ready to join? Submit your application and pick your start date to join.

3. **Complete your Interview**
   - Schedule an interview with admissions. The interview is non-technical - no technical experience is required.

4. **Deposit to Enroll**
   - If accepted, submit your deposit to save your seat and gain access to bootcamp prep materials for your start date.

**Financing Options**

Schedule a call with Admissions to discuss which payment or financing option is right for you.

- **Pay in Full**
  - Save on tuition by paying in full upon enrollment

- **Pay in Installments**
  - Spread payments over the course with standard and custom installment plans

- **3rd Party Financing**
  - Finance bootcamp with a third party loan from a variety of lenders

Apply Now