Austin Peay State University

Cybersecurity Bootcamp Syllabus

The Cybersecurity Bootcamp at Austin Peay State University is an accelerated training program designed to successfully prepare people with little or no background in IT for entry-level jobs in cybersecurity – one of the most in-demand technology fields.

THRIVEDX'S METHODOLOGY

Developed around military training methodologies and hands-on learning, the program focuses on the key skills sought by employers. The Bootcamp prepares students not only with technical knowledge, but also with the best practical cybersecurity skills to help them excel in the tech job market.

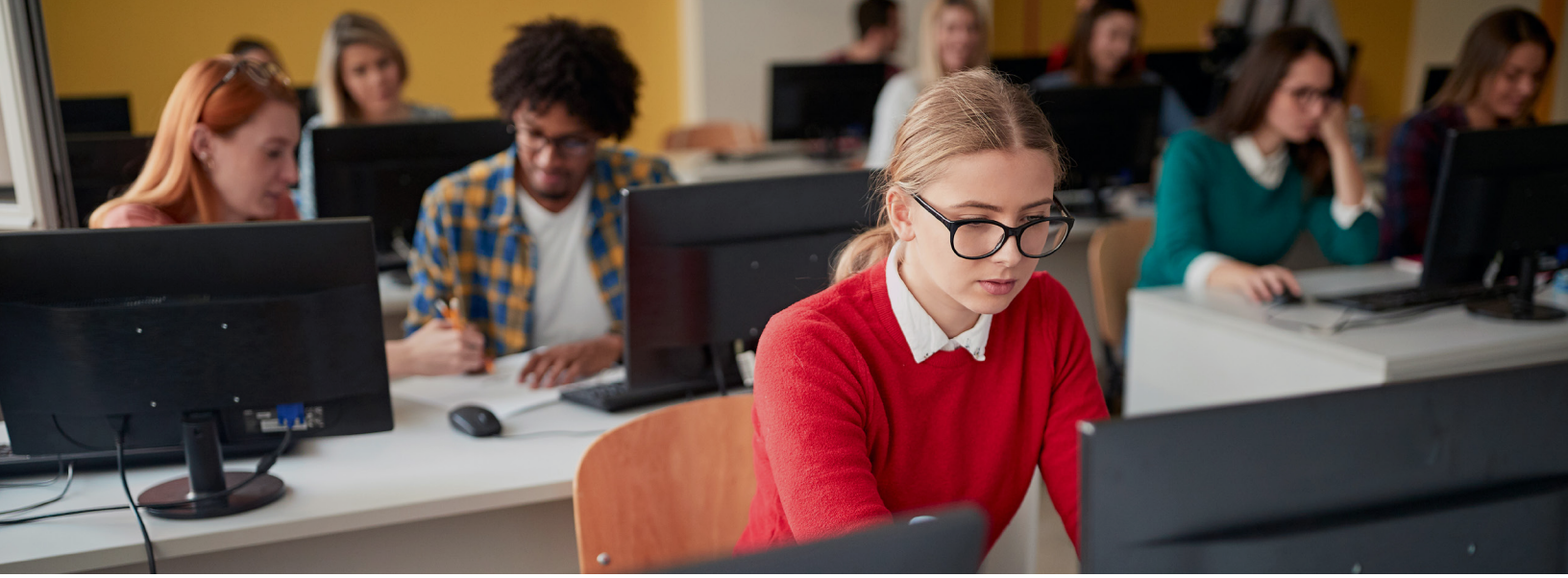
This is accomplished with:

- Practical and theoretical knowledge delivered through demos, real-world examples, videos, infographics, quizzes, and games
- Technical skills, frameworks, and tools taught through hands-on exercises in a safe virtual environment
- Essential soft-skills training – from teamwork to interview prep – embedded throughout the program

www.apsu.edu/continuing-education/

Austin Peay State University
CLARKSVILLE TENNESSEE

impact ThriveDX



Bootcamp Structure

PREWORK

Prior to the start of the Bootcamp, learners will complete the self-paced Prework module, whose objective is to bring everyone to the same level of technical expertise.

FOUNDATIONAL MODULES

The first part of the Bootcamp covers the foundations of cybersecurity. This includes the modules Bootcamp Introduction, Network Administration, Introduction to Cybersecurity, Network and Application Security, and Incident Handling.

MIDTERM

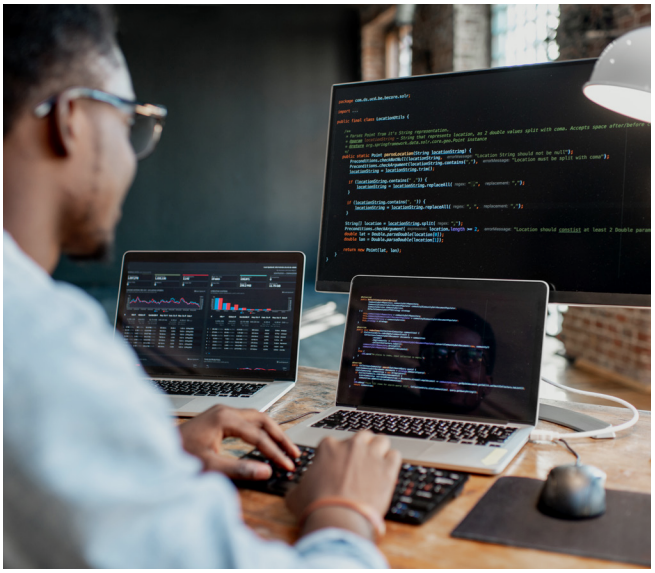
After the first part of the Bootcamp, learners will take a midterm exam.

ADVANCED MODULES

The second part of the Bootcamp dives deeper into advanced topics and introduces students to different areas of specialization. These modules include Forensics, Malware Analysis, Ethical Hacking and Incident Response, Secure Design Principles, Risk Management, and Threat Intelligence.

FINAL ASSESSMENTS

During the last module, bootcampers will complete several final scenarios and a cumulative final exam.



Syllabus

PREWORK

Prior to the start of the Bootcamp, learners are required to complete the self-paced Prework module, whose objective is to bring everyone to the same level of technical expertise. This module will familiarize learners with the platform and acknowledge key details of the Bootcamp. The Prework can take anywhere from 10-40 hours depending on the learner's technical background.

Topics Covered:

- The cybersecurity field, the main challenges in theindustry,
- The cybersecurity mindset and "learning how to learn."
- Computer fundamentals, operating systems (Windows,Linux, macOS), and command line utilities.
- Computer networks, OSI model, and network protocols
- MITRE ATT&CK Framework tactics and techniques

TOOLS: Wireshark, Putty

I. BOOTCAMP INTRODUCTION

The Bootcamp Introduction provides learners with the tools required to make the Bootcamp an enjoyable and efficient learning experience. During this module, they will learn how the Bootcamp will be structured as well as the basics of computers.

Topics Covered:

- Overview of Bootcamp and Cybersecurity Industry
- Cybersecurity Career Paths
- Prework Content Review

II. NETWORK ADMINISTRATION

In the Prework module, bootcampers are taught the fundamental principles and concepts of networking. This module dives even deeper and focuses on designing, configuring, and troubleshooting networks. Bootcampers will learn the necessary skills for running and monitoring a network in an insightful manner.

Topics Covered:

- Network Configuration – LAN, WAN
- Segmentations, VLANs and Subnetting
- Network Mapping Tools
- Troubleshooting and Monitoring Networks
- Network Devices – Switches, Routers
- Telecommunication
- System Administration

TOOLS: Cisco Packet Tracer, Nmap, Windows PowerShell

III. CYBERSECURITY FUNDAMENTALS

This module is designed to teach how organizations implement cybersecurity and introduce the different roles in the industry. Additionally, bootcampers will get to know the history of famous hackers from the 1950s until today. This module will then explore modern hackers and their motives, capabilities, and techniques, as well as the different types of malwares they use to attack their victims.

Topics Covered:

- Most common vurnerabilities, Risks, And Threats
- The Main Concepts In Cybersecurity
- Types Of Malaware And Attackers
- NIST & International Cybersecurity Framework
- Most common Cyber-Attacks
- Famous Cyber-Attacks

IV. NETWORK AND APPLICATION SECURITY

In this module, bootcampers learn about network and application security defense methodologies. They will be able to identify which tools are required based on the network and the needs of the organization. It also covers construction of secure network architectures. For each method, bootcampers will learn how to detect and eventually block malicious actors from carrying out cyber-attacks and crimes.

Topics Covered:

- Cryptography – Symmetric vs Asymmetric Keys
- Encryption/Decryption, Hash functions
- Security Architecture
- Security Tools – Firewalls, Antivirus, IDS/IPS, SIEM
- Access Control Methods, Multi-factor Authentication, Authentication Protocols
- Honeypots and Cyber Traps

TOOLS: Kali Linux, Splunk, Snort IDS, Active Directory, Nmap, Windows Firewall, Linux iptables

V. INCIDENT HANDLING

This module will teach students about the most common cybersecurity attack types in the web, domain, and malware areas. They will learn the goal of each type, how they work, their impact, and how to detect them. Then, they will practice detection and analysis of incidents in security applications as they learned in the Network & Security Application module and will practice the role of a cybersecurity analyst in real life.

Topics Covered:

- Types Of Attacks in The Web Area (DDOS, SQLInjection, XSS, LFI, Command Injection)
- Types Of Attacks in The Domain Area (Typo Squatting, Domain Hijacking, Pass The Hash, Pass The Ticket, LDAP Reconnaissance, Brute Force)
- Types Of Attacks in The Malware Area (Ransomware, Virus, Worm, Trojan Horse, Adware)
- Practicing The Role of SOC Analysts by Detecting And
- Analyzing Alerts And Incidents In Splunk, SIEM, And EDR
- Analyzing Malicious Indicators Using VirusTotal
- Group and Individual Incident Report Writing

TOOLS: Splunk, In-House SIEM, Wazhu, VirusTotal, Powershell, Wireark

VI. FORENSICS

In this module, bootcampers will learn digital forensic processes for analyzing threats in digital devices. This includes identification, recovery, investigation, and validation of digital evidence in computers and other media devices.

Topics Covered:

- Computer Memory Forensics, Memory Dump Analysis
- FTK Imager, Autopsy, Redline and RAM capturing
- Digital Evidence Acquisition Methodologies
- Registry Forensics
- Windows Timeline Analysis and Data Recovery
- Network Forensics, Anti-Forensics and Steganography

TOOLS: Volatility Framework, FTK Imager, Autopsy, NetworkMiner, Wireshark, OpenStego, ShellBags Explorer, winmd5free, Magent RAM Capture, Redline, HxD

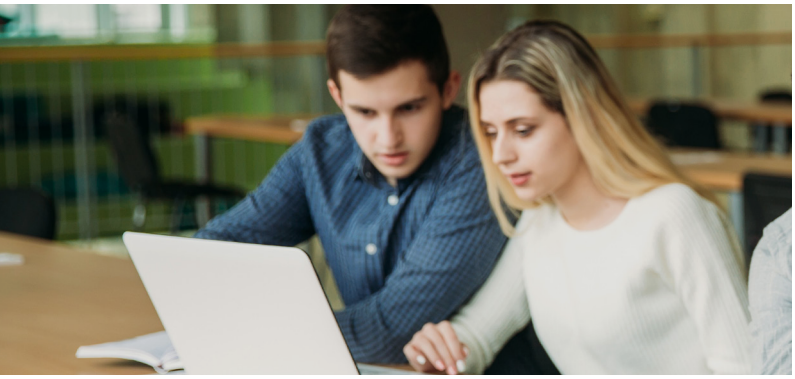
VII. MALWARE ANALYSIS

Bootcampers will learn different techniques for analyzing malicious software and understanding its behavior. This will be achieved using several malware analysis methods such as reverse engineering, binary analysis, and obfuscation detection, as well as by analyzing real-life malware samples.

Topics Covered:

- Dynamic Malware Analysis, Reverse Engineering and Malware Obfuscation
- Fileless Malware Analysis
- Containment, Eradication and Recovery Malware Stages
- Analysis using Sysinternals

TOOLS: Procexp, Procmon, Autoruns, TCPView, PuTTY, ExeInfo PE, ProcDOT, HashCalc, FileAlyzer, PDFStreamDumper, HxD, Wireshark, UPX



VIII. ETHICAL HACKING AND INCIDENT RESPONSE

As future Cybersecurity Analysts, it is essential for bootcampers to understand offensive methodologies in cyber warfare. In Ethical Hacking, they will learn how to perform cyber-attacks, which will provide them with insights on cyber defense best practices, vulnerability assessments, forensics, and incident response processes. In Incident Response, bootcampers will learn the relevant response methodologies used once an attack has occurred. They will overview identifying cybersecurity breaches, insider/outsider threats, incident response life cycles, performing relevant assessments, and developing protection plans.

Topics Covered:

- Hacking, Ethical Hacking and the Penetration Testing Frameworks
- Ethical Hacking Phases: Reconnaissance, Scanning,Obtaining Access, Maintaining Access, Covering tracks, and The Cyber Kill Chain.
- Network Hacking - Metasploit Framework
- Web Application Hacking - OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post-Incident Activities
- Capture the Flag Challenge

TOOLS: Metasploit, SQLMap, Nmap, OSINT Framework, CUPP, Hydra, Recon-ng, Burp Suite

IX. SECURE DESIGN PRINCIPLES

In this module, bootcampers will learn about trend analysis and how to perform it. They will become familiar with the newest cybersecurity trends, threats and more. Furthermore, bootcampers will learn cybersecurity design best practices, as well as how to assess and detect security design flaws.

Topics Covered:

- Trend Analysis
- Artificial Intelligence in Cybersecurity
- Zero-Trust Policy
- Best Detection Methodologies
- Incident Impact Mitigation

X. RISK MANAGEMENT

In this module, bootcampers will learn about risk management, and dive into the cybersecurity aspects involved. In today's world, almost any action can become a potential risk. Therefore, bootcampers will learn risk management methodologies and processes that will assist in effectively managing such risks – while understanding that not all risks can be eliminated immediately.

Topics Covered:

- Risk Management Processes
- Analyzing, Prioritizing, Evaluating and Monitoring Severity of Internal and External Risks
- Risk Management Policies, Procedures, Standards, and Guidelines
- Security models

TOOLS: ThriveDX Security Awareness Training

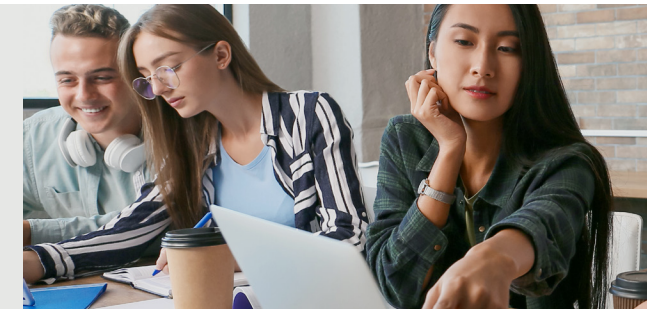
XI. THREAT INTELLIGENCE

One of the ways to protect your organization is to know your enemy. In this module, bootcampers will learn different methods, processes, techniques, and tools involved in gathering intelligence about potential threats such as hackers and attack vectors.

Topics Covered:

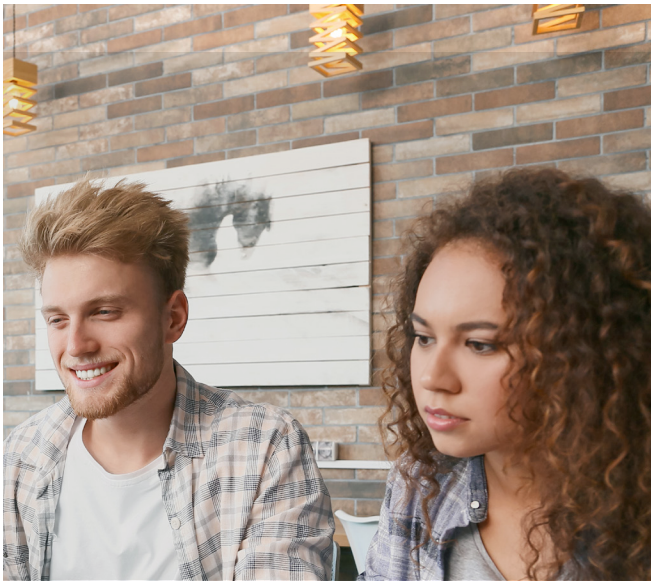
- Threat Intelligence Cycle Methodology and Industry Implementation
- Google Hacking – Operators, Finding Sensitive Data, Directory Listing, Devices and Hardware
- Dark Web and Dark Market Investigation
- Online Anonymity using Metadata, Google Cache, VPN and Tor
- Trend Analysis, Basic Excel Data Analysis
- Industrial Tool Practice in Real Environments

TOOLS: Elasticsearch, Kibana, Webhose data (logs from the darkweb), Web Scraping, Tor Browser, IntSights Threat Intelligence Platform



XII. FINAL SCENARIOS AND INTERVIEW PREP

The final module includes real-life scenarios of cybersecurity incidents, and a final exam covering all the content learned along the Bootcamp. In the Full-Time Bootcamp, learners will present group projects which were worked on throughout the course. We will also review technical and soft-skill preparation for job interviews.



For additional information, please email us at pro-work-center@apsu.edu or call 931-221-6487.

www.apsu.edu/continuing-education/

Austin Peay State University
CLARKSVILLE TENNESSEE

impact ThriveDX