SANS Foundations Syllabus

SEC275.1: System Architecture, Operating System, and Linux

Overview

The course starts with an introduction to the course and learning platform, but quickly dives into computer components and concepts, including hardware, data storage & representation, logic & data manipulation, and cloud computing.

Next, learn all about operating systems, virtualization, and containers. Understanding the lower levels of your operating system will help when it comes to troubleshooting, advanced configuration, and cybersecurity fundamentals.

Linux is a modular and powerful platform from which to chain together tools for complex tasks. Build your knowledge of Linux and the concepts that help secure it. This section is rich in labs covering commands such as grep, cp, apropos, and many more.

Exercises

- Debugging Challenge
- Linux Architecture and Components
- Linux Commands
- Linux Navigation
- The Linux Environment

Topics

- Intro to Computer Hardware
- Data Storage and Representation
- Logic and Data Manipulation
- Storing Data and Files
- Cloud Computing
- CPU and Memory
- Monitoring and Execution
- Advanced Storage
- Operating Systems
- Virtualization
- Containers
- Introduction to Linux
- The Linux Environment
- Linux Navigation
- Linux Commands
    - Basics
    - Remote Access
    - Building Software
    - Troubleshooting
- Linux Architecture & Components

SEC275.2: Search, Web, and Networking

Overview

This section provides a look into how search engines work and the most efficient ways to use them. You will be able to search Google with style and efficiency; perform advanced searches using keywords to narrow results by filetype; and troubleshoot basic computer problems using Google and other search engines.

Web applications and websites represent a huge volume of modern business and consumer applications. Understand what happens when you visit a web page by learning about concepts such as web servers, HTTP, JavaScript, cookies, and more.

In this section, we cover the inner workings of a network in order to understand how computers communicate with each other, and for what reasons. Learn about networking concepts such as IP addresses, packets, protocols, and more.

Exercises

- Search Superpowers
- WWW and Serving
- Networking
- Types of Networks
- Protocols
- Email networking
- DNS
- IP addresses

Topics

- Search Superpowers
- WWW and Serving
- Networking
- Types of Networks
    - Protocols
    - Email networking
    - DNS
    - IP addresses

SEC275.3: Introduction to Servers and Programming

Overview

Servers are a crucial part of any network and a key location where lots of data is held, making them a tempting target for attackers. We take a look at some common server types, including web, DNS, log, and email, their basic setup, and installation procedures.

We start this section with a basic introduction of what a computer program is, how it works, and different types of programming languages. We cover programming in Python and C, writing basic programs and introduce various strategies, tools, and conventions. The concepts taught in this section are invaluable in understanding how mistakes made during development can lead to security issues.

Exercises

- Git Hands On
- Printing in Python
- Variables in Python
- String Manipulation Practice
- Manipulating Numbers
- Type Conversion
- Dictionary Practice
- Bringing It Together
- For Loops
- User Input Prompts
- CLI User Input Lab
- Conditionals
- Class and Objects Lab
- While Loops
- Exceptions Lab
- Functions
- Reading and Writing Files
- Create a Portscanner
- Printing
- String Handling
- Variables
- Comments
- Pointers and Memory

Topics

- Introduction to Servers
- Web Servers
- Database Servers
- DNS Servers
- Log Servers
- Email Servers

- Programming
  - Python
  - Conditionals, loops, functions, user input, and objects
  - PEP 8 style guide
  - C
  - Pointers

SEC275.4: Security Concepts and Advanced Security Concepts

Overview

This section provides an introductory understanding of a wide variety of security concepts, terminology, and tools. Familiarize yourself with common security terminology, including Red Team vs. Blue Team, Critical Security Controls, and the stages of an attack. Learn to recognize tools like Slingshot, SIFT, and Kali. Dive deeper into concepts across disciplines including digital forensics, offensive security, and risk management.

Exercises

- Symmetric Encryption Challenge
- Asymmetric Encryption Challenge
- Hashing Challenge
- Break Me Challenge
- Steganography Challenge
- Exfiltration Challenge Lab
- Buffer Overflows
- Format String Lab
- Privilege Escalation Lab

Topics

- Encryption
- Security
- Security Distributions
- Reconnaissance
- Forensics
- Exploitation
- Privilege Escalation
- Persistence
- Lateral Movement
- Exfiltration