SANS SEC660:

- **1: Network Attacks for Penetration Testers**
  - Bypassing network access/admission control (NAC)
  - Impersonating devices with admission control policy exceptions
  - Custom network protocol manipulation with Ettercap and custom filters
  - Multiple techniques for performing network-based tampering
  - IPv6 for penetration testers
  - Exploiting OSPF authentication to inject malicious routing updates
  - Overcoming TLS/SSL transport encryption security with SSL-stripping

- **2: Crypto and Post-Exploitation**
  - Pen testing cryptographic implementations
  - Exploiting CBC bit flipping vulnerabilities
  - Exploiting hash length extension vulnerabilities
  - Delivering malicious operating systems to devices using network booting and PXE
  - PowerShell as a victim
  - PowerShell as an attacker
  - Post Exploitation with PowerShell and alternatives
  - Escaping Software Restrictions
  - Two-hour Capture the Flag exercise against an enterprise Data Loss Prevention solution

- **3: Python, Scapy, and Fuzzing**
  - Becoming familiar with Python types
  - Leveraging Python modules for real-world pen tester tasks
  - Manipulating stateful protocols with Scapy
  - Using Scapy to create a custom wireless data leakage tool
  - Product security testing
  - Using Sulley for quick protocol mutation fuzzing
  - Optimizing your fuzzing time with smart target selection
  - Automating target monitoring while fuzzing with Sulley
  - Source code-assisted binary fuzzing and code coverage measurement using AFL++
  - Block-based code coverage techniques using DynamoRio

- **4: Exploiting Linux for Penetration Testers**
  - Stack memory management and allocation on the Linux OS
  - Disassembling a binary and analyzing x86/x86-64 assembly code
  - Performing symbol resolution on the Linux OS
  - Identifying vulnerable programs
  - Code execution redirection
  - Identifying and analyzing stack-based overflows on the Linux OS

- Performing return-to-libc (ret2libc) attacks on the stack
- Return-oriented programming
- Defeating stack protection on the Linux OS
- Defeating ASLR on the Linux OS

- **5: Exploiting Windows for Penetration Testers**
  - The state of Windows OS protections on the Windows OS
  - Understanding common Windows constructs
  - Stack exploitation on Windows
  - Defeating OS protections added to Windows
  - Creating a Metasploit module
  - Advanced stack-smashing on Windows
  - Using ROP
  - Building ROP chains to defeat DEP and bypass ASLR
  - Windows 10 exploitation
  - Client-side exploitation
  - Windows Shellcode

- **6: Capture the Flag Challenge**

SANS SEC642:

- **1: Advanced Attacks**
  - Review of the testing methodology
  - Using Burp Suite in a web penetration test
  - DOM-XSS to steal and use a CSRF token
  - Discovering and exploiting SSRF
  - Discovering and exploiting LDAP injection
  - Discovering and exploiting NoSQL injection
  - Using HTTP desynchronization attacks
  - Performing privilege escalation in SAML SSO
  - Learning advanced exploitation techniques

- **2: Web Cryptography**
  - Identifying the cryptography used in the web application
  - Identifying and exploiting hash length extension attacks
  - Analyzing and attacking the encryption keys
  - Exploiting stream cipher IV collisions
  - Exploiting Electronic Codebook (ECB) Mode Ciphers with block shuffling
  - Exploiting Cipher Block Chaining (CBC) Mode with bit flipping
  - Vulnerabilities in PKCS#7 padding implementations

- **3: Alternative Interfaces and XML**
  - Interacting with a mobile application backend
  - SOAP and REST web services
  - Penetration testing of web services

    - GraphQL services
    - XML Xpath injection
    - XML External Entities (XXE)

- **4: Modern Web Application Attacks Part 1**
    - Web architectures
    - MVC and its architecture components
    - JavaScript and JavaScript frameworks
    - Server-Side JavaScript
    - Modern PHP
    - PHP deserialization bugs
    - Deserialization through PHAR

- **5: Modern Web Application Attacks Part 2**
    - Ruby and Rack applications
    - Java, Java Gadgets, and Java Payloads
    - Java Payload Weaponization
    - Java serialization
    - Fingerprinting the defense techniques used
    - Learning how HTML5 injections work
    - Using UNICODE, CTYPEs, and Data URIs to bypass restrictions
    - Bypassing a Web Application Firewall's best-defended vulnerabilities, XSS and SQLi
    - Bypassing application restrictions

- **6: Capture-the-Flag Challenge**

Offensive Python:

- **Python Basics**
    - Syntax
    - Variables
    - Math Operators
    - Strings
    - Functions
    - Control Statements
    - Modules
    - Lists
    - Loops
    - Tuples
    - Dictionaries
    - Virtual Environments

- **Offensive Python**
    - Network Socket Operations
    - Exception Handling

- Process Execution
- Blocking and Non-blocking Sockets
- Using the Select Module for Asynchronous Operations
- Python Objects
- Argument Packing and Unpacking