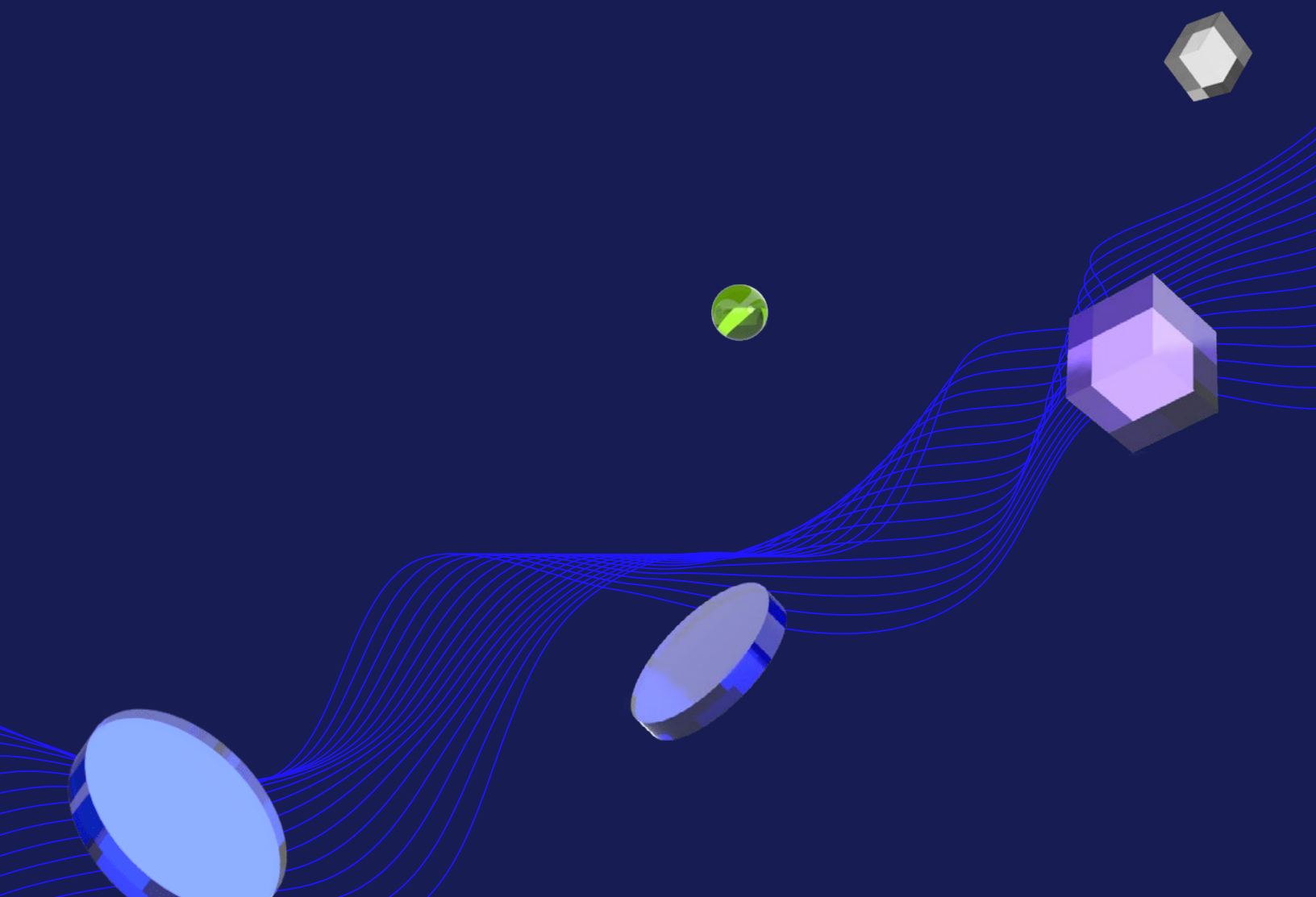
INDIVIDUAL LEARNERS

UDACITY

SCHOOL OF CYBERSECURITY

Ethical Hacker

Nanodegree Program Syllabus



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.

Learning Objectives

A graduate of this program will be able to:

- Manage the vulnerability lifecycle including scanning, analyzing, prioritizing, and managing risk.
- Perform security audits of internal systems, web applications, and information leakage.
- Manage security awareness programs and emulate attacks to demonstrate risk.
- Produce meaningful reports that detail findings, prioritize risk or criticality, and suggest mitigations.
- Perform stealthy reconnaissance against organizations to avoid potential tripwires.
- Scan systems and identify common security risks and oversights in best practices that can allow compromise.
- Investigate and research vulnerabilities in specific packages of software, identify applicable exploits, and “stand up” appropriate attack platforms (Python environment, web intercepting proxy, etc.).
- Perform exploitation using common tools and exploit code of identified vulnerabilities in open services.

Program information

Estimated Time

2 months at 10hrs/week*

Skill Level

Advanced

Prerequisites

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

Required Hardware/Software

Learners need access to:

- 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)

Note: This program uses the Oracle VM VirtualBox hypervisor tool that is incompatible with Apple's new M1 chip computers.

*The length of this program is an estimation of total hours the average student may take to complete all required coursework, including lecture and project time. If you spend about 5-10 hours per week working through the program, you should finish within the time provided. Actual hours may vary.

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, 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. Demonstrate vulnerability chaining, modification of exploit code, using documentation to learn new tests, and effective report writing.

Lesson 1

Vulnerability Management

- Configure, launch, and manage vulnerability scans.
- Calculate risk scores and assign risk ratings.
- Prioritize vulnerabilities and manage response efforts.

Lesson 2

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 3

Application Auditing

- Explain the benefits of utilizing the Bitcoin Core testnet.
- Describe the difference between the public testnet and regression testing.

Lesson 4

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 5

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, utilize and implement modern penetration tester and red teamer methodologies on PJBank CISO's virtual operations. Demonstrate the ability to use all the skills 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 one's understanding of business applications of security testing.

Lesson 1

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 2

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.

Lesson 3

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 4

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 5

Cover Tracks & Reporting

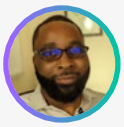
- Learn techniques on covering tracks after exploitation.
- Clear logs on Windows and Linux targets.
- Deploy toolkits to automate log clearing.
- Assess digital footprints on the network and remove or hide them.
- Draft and update a pen test report.
- Draft non-technical executive summaries.

Meet your instructors.

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.

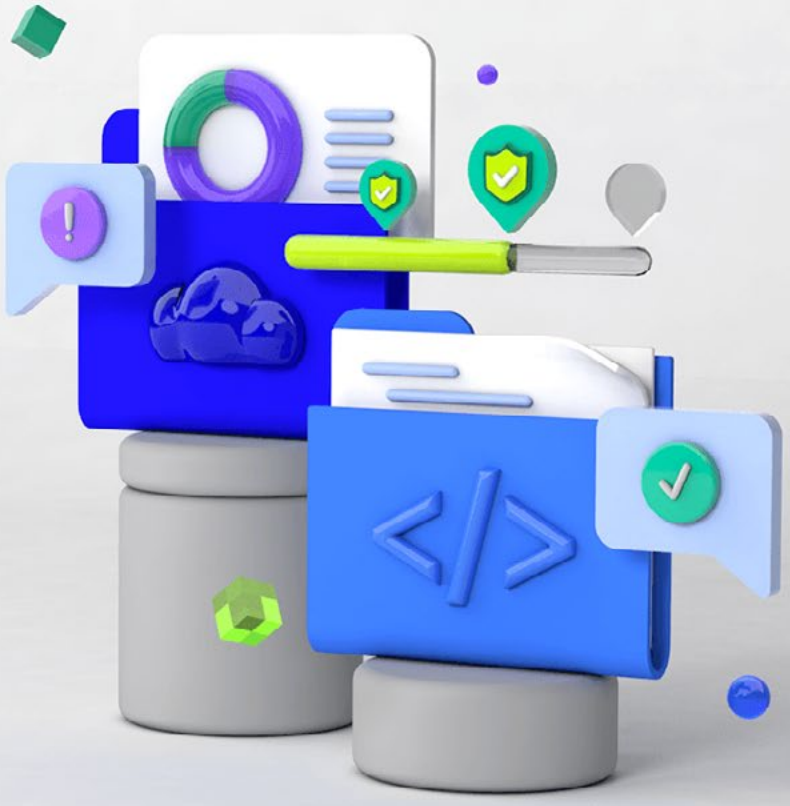


Paul Oyelakin

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) and Certified Information System Security Professional (CISSP).

Udacity's learning experience



Hands-on Projects

Open-ended, experiential projects are designed to reflect actual workplace challenges. They aren't just multiple choice questions or step-by-step guides, but instead require critical thinking.

Quizzes

Auto-graded quizzes strengthen comprehension. Learners can return to lessons at any time during the course to refresh concepts.

Knowledge

Find answers to your questions with Knowledge, our proprietary wiki. Search questions asked by other students, connect with technical mentors, and discover how to solve the challenges that you encounter.

Custom Study Plans

Create a personalized study plan that fits your individual needs. Utilize this plan to keep track of movement toward your overall goal.

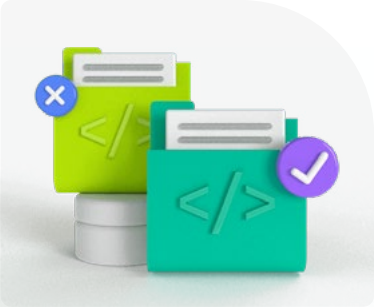
Workspaces

See your code in action. Check the output and quality of your code by running it on interactive workspaces that are integrated into the platform.

Progress Tracker

Take advantage of milestone reminders to stay on schedule and complete your program.

Our proven approach for building job-ready digital skills.



Experienced Project Reviewers

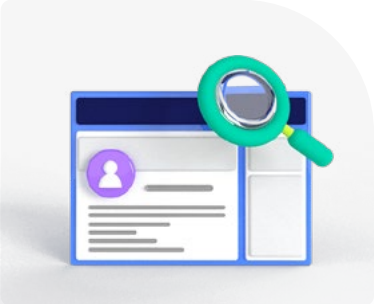
Verify skills mastery.

- Personalized project feedback and critique includes line-by-line code review from skilled practitioners with an average turnaround time of 1.1 hours.
- Project review cycle creates a feedback loop with multiple opportunities for improvement—until the concept is mastered.
- Project reviewers leverage industry best practices and provide pro tips.

Technical Mentor Support

24/7 support unblocks learning.

- Learning accelerates as skilled mentors identify areas of achievement and potential for growth.
- Unlimited access to mentors means help arrives when it's needed most.
- 2 hr or less average question response time assures that skills development stays on track.



Personal Career Services

Empower job-readiness.

- Access to a Github portfolio review that can give you an edge by highlighting your strengths, and demonstrating your value to employers.*
- Get help optimizing your LinkedIn and establishing your personal brand so your profile ranks higher in searches by recruiters and hiring managers.

Mentor Network

Highly vetted for effectiveness.

- Mentors must complete a 5-step hiring process to join Udacity's selective network.
- After passing an objective and situational assessment, mentors must demonstrate communication and behavioral fit for a mentorship role.
- Mentors work across more than 30 different industries and often complete a Nanodegree program themselves.

*Applies to select Nanodegree programs only.

UDACITY

Learn more at

www.udacity.com/online-learning-for-individuals →

12.16.22 | V1.0