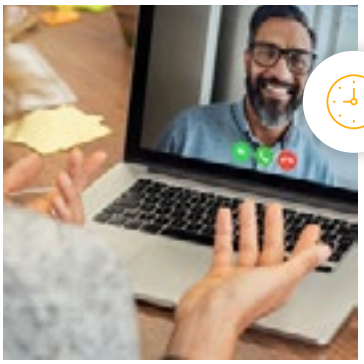
UDACITY

NANODEGREE PROGRAM SYLLABUS

Ethical Hacker

Overview

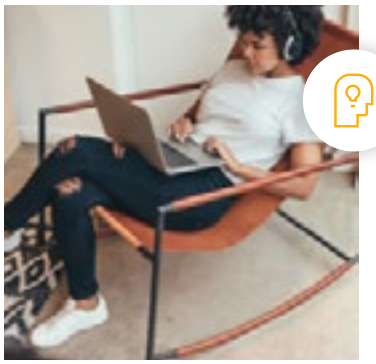
This program will equip students with the skills they need to advance in their security career and become an ethical hacker or penetration tester. Offensive security professionals in these roles play a critical role in any organization. Students will learn how to find and exploit vulnerabilities and weaknesses in various systems, design and execute a penetration testing plan, and report on findings using evidence from the project.



Estimated Time:
2 Months at
10hrs/week

Prerequisites:

- Basic Linux file structure
- Networking basics
- Three-way handshake, encryption and hashing
- One programming language (Python is preferred)



Flexible Learning:
Self-paced, so you can learn on the schedule that works best for you.

Need Help?
udacity.com/advisor
Discuss this program with an enrollment advisor.

Course 1: Intro to Ethical Hacking

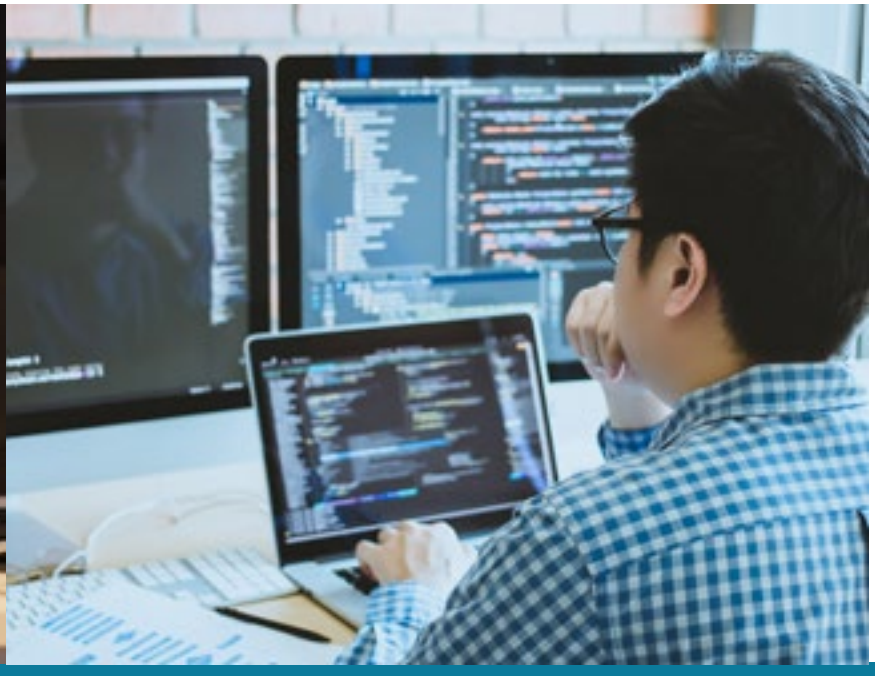
The purpose of this course is to introduce students to the broad set of techniques and job responsibilities associated with the role of an Ethical Hacker. Ethical Hackers leverage their knowledge of business' processes to evaluate risks while protecting core operations. The results of an Ethical Hacker's efforts are improvements to business policies, procedures and standards of conduct on its computer systems.

Course Project :
Audit ExampleCorp

In this project, you will manage a full-fledged security audit of a fictitious company called ExampleCorp. This project requires practical knowledge of all major elements of ethical hacking, including vulnerability management, hacking systems and applications, social engineering, and open-source intelligence. You will demonstrate vulnerability chaining, modification of exploit code, using documentation to learn new tests, and effective report writing.

		LEARNING OUTCOMES
LESSON ONE	**Vulnerability Management**	• Configure, launch and manage vulnerability scans • Calculate risk scores and assign risk ratings • Prioritize vulnerabilities and manage response efforts
LESSON TWO	**System Auditing**	• Interpret test scopes to conduct assessments • Perform information gathering • Research vulnerabilities and validate the exploits • Write a report to communicate audit results
LESSON THREE	**Application Auditing**	• Audit web applications using OWASP WSTG • Use semi-automated tools to increase efficiency and accuracy • Use fully-automated tools to test specific vulnerabilities and products

		LEARNING OUTCOMES
LESSON FOUR	**Social Engineering**	• Understand techniques attackers use to exploit employees • Conduct a phishing simulation • Create malware to use in test attacks • Design a simulated landing page to use in social engineering tests
LESSON FIVE	**Open-source Intelligence**	• Uncover information leakage • Use exploratory link analysis to find information and establish links • Analyze data relationships to develop conclusions



Course 2: Penetration Testing & Red Teaming Operations

The purpose of this course is to take a deep dive into the specific technique of penetration testing and how it can be used to perform a cybersecurity assessment on a specific system and conducted as a part of a specific penetration testing project within an organization to identify vulnerabilities, flaws and risks.

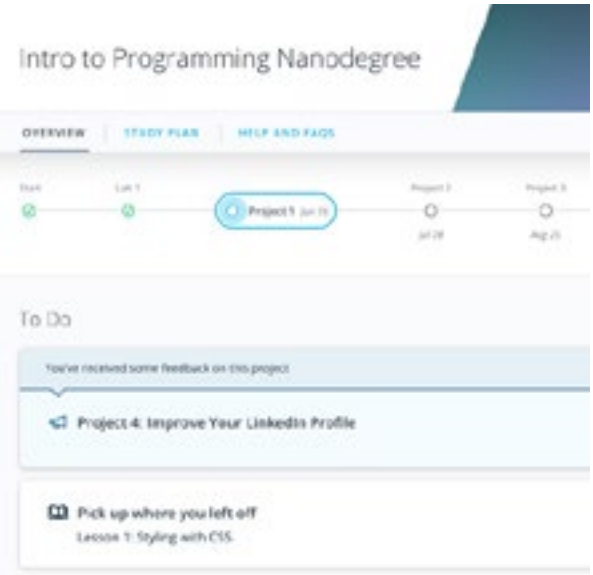
Course Project:
Red Teaming Operations

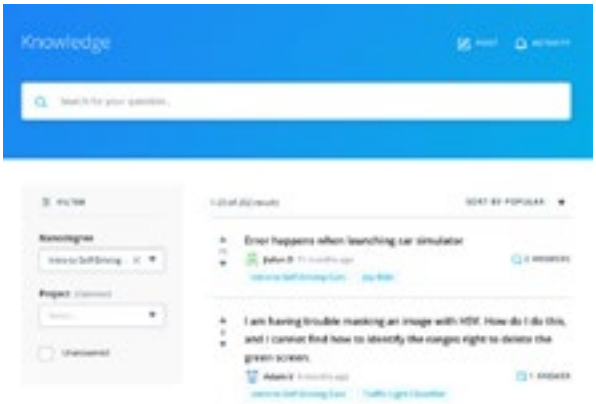
In this project, you will utilize and implement modern penetration tester and red teamer methodologies on PJBank CISO's virtual operations. You will demonstrate your ability to use all the skills you learned throughout the course while maintaining clear and concise documentation and testing efforts to generate a report in a timely fashion. The reporting process will demonstrate your understanding of business applications of security testing.

		LEARNING OUTCOMES
LESSON ONE	**Reconnaissance**	• Identify the appropriate tool for a given phase of reconnaissance • Identify IP addresses belonging to a company using public DNS • Identify various web frameworks and content management systems • Conduct passive, active and physical reconnaissance • Document the discovery, mapping and reconnaissance phase of red teaming
LESSON TWO	**Scanning & Research**	• Use common tools for network service scanning to map open ports, network services and associated versions • Extend the basic web application scanning to grab banners and find vulnerabilities in available services • Capture command usage, explain the usage, and provide results with screenshots and findings • Use software version discoveries to find common vulnerabilities and exposures (CVEs), MAP CVE to available exploit code • Identify the appropriate database to conduct vulnerability research

	LEARNING OUTCOMES	
LESSON THREE	**Gaining Access**	• Use Python, SQL query and other languages to run exploit code • Conduct web application and on-premise software attacks • Conduct password attacks • Conduct phishing and social engineering attacks • Exploit software vulnerabilities
LESSON FOUR	**Maintaining Access**	• Learn advanced persistent threat techniques • Maintain access through persistent connection • Traverse subnets by pivoting • Avoid IPS by obfuscating backdoor connection • Uncover root account passwords and conduct privilege escalation
LESSON FIVE	**Cover Tracks & Reporting**	• Learn techniques on covering tracks after exploitation • Clear logs on Windows and Linux targets • Deploy toolkits to automate log clearing • Assess digital footprints on the network and remove or hide them • Draft and update a pen test report • Draft non-technical executive summaries

Our Classroom Experience





REAL-WORLD PROJECTS

Build your skills through industry-relevant projects. Get personalized feedback from our network of 900+ project reviewers. Our simple interface makes it easy to submit your projects as often as you need and receive unlimited feedback on your work.

KNOWLEDGE

Find answers to your questions with Knowledge, our proprietary wiki. Search questions asked by other students and discover in real-time how to solve the challenges that you encounter.

STUDENT HUB

Leverage the power of community through a simple, yet powerful chat interface built within the classroom. Use Student Hub to connect with your technical mentor and fellow students in your Nanodegree program.

WORKSPACES

See your code in action. Check the output and quality of your code by running them on workspaces that are a part of our classroom.

QUIZZES

Check your understanding of concepts learned in the program by answering simple and auto-graded quizzes. Easily go back to the lessons to brush up on concepts anytime you get an answer wrong.

CUSTOM STUDY PLANS

Work with a mentor to create a custom study plan to suit your personal needs. Use this plan to keep track of your progress toward your goal.

PROGRESS TRACKER

Stay on track to complete your Nanodegree program with useful milestone reminders.

Learn with the Best

Sagar Bansal

CHAIRMAN AT BANSAL X

Sagar Bansal is a consultant, speaker and author in the information security industry. He helps large enterprises, governments and intelligence agencies reduce the cost of security by creating reliable and proactive security workflows.

Paul Oyelakin

FOUNDER OF PJ PROS

Paul Oyelakin is the founder of PJ Professional IT Services. He has experience in Security Compliance, Penetration Testing and Architecting Network Security Solutions for Private and Government. He has an MS in Cybersecurity, an MBA and is a Certified Ethical Hacker (CEH) & Information System Security Professional (CISSP).

All Our Nanodegree Programs Include:

EXPERIENCED PROJECT REVIEWERS

REVIEWER SERVICES

- Personalized feedback & line by line code reviews
- 1600+ Reviewers with a 4.85/5 average rating
- 3 hour average project review turnaround time
- Unlimited submissions and feedback loops
- Practical tips and industry best practices
- Additional suggested resources to improve

TECHNICAL MENTOR SUPPORT

MENTORSHIP SERVICES

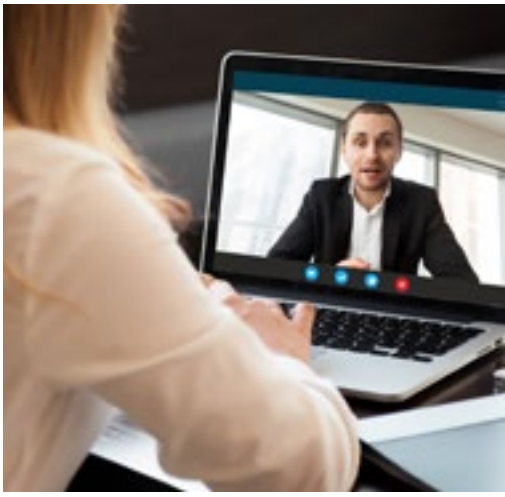
- Questions answered quickly by our team of technical mentors
- 1000+ Mentors with a 4.7/5 average rating
- Support for all your technical questions

PERSONAL CAREER SERVICES

CAREER SUPPORT

- Resume support
- Github portfolio review
- LinkedIn profile optimization

Frequently Asked Questions



PROGRAM OVERVIEW

WHY SHOULD I ENROLL?

The global cybersecurity market is currently worth $173B in 2020, growing to $270B by 2026. This program was designed to help you take advantage of the growing need for skilled ethical hackers. Prepare to meet the demand for cybersecurity professionals who are trained to play a critical role in protecting an organization's computer networks and systems.

WHAT JOBS WILL THIS PROGRAM PREPARE ME FOR?

The need for a strong computer security culture in an enterprise organization is greater than ever. The skills you will gain from this Nanodegree program will qualify you for jobs in several industries as countless companies are boosting security protocol.

HOW DO I KNOW IF THIS PROGRAM IS RIGHT FOR ME?

The course is for individuals who are looking to advance their cybersecurity careers with the cutting-edge skills to manage a security team and set themselves apart at work while wearing a white hat.

ENROLLMENT AND ADMISSION

DO I NEED TO APPLY? WHAT ARE THE ADMISSION CRITERIA?

No. This Nanodegree program accepts all applicants regardless of experience and specific background.

WHAT ARE THE PREREQUISITES FOR ENROLLMENT?

The Ethical Hacker Nanodegree Program is an advanced course. Learners should already have knowledge of:

- Basic Linux file structure and commands
- Networking basics (ports, IP addresses, subnetting)
- Three-way handshake, encryption and hashing
- One programming language (Python is preferred)
- Familiarity with Windows OS

IF I DO NOT MEET THE REQUIREMENTS TO ENROLL, WHAT SHOULD I DO?

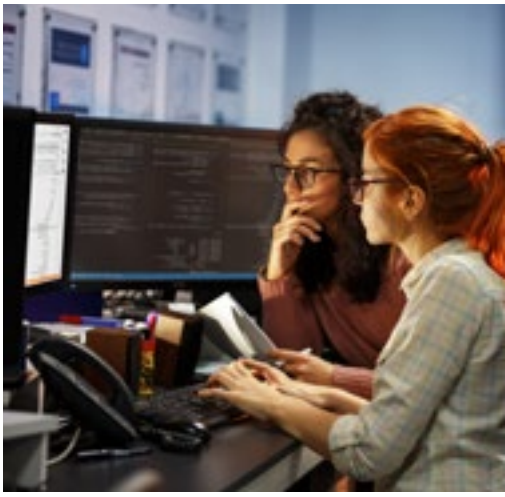
Students who do not feel comfortable in the above may consider taking Udacity's Introduction to Cybersecurity course to obtain prerequisite skills.

TUITION AND TERM OF PROGRAM

HOW IS THIS NANODEGREE PROGRAM STRUCTURED?

The Ethical Hacker Nanodegree program is comprised of content and curriculum to support 2 projects. We estimate that students can complete the program in four 2 months working 10 hours per week.

FAQs Continued



Each project will be reviewed by the Udacity reviewer network. Feedback will be provided and if you do not pass the project, you will be asked to resubmit the project until it passes.project until it passes.

HOW LONG IS THIS NANODEGREE PROGRAM?

Access to this Nanodegree program runs for the length of time specified above. If you do not graduate within that time period, you will continue learning with month to month payments. See the **Terms of Use** and **FAQs** for other policies regarding the terms of access to our Nanodegree programs.

SOFTWARE AND HARDWARE

WHAT SOFTWARE AND VERSIONS WILL I NEED IN THIS PROGRAM?

Software and hardware requirements include:

- Operating System - Windows, OSX, or Linux
- Processor - Minimum 2 GHz Speed with Virtualization and x64 support
- RAM - 8 GB DDR3 or Higher (16 GB DDR4 RAM is preferred)
- Storage - 100 GB Free Space (SSD is preferred over HDD)
- This program uses the Oracle VM VirtualBox hypervisor tool that is incompatible with Apple's new M1 chip computers