FLORIDA ATLANTIC UNIVERSITY
CENTER FOR ONLINE AND CONTINUING EDUCATION

Cybersecurity Bootcamp

Florida Atlantic University Cybersecurity Bootcamp not only equips you with the necessary skills, but also prepares you to earn in-demand and globally accepted cybersecurity certifications. This bootcamp is designed to be flexible, allowing students with full-time careers to enroll and start their journey to becoming well rounded cybersecurity experts

Bootcamp Curriculum Overview

The Cybersecurity bootcamp program is an immersive and accelerated training with a focus on creating the next generation of cybersecurity professionals. You will attend courses, do hands on labs and apply your learning to successfully complete projects that address different cybersecurity topics. You will interact with experts who guide you throughout the bootcamp program, answer questions, and help with labs and project. The bootcamp will end with a capstone project where you will apply your learnings to real-life cybersecurity challenges.

This is a 28 weeks program and students are expected to spend 15 to 25 hours a week to master the material. Graduates of this program will learn critical skills for different cybersecurity careers and will have access to career services throughout the program.

Skills You Will Gain

This bootcamp covers following networking and cybersecurity areas:

Computer/Systems Fundamentals	**Networking**	**Cybersecurity**	**Security Analyst**
Hardware Architecture	Network Management / Troubleshooting	System / Network Security	Managing and Remediating Vulnerabilities
Operating System (Windows, Linux, Cisco)	WAN	Security Threats (Social Engineering & Malware)	Security and Software Development
Troubleshooting	Visualization Techniques	Vulnerability Assessment	Incidence Response
	TCP/IP	Identity and Assess Management	Forensic Tools
	Scanning / Sniffing (Wireshark Nmap etc.)	Cryptography	Cloud Security Tools

Penetration Testing	Ethical Hacking	Scripting
OS Vulnerabilities Exploitation	Footprinting	Python
Multi-level Pivoting	Reconnaissance	Hacking
SQL Injection	Networks Scanning	Automation
Host-Based Application Exploits	Enumeration	Tooling
XSFR	Session Hijacking	Shell Scripting
	Hacking Web Application	Data Analysis
	IoT Hacking	

Certifications You'll be Prepared for:

This bootcamp will cover the material needed for following certifications:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA CySA+
- Certified Ethical Hacking
- CompTIA Pentest+

During the bootcamp, you will work with your Career Counselor and Mentor to develop specific certification exams that you should take and additional activities you need to do to pass those certifications. We don't anticipate our students to take all these exams during the bootcamp

How Will We Help You Succeed?

As you learn new things to get on your way to learning about Cybersecurity, we will make sure that you have all the support throughout the entire journey to answer all your questions and get you fully prepared for the next stage in your career. Following are some of the support services that will ensure you're successful.

- Official University Certification
- Access to Expert Mentors
- Career Counselling
- Portfolio Building
- Real World Learning
- Job Opportunities

Career Opportunities:

Graduates of the bootcamp will learn critical skills needed for following careers:

- Cybersecurity Specialist
- Penetration Tester
- Incident Response Analyst
- Desktop/Network Support Specialist
- Network/System Security Administrator
- Cyber Network Defender
- Information Assurance Specialist
- Vulnerability Assessment Analyst
- Digital Forensics Examiner
- Cybersecurity Operations Specialist
- Secure Coding Specialist
- Forensic Computer Analyst
- Security Systems Administrator
- IT Security Consultant

Who Should Attend?

- You are happy in your current field but want to move to another company—or stay put but shift from a non-technical into a technical position.
- You are looking to understand the implications of cyber and information security on the technology and overall business operations.
- You are looking for a career in Cybersecurity or looking to change your careers to Cybersecurity.
- You want to engage more deeply with your current job—or boost your earnings and broaden your experience with freelance work.
- You have an entrepreneurial idea and need to acquire the skills to go “all in” on it and launch your business.
- You’re a full-time student but hungry to learn more and expand your skill set.
- You need to have at least an associate degree and commitment to work 15 to 25 hours a week over next 6 months to earn these skills

Course Structure

Over the course of 28 weeks, you’ll attend informative lectures, do hands-on labs. Apply your learning to real life projects. The goal is to give you a comprehensive learning experience and true insight into a “day in the life” of a cybersecurity specialist.

See “Course Outline” section and follow as your guide to completing courses in order.

Discussions by Instructors

Live Instructor-led discussions throughout your self-paced guides you through the entire program and provides you opportunity to ask questions and get help. To take this a step further, you will have access to the instructors throughout the program through over mentoring and discussions forum. This way, help is always available for you to succeed.

See “Mentoring & Discussions” section for how to connect with your mentor.

Labs

You'll put whatever you learn into practice by doing hands-on labs. You will be provided access to virtual environments where you can practice what you learnt in a safe environment.

See "Course Outline" section on how to access labs during the course.

Projects & Capstone Project

Your portfolio signals to employers that you are ready for primetime! You'll build a substantial portfolio of projects that demonstrate your abilities across a wide variety of technologies. Throughout the bootcamp you will be asked to do these projects.

Once finished with the bootcamp, you will work independently on set of final capstone projects. The skills you learn during this project will truly help you to prepare for your first interviews and jobs! The skills you need to complete this project will be everything you have learned from this bootcamp. We encourage students to come-up with their own Capstone projects, if you, you must meet certain objectives provided by your mentor.

See "Course Outline" section on project assignments and capstone project.

Career Counseling

You will have access to our career counselor (up to four, 30-minute sessions) who will help you with resume writing, linked profile, mock interviews and other ways to market yourself. We'll help you showcase your projects to potential employers and work with you to find you internships during the program.

Mentoring & Discussions

Coach will give 4 quality hours every week in the form of ATLEAST 2 LIVE sessions 6pm to 8pm CST. Days of the week TBD (To Be Determined) after initial Kick-Off Session and consultation with coach and cohort. Either **Mondays & Wednesdays** or **Tuesdays & Thursdays**.

You'll have access to a dedicated bootcamp discussion forum to collaborate and seek help from industry experts and other students.

Q&A Session* - Bring all your questions you may have and get the answers you're looking for. **Review Session*** - During this session, we will review the previous weeks work, what is expected the following week, and any other questions you may have that need answers.

** Actual duration of sessions can be reduced based on student participation*

Please read important information below on connecting with mentor.

Zoom Sessions - You will be provided a specific link issued to the class for attending the weekly sessions 3 to 4 days prior to the Cohort start date. Using this link, you can connect to Zoom and interact with instructors. You can also use the following link to join by placing in your assigned Meeting ID

https://www.zoom.us/join

Course Outline

Following is approximate course outline. Actual course may slightly vary based on course cohort performance. Choose between Security Analyst+ Ethical Hacking track or Ethical Hacking+ PenTesting Track

Courses	Duration - Track Security Analyst + Ethical Hacking	Duration - Track Ethical Hacking + PenTesting
Hardware and Operating System fundamentals	2 Weeks	
Networking Fundamentals	2 Weeks	
Security Fundamentals	3 Weeks	
Project A	2 Weeks	
Python - Introduction	2 Weeks	
Project B	1 Week	
Security Analyst		
Ethical Hacking	4 Weeks	
Penetration Testing		3 Weeks
Project C	2 Weeks	
Project D		2 Weeks
Capstone Project	3 Weeks	

Course Labs

IMPORTANT - PLEASE READ:

Labs are an interactive experience where you access remote environments and participate in coding exercises, development scenarios, and hands-on training in a remote desktop scenario. Reach out to
your **Customer Success Manager** to schedule and create your lab for this course.

Sample Project 1 - High Level Definition

Sample Project 1 focuses on first four weeks of learning acquired by student in this bootcamp. These initial four weeks of this cybersecurity bootcamp target mostly Networking, Operating Systems, and Hardware domains. Spending 20 hours (one week) on this project will ensure that student has got opportunity to validate all the knowledge, skills and learning obtained during first four weeks of lectures and labs. This project will challenge student's understanding acquired during lectures/labs and provide a way for him/her to work independently and gain confidence over his/her practical skills. This learning will result in student's success in professional/real-world corporate environment and make him/her prepare for various professional roles and ready for smooth entry in a fast paced technically challenging work environment where technical skills are valued and appreciated.

Overview

For entry-level roles (or even experienced roles) like Network Technician / Network Admins / Help- Desk staff, it is often necessary to troubleshoot in order to resolve day to day operational issues and be sure about the health of the network is up to mark. Sample Project 1 helps students to learn various things including the use of command line utilities which are offered by various Operating Systems to provide important network specific information. Sample Project 1 also indirectly validates that student can work on Linux, Network Sniffers, Port Scanning tools, Cabling, and Network appliances. A bonus assignment will give opportunity to students to learn configuring a vendor-specific industry-based network appliance using various Operating Systems.

Tasks

5 practical tasks along with a bonus task.

Allotted Duration

1 Week (20 hours)

Learning Objectives

- Get comfortable in installation and operation of Linux Operating System
- Become proficient in usage of network sniffer like WireShark and observe network traffic
- Learn the use of Port Scanning tool (Nmap) and detecting vulnerabilities
- Gain exposure of working on a vendor specific network appliance (firewall) along with its con- figuration and settings.
- Acquire necessary skills and knowledge for smooth entry into highly technical workforce environment.

Tools/Skills

WireShark (Sniffing), Linux Operating System, Nmap, Cisco Firewall, Hypervisor, Virtual Machines, Access Control Lists, Command Line Utilities, Various networking protocols, Router/Switch configuration and others.

Resources and Guidance

Resources/tools are supplied and advised by QuickStart where necessary. Consultation/guidance of an industry expert will be available during scheduled hours.

Sample Project 2 - High Level Definition

Sample Project 2 focuses on two weeks of intense learning in security domain acquired by student in this bootcamp. These two weeks of this cybersecurity bootcamp target only Security concepts for a novice. Spending 20 hours (one week) on this project will ensure that student has got opportunity to validate all the knowledge, skills and learning obtained during two weeks of lectures and labs. This project will challenge student's understanding acquired during lectures/labs and provide a way for him/her to work independently and gain confidence over his/her practical skills. This learning will result in student's success in professional/real-world corporate environment and make him/her prepare for various professional roles and ready for smooth entry in a fast paced technically challenging work environment where technical skills are valued and appreciated.

Overview

Sample Project 2 helps students to learn and develop concepts in security domain. It includes working with forensic tools, dealing with incidents, securing organization network by addressing vulnerabilities and dealing with threats, awareness on software security during development process, Denial of Service attacks and usage of Intrusion Detection System. Sample Project 2 also indirectly validates that student can work on Linux, Network Sniffers, Port Scanning tools, IDS, Network appliances, Hping3 and others, Practical assignment will give opportunity to students to learn conducting DoS attacks and install/configure an Intrusion Detection System.

Tasks

6 Tasks (four theoretical plus two hands-on)

Allotted Duration

1 Week (20 hours)

Learning Objectives

- Learn installation and operation of Intrusion Detection System.
- Become proficient in use of Hping3 tools and see how Denial of Service attacks are carried out and how to protect your network.
- Gain exposure to forensic tools and their usage.
- Familiar with Incident Response process and practices.
- Learn addressing vulnerabilities and threats to your network and making your network se- cure.
- Practices to adopt for developing a secure software.

Tools/Skills

Hping3 (various versions), IDS (Snort), Network Sniffer (WireShark), Linux O/S, Nmap, Virtual Machines, various networking protocols, DoS, Incident Response, Forensic Tools, DLP, Integrity, Secure Coding Practices and others.

Resources and Guidance

Resources/tools are supplied and advised by QuickStart where necessary. Consultation/guidance of an industry expert will be available during scheduled hours.

Sample Project 3 - High Level Definition

Sample Project 3 focuses on two weeks of past intense learning in cybersecurity domain acquired by student during bootcamp. These two weeks of this cybersecurity bootcamp target only Cybersecurity concepts. Spending 20 hours (one week) on this project will ensure that student has got opportunity to validate all the knowledge, skills and learning obtained during two weeks of lectures and labs. This project will challenge student's understanding acquired during lectures/ labs and provide a way for him/her to work independently and gain confidence over his/her practical skills. This learning will result in student's success in professional/real-world corporate environment and make him/her prepare for various professional roles and ready for smooth entry in a fast paced technically challenging work environment where technical skills are valued and appreciated.

Overview

Sample Project 3 helps students to learn and develop concepts in cybersecurity domain. It includes learning Disaster Recovery Planning, identifying and evaluating security risks present in your organization network/infrastructure, dealing with changing and implementing change management process, and gaining awareness on various access control models. Sample Project 3 also indirectly validates that student can understand the importance of security policies and procedures, risk management, authentication and authorization methods, and cloud security.

Tasks

4 Tasks

Allotted Duration

1 Week (20 hours)

Learning Objectives

- Understand Disaster Recovery Planning and how to mitigate disasters.
- Understand and evaluate risks present in your environment and using risk management process to address them.
- Gain exposure to dealing with change by using change management process.
- Observe various access control models and learn their practical implementation.

Tools/Skills

Access Control Models, Identity Management, AAA server, Incident Management, Disaster Recovery, Change Management, Cloud Security and others.

Resources and Guidance

Resources/tools are supplied and advised by QuickStart where necessary. Consultation/guidance of an industry expert will be available during scheduled hours.

Sample Project 4 - High Level Definition

Sample Project 4 focuses on six weeks of intense learning in security domain acquired by student in this bootcamp with emphasis on hacking and Pen Testing. These six weeks of cybersecurity bootcamp target specific security skills on ethical hacking and simulated attacks. Spending 40 hours (two weeks) on this project will ensure that student has got opportunity to validate all the knowledge, skills and learning obtained during past six weeks of lectures and labs. This project will challenge student's understanding acquired during lectures/labs and provide a way for him/ her to work independently and gain confidence over his/her practical skills. This learning will result in student's success in professional/real-world corporate environment and make him/her prepare for various professional roles and ready for smooth entry in a fast paced technically challenging work environment where technical skills are valued and appreciated.

Overview

Sample Project 4 helps students to learn and develop concepts in system hacking and pen testing. It includes working with system hacking tools, simulated attacks, IoT threats, social engineering attack methods and SQL Injection attacks. Sample Project 4 also indirectly validates that student is capable to work on Linux, Network Sniffers, Port Scanning tools, Network security appliances, Burpsuite, Website Footprinting, Maltego and other tools, Practical assignment will give opportunity to students to learn conducting foot printing and Ping Sweep.

Tasks

6 Tasks (four theoretical plus two hands-on)

Allotted Duration

2 Weeks (40 hours)

Learning Objectives

- Learn installation and operation of Footprinting tools.
- Become proficient in usage of various tools and software including Maltego, Ping Sweep, Burp- suite and others.
- Gain exposure to complete hacking process and practices.
- Get familiar with IoT threats.
- Learn negotiating various types of Social Engineering attacks.
- Practices to adopt for avoiding database specific SQL Injection attacks.

Tools/Skills

SQL Injection attacks, Footprinting, Maltego, Burpsuite, Ping Sweep, Network Sniffer (WireShark), Linux O/S, Nmap, Virtual Machines, various networking protocols and others.

Resources and Guidance

Resources/tools are supplied and advised where necessary. Consultation/guidance of an industry expert will be available during scheduled hours.

*Subject to change / revision based on student progress & input, mentors input based on market needs.