

THE SCHOOL OF CYBERSECURITY

Ethical Hacker



Overview

Ethical Hacker Nanodegree Program

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.

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



TIME

2 months
Study 10 hours/week



LEVEL

Specialist



PREREQUISITES

- 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



HARDWARE/SOFTWARE REQUIRED

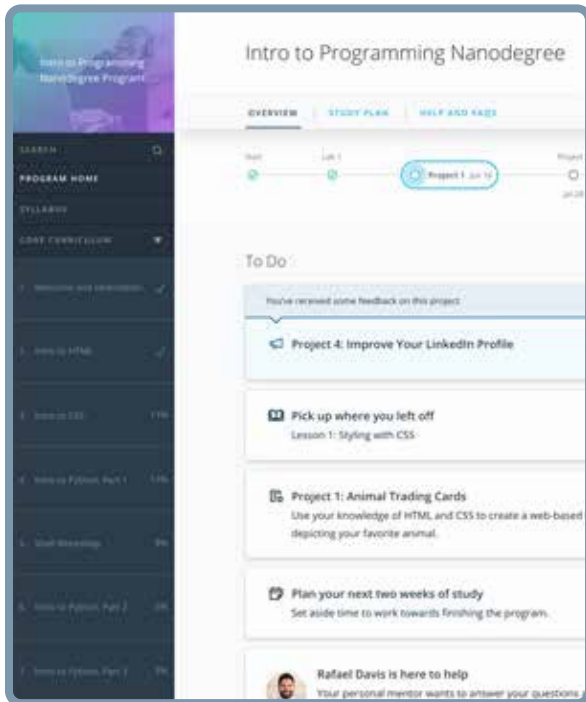
- Operating System - Windows, OSX, or Linux
- Processor—Minimum 2 GHz Speed with Virtualization and x64 support
- RAM - 8 GB DDR3 or Higher (16 GB DDR4 RAM is preferred)
- Storage—100 GB Free Space (SSD is preferred over HDD)



LEARN MORE ABOUT THIS NANODEGREE

Contact us at enterpriseNDs@udacity.com.

Our Classroom Experience



REAL-WORLD PROJECTS

Learners build new skills through industry-relevant projects and receive personalized feedback from our network of 900+ project reviewers. Our simple user interface makes it easy to submit projects as often as needed and receive unlimited feedback.

KNOWLEDGE

Answers to most questions can be found with Knowledge, our proprietary wiki. Learners can search questions asked by others and discover in real-time how to solve challenges.

LEARNER HUB

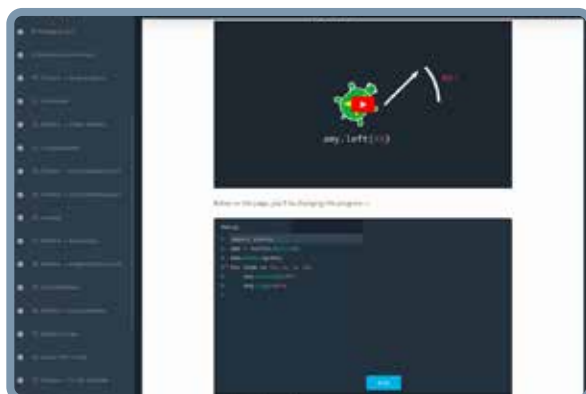
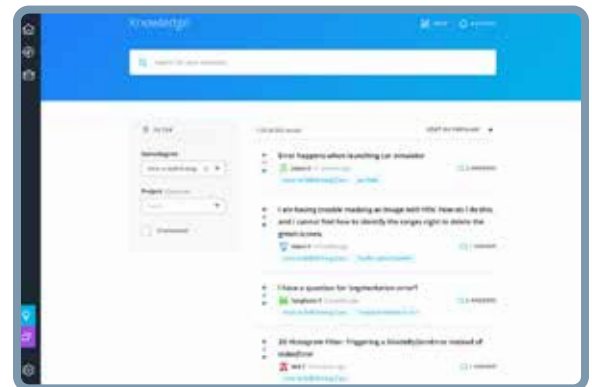
Learners leverage the power of community through a simple, yet powerful chat interface built within the classroom. Learner Hub connects learners with their technical mentor and fellow learners.

WORKSPACES

Learners can check the output and quality of their code by testing it on interactive workspaces that are integrated into the classroom.

QUIZZES

Understanding concepts learned during lessons is made simple with auto-graded quizzes. Learners can easily go back and brush up on concepts at anytime during the course.



CUSTOM STUDY PLANS

Mentors create a custom study plan tailored to learners' needs. This plan keeps track of progress toward learner goals.

PROGRESS TRACKER

Personalized milestone reminders help learners stay on track and focused as they work to complete their Nanodegree program.

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).



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.

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.

LESSON TITLE

LEARNING OUTCOMES

VULNERABILITY MANAGEMENT

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

SYSTEM AUDITING

- Interpret test scopes to conduct assessments
- Perform information gathering
- Research vulnerabilities and validate the exploits
- Write a report to communicate audit results

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

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
SOCIAL ENGINEERING	<ul style="list-style-type: none">• 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
OPEN-SOURCE INTELLIGENCE	<ul style="list-style-type: none">• 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.

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.

LESSON TITLE

LEARNING OUTCOMES

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

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

Nanodegree Program Overview

LESSON TITLE

LEARNING OUTCOMES

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

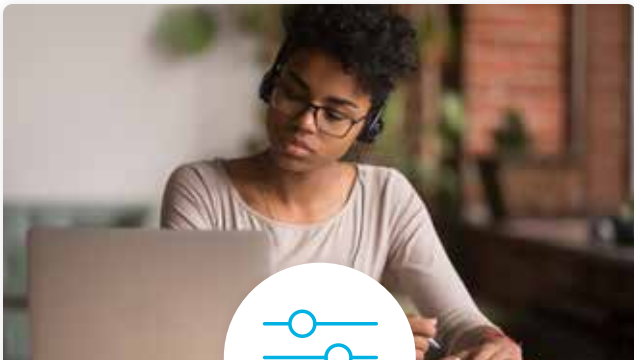
MAINTAINING ACCESS

- 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

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





Pre-Assessments

Our in-depth workforce assessments identify your team's current level of knowledge in key areas. Results are used to generate custom learning paths designed to equip your workforce with the most applicable skill sets.



Dashboard & Progress Reports

Our interactive dashboard (enterprise management console) allows administrators to manage employee onboarding, track course progress, perform bulk enrollments and more.



Industry Validation & Reviews

Learners' progress and subject knowledge is tested and validated by industry experts and leaders from our advisory board. These in-depth reviews ensure your teams have achieved competency.



Real World Hands-on Projects


Through a series of rigorous, real-world projects, your employees learn and apply new techniques, analyze results, and produce actionable insights. Project portfolios demonstrate learners' growing proficiency and subject mastery.

Our Review Process

Real-life Reviewers for Real-life Projects

Real-world projects are at the core of our Nanodegree programs because hands-on learning is the best way to master a new skill. Receiving relevant feedback from an industry expert is a critical part of that learning process, and infinitely more useful than that from peers or automated grading systems. Udacity has a network of over 900 experienced project reviewers who provide personalized and timely feedback to help all learners succeed.


All Learners Benefit From:




Line-by-line feedback for coding projects



Industry tips and best practices



Advice on additional resources to research



Unlimited submissions and feedback loops


How it Works

Real-world projects are integrated within the classroom experience, making for a seamless review process flow.


- Go through the lessons and work on the projects that follow
- Get help from your technical mentor, if needed
- Submit your project work
- Receive personalized feedback from the reviewer
- If the submission is not satisfactory, resubmit your project
- Continue submitting and receiving feedback from the reviewer until you successfully complete your project

About our Project Reviewers


Our expert project reviewers are evaluated against the highest standards and graded based on learners' progress. Here's how they measure up to ensure your success.



Expert Project Reviewers
Are hand-picked to provide detailed feedback on your project submissions.



Projects Reviewed
Our reviewers have extensive experience in guiding learners through their course projects.



Hours Average Turnaround
You can resubmit your project on the same day for additional feedback.



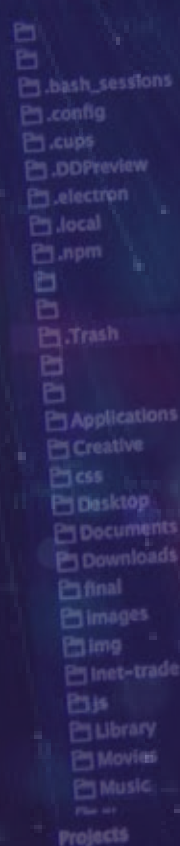
Average Reviewer Rating
Our learners love the quality of the feedback they receive from our experienced reviewers.



Vaibhav
UDACITY LEARNER

"I never felt overwhelmed while pursuing the Nanodegree program due to the valuable support of the reviewers, and now I am more confident in converting my ideas to reality."

now at
CODING VISIONS INFOTECH



```
php *
Users >
php
Gets the email message from the mailbox to add
post, Mailbox connec
configured under Settings > Writing
age.
bootstrap by continuing. */
10 /** @since 2.9.0 */
11 require_once( ABSPATH . WPINC . '/load.php' );
12
13 /** This filter is applied to the email configuration, true */
14 if ( ! apply_filters( 'wp_mail_configuration', true ) )
15     wp_die( __( 'This action has been disabled by the administrator.' ), 403 );
16
17 $mailserver_url = get_option( 'mailserver_url' );
18
19 if ( 'mail.example.com' === $mailserver_url || empty( $mailserver_url ) ) {
20     wp_die( __( 'This action has been disabled by the administrator.' ), 403 );
21 }
22
23 /**
24  * Fires to allow a plugin to do a complete takeover of Post by Email.
25  *
26  * @since 2.9.0
27  */
28 do_action( 'wp-mail.php' );
29
30 /** Get the POP3 class with which to access the mailbox. */
31 require_once( ABSPATH . WPINC . '/class-pop3.php' );
32
33 /** Only check at this interval for new messages. */
34 if ( ! defined( 'WP_MAIL_INTERVAL' ) )
35     define( 'WP_MAIL_INTERVAL', 300 ); // 5 minutes
36
37 $last_checked = get_transient( 'mailserver_last_checked' );
38
39 if ( ! $last_checked )
40     wp_die( __( 'Slow down cowboy, no need to check for new mails so often!' ) );
41
42 set_transient( 'mailserver_last_checked', true, WP_MAIL_INTERVAL );
43
44 $time_difference = get_option( 'gmt_offset' ) * HOUR_IN_SECONDS;
45
46 $phone_delim = '::';
47
48 $pop3 = new POP3();
```

UDACITY

FOR ENTERPRISE

Udacity © 2021

2440 W El Camino Real, #101
Mountain View, CA 94040, USA - HQ

For more information visit: www.udacity.com/enterprise