



Cybrary Penetration Testing Cohort

Description: With this course the goal is to build up skills in performing penetration tests. The courses outlined below along with the recommended timelines to complete each.

Week 1 & 2

- CompTIA Linux + 1-2
- IDS/IPS
- Fundamental Linux Administration Lab 1-2
- Introduction to Wireshark
- Network Traffic Analysis

Week 3

- Penetration Testing and Ethical Hacking

Week 4

- CEH

Week 5

- Malware Fundamentals
- Security Assessment & Testing
- Computer Hacking and Forensics

Week 6 & 7

- Computer Hacking and Forensics Virtual Lab
- CompTIA CySA

Week 8

- CompTIA CySA (Threat Management)

- Injection Flaws
- Security Misconfigurations
- Cross-Site Scripting
- Wireless Access Exploitation
- Password Cracking
- Analyze Structured Exception Handler Buffer Overflow
- Analyze Various Data Sources to Confirm Suspected
- Conduct Log Analysis and Cross Examination for False Positives

Week 9

- Incident Response and Advanced Forensics (Course)
- Incident Response and Advanced Forensics (Assessment)
- Assessing Vulnerabilities Post Addressal
- Check for Indicators of other Activity
- Core Impact Vulnerability Scan
- Secure Coding
- Fundamentals Vulnerability Management
- Analyze SQL Injection Attack
- Identifying System Vulnerabilities in OpenVAS

Week 10

- Python for Security Professionals
- Metasploit

Week 11

- Dynamic Malware Analysis
- Open Source Intelligence
- Forensics
- Log Analysis