UDACITY
FOR ENTERPRISE

THE SCHOOL OF CYBERSECURITY

Security Engineer

NANODEGREE SYLLABUS

Overview

Security Engineer Nanodegree Program

In this program, you'll learn the foundational skills of security engineering and provide an overview of how security engineering is applied to various technology stacks. This program will focus on the unique skills needed to protect the computer systems, networks, applications and infrastructure of a company from security threats or attacks.

Program Information

TIME
4 months
Study 10 hours/week

LEVEL
Practitioner

PREREQUISITES
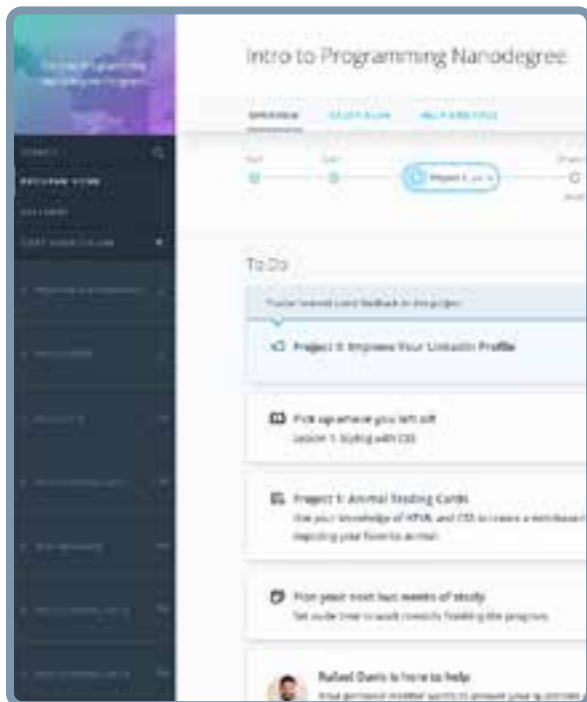Basics of Python, experience configuring AWS and Linux environments.

HARDWARE/SOFTWARE REQUIRED
Access to the internet and a 64-bit computer.

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.

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
Create a custom study plan to suit your personal needs and use this plan to keep track of your progress toward your goal.
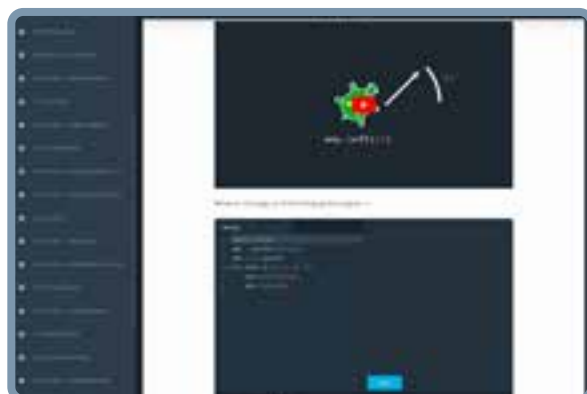
PROGRESS TRACKER
Personalized milestone reminders help learners stay on track and focused as they work to complete their Nanodegree program.

Learn with the Best

Taylor Lobb

HEAD OF INFORMATION SECURITY,
CLEARWATER ANALYTICS

Taylor is an information security leader with over 10 years experience building a wide range of security programs. Taylor is currently head of information security for Clearwater Analytics. Previously he was a leader in application security at Adobe.

Rod Soto

PRINCIPAL SECURITY RESEARCH
ENGINEER, SPLUNK

Rod has over 15 years of experience in information technology and security. He has worked at Prolexic, Akamai, Caspida, and Splunk. He is the co-founder of HackMiami and the Pacific Hackers meetup and conferences.

Dev Badlu

VP OF PRODUCT INNOVATION

Dev has worked in the cybersecurity field for more than 10 years, and is now VP of Product Innovation at one of the top cybersecurity companies. His area of expertise is red team and exploit development, with a focus on active cybersecurity defense.

Abhinav Singh

ENGINEER/CONSULTANT,
AMAZON WEB SERVICES

Abhinav is a cybersecurity researcher with nearly a decade of experience working for global leaders in security technology, financial institutions and as an independent consultant. He is the author of Metasploit Penetration Testing Cookbook and Instant Wireshark Starter, as well as many papers, articles, and blogs.

Course 1: Security Engineering Fundamentals

This course introduces the fundamental concepts and practices of security engineering. These are the basic principles and properties a security engineer will apply when evaluating, prioritizing and communicating security topics. Additionally, you'll learn about the practical applications of cryptography. You will also learn about strategies for risk evaluation, security review and audit.

Project	TimeSheets

Your company utilizes a custom application, called TimeSheets, to log timesheets. This custom application was built in-house. Until recently, this application was only accessible via the internal corporate network. Shortly after exposing TimeSheets externally, the IT and security operations teams began noticing odd behavior related to TimeSheets. IT has seen a significant amount of users reporting incorrect data in the system. The security operations center has noticed logins from unexpected locations and unexpected times. After raising an incident, it was determined that unauthorized logins were occurring.

After resolving the incident, your team was asked to come in and assess the application and provide recommendations. A senior security engineer from your team completed the initial threat model related to the incident. During the threat model, your colleague discovered the root cause for the incident as well as several other vulnerabilities — all of which are related to encryption. Due to other obligations, your colleague has asked you to complete their work.

LESSON TITLE	LEARNING OUTCOMES
WHAT IS SECURITY ENGINEERING?	· Understand common strategies used by offensive and defensive security teams · Identify and explain the discrete functions of security roles · Use resources in order to be up-to-date on security issues · Explain the difference between governance, compliance and privacy fields and how they relate to information security

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
SECURITY PRINCIPLES	• Define each element in the CIA triad and understand why they're important to information security • Define each element in Authentication, Authorization and Non-Repudiation and understand why they're important to information security • Explain OWASP and application of secure principles • Explain the role of a security engineer when it comes to defining security requirements • Explain the different pieces of security strategy, specifically policies and enforcement

PRACTICAL CRYPTOGRAPHY	• Understand how encryption in transit works and when to apply it
	• Understand conceptual and practical application of several common cryptographic techniques:
	  • Encryption
	  • Hashing
	  • Signing
	  • Authentication
	  • Certificates and Public Key Infrastructure

RISK EVALUATION	• Explain vulnerabilities, asset valuation and mitigation and how they relate to one another • Define and understand the process for threat modeling • Understand strategies for evaluating risk and assigning priority
SECURITY REVIEW AND AUDIT	• Explain the role of audit and how it relates to information security • Understand infrastructure and control audits • Understand design, code and architecture security reviews and when to utilize them • Know how to find and implement best practices and industry requirements • Create reports based on findings from security reviews

Course 2: System Security

In this course, you'll start by exploring the basics of system security and its implementation at the operating system level. You will learn about implementing authentication and authorization as a means to protect access to data and services. You will also learn about detecting unauthorized changes to a system and how to effectively counter them. By the end, you will understand how to build logging, monitoring and auditing tools that can alert you to system security breaches and how to effectively counter them in a real-world case.

Project	Responding to a Nation-State Cyber Attack

South Udan is a small island nation that is peaceful and technologically advanced. Its neighbor, North Udan, carries out a cyber attack on their nuclear reactor plant in order to disrupt their advanced research on generating clean energy by using Tridanium. Your task will be to implement the course learnings to investigate a Linux virtual image that was taken from the server that was compromised in the cyber espionage campaign carried out by North Udan. You will work towards identifying the infection chain along with assessing and improving the system's resilience against malicious attacks by building scanning, monitoring and auditing tools.

LESSON TITLE	LEARNING OUTCOMES
IDENTIFYING VULNERABILITIES	· Explore operating system's security model · Understand CVEs and third party advisory reports · Detect vulnerabilities in software and third-party libraries · Patch identified vulnerabilities
AUTHENTICATION	· Explore Unix password storage management and its security features · Defend remote service authentication mechanisms & server hardening principles · Implement encryption for data at rest and in motion

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
AUTHORIZATION	• Understand access controls and their implementation as a means for securing data • Explore ways to detect unauthorized services and processes and how to remediate them • Use networking features to prevent unauthorized access to the system or server
ISOLATION	• Learn how to implement a chroot jail enhance system security • Understand mandatory access control and how it differs from discretionary access control • Understand advanced attacks like buffer overflows
AUDITING	• Implement auditing controls on critical files and services • Implement host-based intrusion detection • Implement file integrity monitoring through osquery • Detect the presence of malware through system scans • Write YARA rules for advanced threat hunting

COURSE 3: Infrastructure Security

In this course, you will be introduced to the industry best practices for security configurations and controls. You will perform an assessment that includes security benchmarks, configurations and controls. You will also scan the main infrastructure operating systems for vulnerabilities and produce a report based on an industry scenario. At the end of this course, you will be familiar with industry terminology and security best practices. You will also learn to perform vulnerability scans and produce industry-standard reports.

Project	Adversarial Resilience: Assessing Infrastructure Security

StaticSpeeds company has recently been acquired by NuttyUtility. We need to decide if StaticSpeeds systems should be integrated into NuttyUtility's extended network and infrastructure. Your task will be to check CIS Benchmarks against Windows and Linux operating systems at StaticSpeeds. You will also need to perform a vulnerability scan using Nmap and produce a comprehensive report including all the required CIS Benchmark checks and vulnerabilities found in these systems. Finally, you will provide a recommendation based on your findings, and evaluate whether StaticSpeeds systems are ready to be integrated with the NuttyUtility extended network.

LESSON TITLE	LEARNING OUTCOMES
INFRASTRUCTURE SECURITY ASSESSMENT	· Identify the importance of asset management · Recognize shadow IT and BYOD risks · Identify the importance of system & third-party updates · Perform software inventory · Define a golden image · Identify industry security frameworks · Apply security framework to hardware and software assets

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
ACCESS MANAGMENT	· Identify the importance of firewalls & access control lists · Apply firewall, ACL-applicable best practices · Implement VLANs & network segmentation · Identify web application vulnerabilities · Use WAF to protect web applications · Apply Microsoft networks domain isolation & IPSec policies · Implement remote access management · Identify IPv6 risks & vulnerabilities · Protect access to the perimeter
MONITORING & DETECTION	· Identify the importance of network monitoring · Use Wireshark and tcpdump for packet analysis · Implement best practices for Windows event logs · Monitor activity with Windows Sysmon, Syslog and Linux auditing · Understand the importance of endpoint security and monitoring · Identify and implement centralized logging best practices · Assess the need for a SIEM · Apply adversarial simulation
IDENTITY ACCESS MANAGEMENT	· Apply principle of least privilege · Apply segregation of duties · Identify suitable Access Control Models (RBAC, MAC) · Audit access and permissions · Identify and apply best practices to service-to-service communication and encryption · Implement enterprise key and certificate management · Implement best practices in credential managers · Audit password policy · Implement multi-factor authentication · Mitigate third-party risk

LESSON TITLE	LEARNING OUTCOMES

TOP SECURITY FAILURES	· Utilize Nmap for discovery of network hosts
	· Implement Nmap best practices for vulnerability discovery
	· Implement vulnerability management
	· Utilize backup best practices
	· Recommend and implement a disaster recovery plan
	· Identify and recommend mitigations for:
	  • Exposed services, unnecessary accounts, excessive permissions
	  • Denial-of-services protocols
	  • Unpatched services
	  • Weaknesses in ciphers

COURSE 4: Application Security

In this course, you will learn the basics of secure web application. You will start by learning about OWASP and the Top 10 list of vulnerabilities within web applications. You will also learn how to do Static code scans using special software and even how to manually test a web application. By the end of this course you will be able to work as a security expert that can help shape the security posture of the development team to help build more security web applications.

Project	>	Vulnerable Web Application

You have been hired by a startup company, USociety, who has received reports from the well known hacker group fcity that their customer data was breached. They need you to identify how the attackers got into their system, extracted all of their customers data, and any other security holes that their application might have. This security audit is considered the highest priority for the company and they need your help.

You will need to review some static code to help identify and prioritize all vulnerabilities and help create recommendations on how best to mitigate these vulnerabilities. You will also need to manually test the vulnerable web application to find all vulnerabilities and create a writeup documentation to help the development team patch the code. The writeup documentation clearly outlines the steps needed to reproduce the security issue and best practices to help the development team better understand the issue.

| LESSON TITLE	LEARNING OUTCOMES
COMMON WEB APPLICATION VULNERABILITIES	· Learn about OWASP organization · The history behind OWASP Top 10 list · Overview of each of the OWASP Top 10 items · Best Practice to mitigate each item in the OWASP Top 10

Nanodegree Program Overview

LESSON TITLE	LEARNING OUTCOMES
WEB PENETRATION TESTING	· You will learn how to do basic reconnaissance · How to simulate different attack vectors · How to Brute Force login a web application · Go over hashes and how to use them · Look at how to perform hash lookup
DISCOVERY METHODOLOGIES	· Learn about Static Application Security Test (SAST) · Perform SAST on test code · Learn to read a SAST report · Prioritization of Vulnerabilities using Risk Factor Calculation · Best Practice for Vulnerabilities
VULNERABILTITY RESPONSE	· Learn how to write a Vulnerability Report · Go through how to write a Walk Through for Vulnerabilities · Set Severity for the Vulnerabilities using Common Vulnerability Scoring System (CVSS) v3.1
MITIGATION AND VERIFICATION	· Learn about Software Development Life Cycle (SDLC) · How to modify the SDLC to incorporate Security testing · Work with both Development and QA to improve security posture

Our Nanodegree Programs Include:
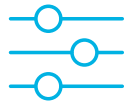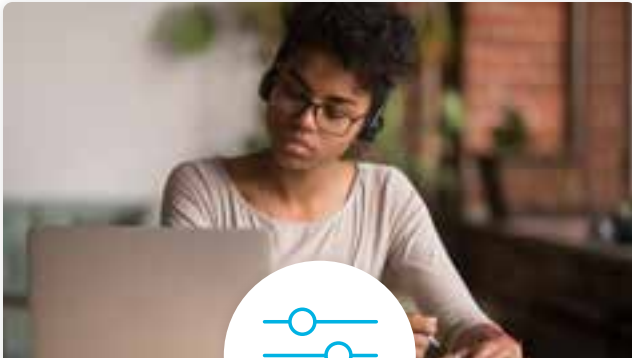
Pre-Assessments

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.

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

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.

900+	1.8M	3	4.85 /5
Expert Project Reviewers	**Projects Reviewed**	**Hours Average Turnaround**	**Average Reviewer Rating**
Are hand-picked to provide detailed feedback on your project submissions.	Our reviewers have extensive experience in guiding learners through their course projects.	You can resubmit your project on the same day for additional feedback.	Our learners love the quality of the feedback they receive from our experienced reviewers.

UDACITY
FOR ENTERPRISE