Chapter 13
The Pentesting

Concepts

Security Assessment

- Policy and Procedures
- Security Audit

Vulnerability Assessment

- Scan Systems for Vulnerabilities
- Dont Exploit Them

Penetration Test

Deliverables

- Executive Summary
- Overall Security Posture
- Identification
- List of Findings
- Details and Steps to Reproduce
- Log Files from Tools

Pentesting

- Scan Systems for Vulnerabilities
- Exploit Them
- Escalate Privileges

Types

External

- Public Information
- Network Scanning
- Enumeration
- Testing from Perimeter

Internal

- Performed Within Organization
- Internal Network and Services

Approaches

- Blackbox
- Greybox
- Whitebox

Tools

- Core Impact
- Metasploit
- CANVAS

Phases

Pre-Attack

- Reconnaissance
- Info Gathering
- Network Ranges
- Open Ports
- WHOIS
- DNS Enumeration

Attack Phase

- Penetrate Network Perimeter
- Acquire Targets
- Execute Attacks
- Elevate Privileges

Post-Attack

- House Cleaning
- Covering Tracks
- Write Final Report