# Security Analyst, Part 2 of 4: Penetration Testing Overview



**Meet the expert:** Don Bowers has been in the computer industry for over 36 years as a database programmer and an information systems and security analyst.  Don’s primary focus over the last 10 years has been in the area of information security and digital forensics.  Don currently serves as an Assistant Professor and the Program Chair for the Cybersecurity program at the College of Western Idaho.  As well as being an associate professor Don also holds the distinction of being a Certified EC-Council Instructor.  Don holds several industry certifications including MCITP Enterprise, MCSE + Security, CISSP, CISA, CEH, CHFI, ECSA (EC-Council Security Analysis), LPT (Licensed Penetration Tester) and ACE (AccessData Certified Examiner).

**Prerequisites:** In order to maximize you leaning experience when taking this course, the following prerequisites are highly recommended:

Security + Certification, knowledge of CEH (Certified Ethical Hacker), knowledge of
CHFI (Computer Hacking Forensic Investigator) and the CBK (Common Body of Knowledge) associated with the CISSP and CISA certifications are also very helpful.

**Runtime:** 02:05:06

**Course description:** There are many ways and methodologies designed to analyze the information security needs of a corporation or government entity. One of the best ways to analyze the security posture of an organization is through penetration testing. Examine the fundamentals of penetration testing including limits (known as the Scope of Work), the several phases of PTests, and additional methodologies and guidelines. Additionally, the importance of information security auditing and vulnerability assessments will be discussed, as well as legal concerns and risks that may arise for both the penetration tester and the organization being tested.

**Course outline:**

**Auditing Vulnerability Assessment and Pen Test**
- Introduction
- Auditing, Vulnerability Assessment, and Pentesting
- Audit, Vulnerability Assess, and Pen Test (cont'd)
- Why Penetration Testing is Important
- What Types of Things Should be Tested
- Summary

**Types and Phases of Penetration Testing**
- Introduction
- Non-destructive, Destructive Penetration Testing
- Blue Team, Red Team Penetration Testing
- Black, White, and Grey Box Penetration Testing
- External, Internal Penetration Testing
- Penetration Testing Processes
- Pre-Attack Phase
- Attack Phase
- Post-Attack Phase
- Summary

**Methodologies and Guidelines**
- Introduction
- Methodologies of Penetration Testing
- Help Designing Your Methodology
- Demo: Open Source Testing Documents
- Demo: Open Source Report Documents
- Penetration Testing Guidelines, Documentation
- Penetration Testing Guidelines, Professionalism
- Penetration Testing Guidelines, Risks and Skills
- Summary

**Penetration Testing Results**
- Introduction
- Penetration Testing Rules, Risks, and Behaviors
- Legal Issues
- Documents Needed for Penetration Testers
- Liability Concerns
- Rules of Engagement I
- Rules of Engagement II
- Demo: Documents Concerning Rules of Behavior
- Summary