UDACITY

NANODEGREE PROGRAM SYLLABUS

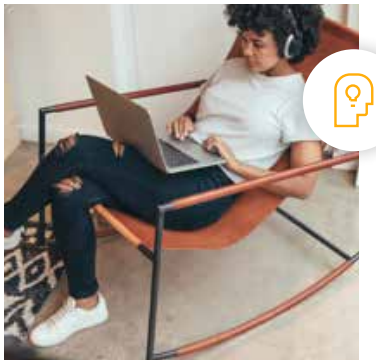
Security Engineer

Overview

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.

Estimated Time: 4 Months at 10hrs/week

Prerequisites: Basics of Python, experience configuring AWS and Linux environments.



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: 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.

Course 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.

	LEARNING OUTCOMES
LESSON ONE	**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

	LEARNING OUTCOMES	
LESSON TWO	**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

LESSON THREE	**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

LESSON FOUR	**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
LESSON FIVE	**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.

Course 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.

		LEARNING OUTCOMES
LESSON ONE	**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
LESSON TWO	**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
LESSON THREE	**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

	LEARNING OUTCOMES	
LESSON FOUR	**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
LESSON FIVE	**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.

Course 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.

		LEARNING OUTCOMES
LESSON ONE	**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
LESSON TWO	**Access Management**	• 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

		LEARNING OUTCOMES
LESSON THREE	**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
LESSON FOUR	**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 FIVE	**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 secure web applications.

Course Project:
Vulnerable Web Application

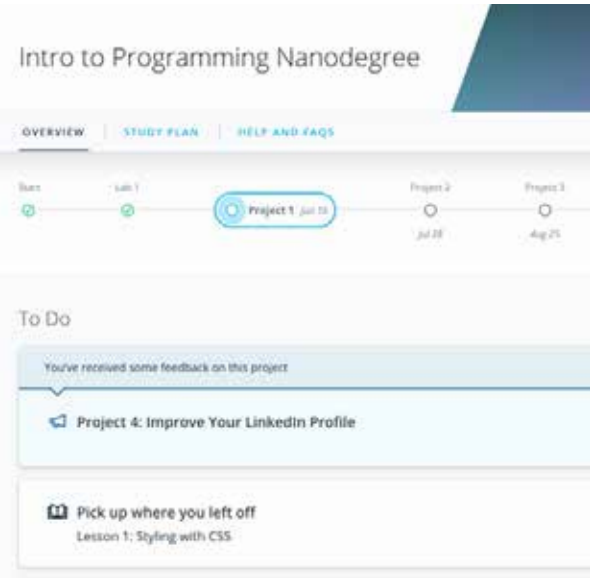
You have been hired by a startup company, USociety, who has received reports from the well known hacker group fcity that their customer data was breached. They need you to identify how the attackers got into their system, extracted all of their customers' data, and any other security holes that their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

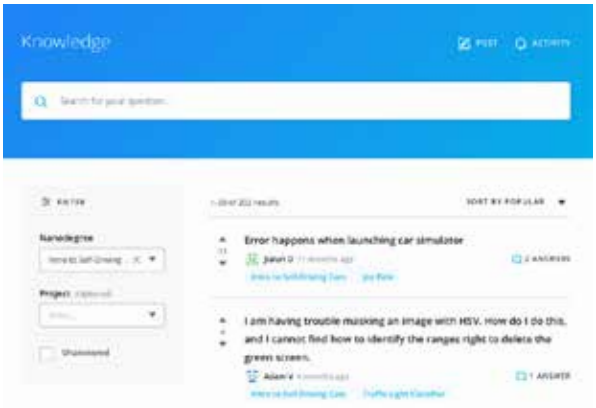
You will need to review some static code to help identify and prioritize all vulnerabilities and help create recommendations on how best to mitigate these vulnerabilities. You will also need to manually test the vulnerable web application to find all vulnerabilities and create a writeup documentation 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.

		LEARNING OUTCOMES
LESSON ONE	**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
LESSON TWO	**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

		LEARNING OUTCOMES
LESSON THREE	**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
LESSON FOUR	**Vulnerability 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
LESSON FIVE	**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 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

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.

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. Despite the downturn in the overall economy, businesses continue to invest in cybersecurity because the majority of the workforce is critically dependent on cyber to function. This program was designed to help you take advantage of this growing need for skilled security professionals.

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 systems engineers roles in any industry as countless companies are boosting security protocols.

HOW DO I KNOW IF THIS PROGRAM IS RIGHT FOR ME?
This course is for developers and IT professionals — with some exposure to security — who want to advance their career by diving deeper into the world of cybersecurity.

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 Security Engineer Nanodegree Program is an intermediate course for developers. Learners should be able to:
- Understand basic operating system fundamentals
- Understand basic principles of networking
- Follow, interpret, and implement minor modifications to Python code
- Set up an AWS environment and perform cloud configuration/management
- Set up a Linux environment and perform system configuration/management

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 Security Engineer Nanodegree program is comprised of content and curriculum to support four 4 projects. We estimate that students can complete the program in four 4 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?

There are no software and version requirements to complete this Nanodegree program. All coursework and projects can be completed via Student Workspaces in the Udacity online classroom.