Cybersecurity Bootcamp Syllabus

The Cybersecurity Bootcamp at Eureka College powered by Cybint is an accelerated cybersecurity training program designed to successfully prepare people with little or no background in IT for entry level jobs in cybersecurity, a highly in-demand and lucrative career path.

OUR METHODOLOGY

We developed the Bootcamp under the principle of "**everything** you need to know but **only** what you need to know." With our accelerated learning methodology – based on military bootcamps – we focus on teaching students the specific skills they will need for success. We accomplish this 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.eureka.edu/cybersecurity

EUREKA COLLEGE

Cybint

Bootcamp Structure

PREWORK

Students are asked to complete the self-paced Prework module, whose objective is to bring everyone to the same level of technical expertise prior to the start of the Bootcamp.

FOUNDATIONAL MODULES

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

MIDTERM

After the first part of the Bootcamp, students will take a Midterm Exam. Students are expected to achieve a grade of 60% to pass.

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 Principals, Risk Management, Threat Intelligence.

FINAL ASSESSMENTS

During the last module Final Scenarios and Interview Prep, students will complete three scenarios and a cumulative Final Exam. Students are expected to achieve an overall grade of 60% in the Final Assessments to pass the Bootcamp.

Syllabus

PREWORK

Prior to the start of the Bootcamp, students 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 students with the Cybint platform and acknowledge key details of the Bootcamp. The Prework can take anywhere from 10-40 hours depending on their technical background.

Topics Covered:

- Basics of Computer and Device Hardware, Software, Operating Systems and Processes in Windows and Linux
- Networking Basics and the OSI Model

TOOLS: *Wireshark, Putty*

I. BOOTCAMP INTRODUCTION

The Bootcamp Introduction will provide students with the tools required to make the Bootcamp an enjoyable and efficient learning experience. During this module, students 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 ADMIN

In the Prework module, we covered the fundamental principles and concepts of networking. This module will dive even deeper and focus on designing, configuring, and troubleshooting networks. Students will be taught 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. INTRODUCTION TO CYBERSECURITY

This module is designed to teach how organizations implement cybersecurity and introduce the different roles in the industry. Additionally, students 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 malware they use to attack their victims.

Topics Covered:

- NIST Framework
- Malware Types
- Social Engineering
- Vulnerabilities, Risks, and Exploits
- Famous Cyber-Attacks

IV. NETWORK AND APPLICATION SECURITY

In this module, students will 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 will also cover construction of secure network architectures. For each method, students 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, OpenVPN, Windows Firewall, Linux iptables*

V. INCIDENT HANDLING

In this module, students will learn about the most common types of cybersecurity attacks. They will practice detection and analysis of incidents as a Cybersecurity Analyst would in real life. Students will analyze different attack vectors and their attributes and identify false-positive cases.

Topics Covered:

- Detection and Analysis of Cyber-Attacks – DDos/Dos, Brute-Force
- OSWAP Top 10 Attacks – SQL Injection, Cross-Site Scripting
- Group and Individual Incident Report Writing

TOOLS: *Splunk*

VI. FORENSICS

In this module, students 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

Students 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
- Android APK Analysis

TOOLS: *HashCalc, Exeinfo PE, PDF Stream Dumper, FileAlyzer, HxD, Yaazhini Vulnerability Scanner, APK Tool, Ghidra, HashCompare, UPX Easy GUI, Wireshark*

VIII. ETHICAL HACKING AND INCIDENT RESPONSE

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

Topics Covered:

- Ethical Hacking Processes and Methodologies
- Network Hacking, Reconnaissance, Google Hacking and Locating Attack Vectors
- Exploitation Techniques
- Web Application Hacking, OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post Incident Activity

TOOLS: *Metasploit, SQLMap, Nmap*

IX. SECURE DESIGN PRINCIPALS

In this module, students will learn about trend analysis and how to perform it. They will become familiar with the newest cybersecurity trends, threats and more. Furthermore, students 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, students will learn about risk management, and dive into the cybersecurity aspects involved. In today's world, every action we take can become a potential risk. Therefore, students 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

XI. THREAT INTELLIGENCE

One of the ways to protect your organization is to know your enemy. In this module, students 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, students will present group projects which were worked on throughout the course. We will also review technical and soft-skill preparation for job interviews.

www.eureka.edu/cybersecurity

EUREKA COLLEGE

Cybint