Akademi

MAY 2026

CYBERSECURITY ENGINEERING BOOTCAMP

Powered by Flatiron School

LEAD INSTRUCTOR

Dupuy Rony Charles

TABLE OF CONTENTS

COURSE OVERVIEW

MAY 2026 - NOVEMBER 2026

Network Security

This course will focus on the core ideas in network security - Ethernet, WIFI, attacks on TCP hijacking, and more.

Systems Security

This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system and memory). Learn to utilize tools such as Metasploit and command line tools in Linux.

Cyber Threat Intelligence

The course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts of how cyberspace has become a new warfighting space

Governance, Risk Management, & Compliance

This course covers how to engage all functional levels within the enterprise to deliver information system security. The course addresses a range of topics on securing the modern enterprise.

Logs & Detection

This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, firewalls and other network security devices.

COURSE OVERVIEW (PART II)

MAY 5, 2025 - OCTOBER 17, 2025

Python

This course provides the fundamental structure and language for creating Python scripts and automation. The focus will be on learning basic coding, code analysis and secure coding practices.

Application Security & Penetration Testing

This course focuses on applications and their vulnerabilities running on both workstations and servers. You'll learn penetration testing for vulnerabilities either in applications or network resources.

Applied Cryptography

This course teaches the components of cryptography, provides hands-on experience on configuring a web server with SSL/TLS, and interfacing with Certificate Authorities, issuing certificates, configuring SSH securely, and sending/receiving encrypted and signed email.

Capstone

The group project will present a scenario and allow the students to work within their individual expertise to work through the particulars. The project will culminate in a professional level oral and written report, which can be used as part of a portfolio.

CYBERSECURITY ENGINEERING PREP

All students are required to complete what we call "Cybersecurity Engineering Prep" at least one week before the start of class. During the prep course, students will get accustomed to the Canvas platform, set up their virtual machines, and obtain a basic understanding of Python, Systems, and Networks to prepare them for day 1 of class.

The prep course generally takes between 30-40 hours to complete, and is bookended by a pre-test and post-test to assess understanding of the concepts covered.

CURICULUM

All instruction is held within Canvas, leveraging content from our curriculum partner, Flatiron School. The Cybersecurity Engineering Bootcamp (Part-Time) is 25 weeks long and requires students to be available at minimum 10-15 hours per week for the duration of the program.

Phase 1	Cybersecurity Foundational Skills Network Security, Systems Security, Applied Cryptography, GRC, and Python
Phase 2	Cybersecurity Intermediate Skills Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, and Python
Phase 3	Cybersecurity Skills Development Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, and Logs & Detection
Phase 4	Gray Hat Hacking Systems Security, Network Security, Logs & Detection, Application Security & Penetration Testing, and GRC
Phase 5	Cybersecurity Skills Application Systems Security, Network Security, Logs and Detection, Application Security and Penetration Testing, & Capstone

NETWORK SECURITY

This course will focus on the core ideas in network security. The first portion of the class will continue review of basic network protocols: Ethernet, 802.11 (WiFi), IP, UDP, TCP, ARP, DHCP, DNS, ICMP, BGP, SMTP, POP/IMAP, FTP, HTTP, IGMP, and the attacks on these basic technologies: TCP hijacking, ARP cache poisoning and domain spoofing, as well as countermeasures. We then explain sniffing and port scanning, firewalls, IDSes and NIDSes and cover wireless protocols and their security. Then we segue into AppSec with a focus on web security. Finally, we look at denial of service and attack payloads.

At the completion of this course, a student will be able to:

- Utilize the layers of the TCP/IP and OSI models in analyzing network protocols.
- Analyze packet captures and draw conclusions about network activity.
- Create a web application and evaluate its security.
- Explain network security protocols as well as their vulnerabilities.
- Utilize attack tools to mount attacks against various types of networks and use countermeasures to forestall these same attacks.
- Map ports on a given IP, fingerprint services, catalog vulnerabilities, bypass firewalls, and mount a large array of web-based exploits.
- Deliver a wide variety of payloads to attain and maintain backdoor access to a compromised machine.
- Analyze AI/ML/ChatGPT traffic and use AI for deep packet inspection.

SYSTEMS SECURITY

This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system and memory). We will also utilize tools, including Metasploit and command line tools in Linux (xxd, gdb, etc) for further analysis of exploits.

We will explore exploits and their countermeasures, including buffer overflows, TOCTOU, shellcode injections, integer overflows and off-by-one errors. We will also cover basic Cloud security and migration considerations, Hypervisor Exploits and Android and iOS security.

At the completion of this course, a student will be able to:

- Utilize AI/ML/ChatGPT for host hardening and secure coding.

CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence 100 provides students with the foundational skills of a Threat Intelligence Analyst. The course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts of how cyberspace has become a new warfighting space that targets private and public critical infrastructure, economic and national security targets across all sectors globally. Students must understand the overall threat environment, how to discern the "so what" of information, and critically think and analyze complex human influenced cyber problems and threats to public and private information enterprises. Threat Intelligence 200 introduces students to the various methodologies of intelligence analysis and planning. Students will learn about the Cyber Kill Chain, Center of Gravity (COG) Analysis and CTI Diamond Model and then learn how to apply them using Cyber Intelligence Preparation of the Environment (IPE). The class, Cyber Mission Analysis, will culminate with students presenting their Mission Analysis Brief to the instructor as if they are the CISO.

A high-level perspective of threat intelligence (its creation and consumption):

- Adversary monetization methods
- Intelligence gathering
- Intel sources
- Intelligence analysis
- Planning with intelligence
- Leveraging AI/ML/ChatGPT for threat intelligence feeds

GOVERNANCE, RISK MANAGEMENT & COMPLIANCE

This course will focus on Governance, Risk, and Compliance (GRC). Students will learn how to engage all functional levels within the enterprise to deliver information system security. To this end, the course addresses a range of topics, each of which is vital to securing the modern enterprise. These topics include inter alia plans and policies, enterprise roles, security metrics, risk management, standards and regulations, physical security, and business continuity. Each piece of the puzzle must be in place for the enterprise to achieve its security goals; adversaries will invariably find and exploit weak links. By the end of the course, students will be able to implement GRC programs at the maturity level that many organizations are not at currently and to establish efficient, effective, and elegant Information Security Programs.

A high-level perspective of threat intelligence (its creation and consumption):

- Plans and policies
- Enterprise roles
- Security metrics
- Risk management
- Standards and regulations
- Physical security
- Business continuity
- Identify AI/ML/ChatGPT
- compliance, privacy, and risk considerations

LOGS & DETECTION

This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, firewalls and other network security devices. We will explore the information stored in logs and how to capture this data for analyzing these logs with a Security Information and Event Manager (SIEM). We will learn the steps involved in Incident Response and Crisis Management.

At the completion of this course, a student will be able to:

- Identify log sources and the configurations necessary to achieve appropriate logging levels.
- Describe the different types of data contained in log files.
- Configure data sources and SIEMs to allow the analysis of log data, including the automation of those tasks.
- Identify steps in Incident Response and Crisis Management.
- Use AI/ML/ChatGPT to detect anomalous and behavioral events.

PYTHON

Python programming is a fundamental skill used by Cybersecurity Engineers. This course course provides the fundamental structure and language for creating Python scripts and automation. The focus will be on learning basic coding, code analysis and secure coding practices.

Python 100 will cover the differences between interpreted and compiled coding languages. The focus for the interpreted languages will be the basic code structure for Python, conditionals, loops and algorithm diagramming tools. Students will work on analyzing basic code, modify that code to add additional functionality and writing simple algorithms.

Python 200 will dive deeper into topics such as more advanced algorithms and Object Oriented Programming. Secure coding techniques and methodologies will also be covered, including standard frameworks.

Python code will be utilized in other courses, such as Networking, Systems and Cryptography.

At the completion of this course, a student will be able to:

- Analyze Python scripts to determine what functionality they provide.
- Write simple Python scripts using conditionals, loops, variables and other data structures.
- Import modules to increase the functionality of the Python script.
- Use coding frameworks to ensure secure coding techniques are utilized.
- Address considerations for AI/ML/ChatGPT for secure coding.

APPLICATION SECURITY & PENETRATION TESTING

Application Security focuses on the applications and their vulnerabilities running on both workstations and servers. Penetration testing is using vulnerabilities either in applications or network resources that allows for exploitation. This can lead to server downtime, service interruptions or in the worst case, root level access for the malicious actor. This course focuses on methodologies utilized by penetration testers to analyze and assess risk to systems, networks, applications and other vulnerable areas of concern to a company. These are the same techniques used by malicious actors to compromise a company. The role of the penetration tester is critical in finding the vulnerabilities and risks before they can be exploited.

APP100 will focus on the basic techniques and tools employed by a penetration tester or hacker. The focus will be on the Penetration Testing Execution Standard (PTES) framework for determining where a company has exposure, testings the vulnerabilities, and basic approaches to exploiting the vulnerabilities. Additionally, network mapping will be revisited and specific techniques for reconnaissance will be discussed.

APP200 will look at specific exploits and how they can be utilized to more efficiently target and exploit systems and networks. The focus will be on crafting specific exploits based on the results of the reconnaissance techniques. Finally, post exploitation activities and reporting will be discussed.

At the completion of this course, a student will be able to:

- Describe the usage of Metasploit and other Kali Linux pentesting tools.
- Describe the Penetration Testing Execution Standard (PTES).
- Utilize attack tools to mount attacks against various types of networks and applications and use countermeasures to forestall these same attacks.

APPLIED CRYPTOGRAPHY

This course in Applied Cryptography teaches students the components of cryptography, provides hands-on experience on configuring a web server with SSL/TLS, and educates students in interfacing with Certificate Authorities, issuing certificates, configuring SSH securely, and sending/receiving encrypted and signed email.

In the 100 module students will be introduced to basic principles of encryption and authentication; additionally, students will understand and analyze historical approaches to cryptography. Students will practice symmetric cryptography, namely block ciphers, hash functions, and message authentication Codes.

The 200 module focuses on asymmetric cryptography (i.e. RSA and Diffie-Hellman Key Exchange). Combined with symmetric encryption, this makes a powerful combination for securing communications. Applications of these technologies will be explored by deploying SSL and SSH solutions. The 300 module covers anonymity and exploits using cryptography. Students explore weaknesses in WEP and SSL that lead vulnerabilities and discover how to counter them.

At the completion of this course, a student will be able to:

- Explain the fundamental goals of cryptography.
- Apply knowledge to use common crypto software.
- Analyze vulnerable applications with respect to cryptographic best practices.
- Create tools to attack and fix applications in a virtual lab environment.
- By the course's conclusion, students will have covered all relevant parts of the cryptography section of the industry-standard CISSP certification program.
- Identify how bad actors could leverage AI/ML/ChatGPT to crack encryption.

PHASE 5: CAPSTONE PROJECT

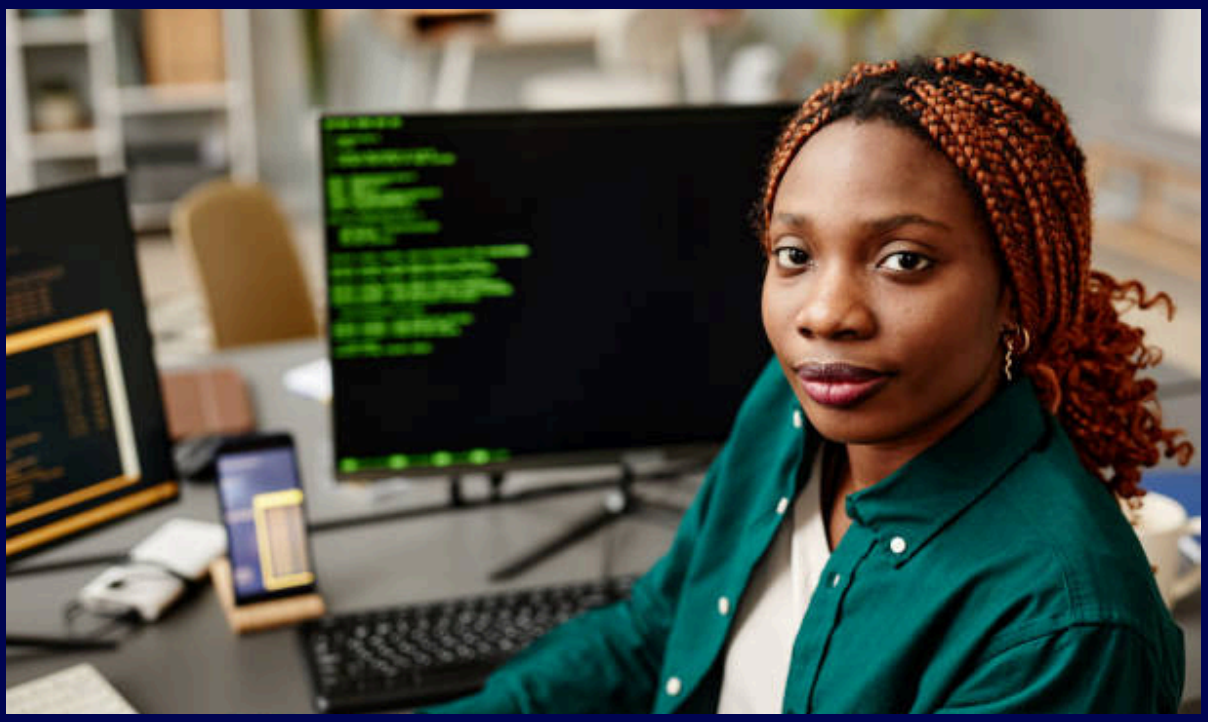
The scenario-based capstone activity allows the student to demonstrate their knowledge and proficiency. The group project will present a scenario and allow the students to work within their individual expertise to work through the particulars. Very little guidance will be given, allowing the students to work along multiple paths to completion. The project will culminate in a professional level oral and written report, which can be used as part of a portfolio.

At the completion of this course, a student will be able to:

- Apply the knowledge from all previous courses to analyze a scenario, for example by performing risk assessments or other security analysis.
- Utilize the knowledge from all previous courses to recommend best practice approaches to improve security posture in the scenario.
- Utilize the knowledge and skills from all previous courses to implement appropriate security controls and countermeasures in the scenario.
- Demonstrate decision-making, compliance, strategy development and professional communications through oral and written reports designed to support and make recommendations to senior management.

QUESTIONS? CONTACT US.

At Akademi, we're committed to helping you learn the skills to start or elevate your career. Contact us for any additional information about the Cybersecurity Engineering Bootcamp.



Akademi

www.myakademi.co
info@myakademi.co