Hacker Methodologies for Security Professionals

Course Summary

Description

This course provides a flexible methodology for use in emulating external and internal network intrusion threat vectors.

Objectives
By the end of this course, students will be able to:

- Impact and Relevance of Today's Cyber Attacks
- Reconnaissance Techniques Used by Most Intruders
- Network, Host and Service Discovery Methods
- Processes Employed to Enumerate System and User Information
- How System Vulnerabilities are Identified
- Multiple Tactics Used to Penetrate Systems
- Various Techniques to Escalate System Privileges
- Password Cracking

Topics

- Footprinting
- Scanning
- Enumeration
- Web Hacking
- System Hacking (Windows)
- System Hacking (Unix)

Audience

- Incident Responders who need to understand and react to IDS alerts
- Network Defenders seeking to understand Common Access Methods
- Security Managers who desire to improve their Defensive Model
- Security Operations Center Staff seeking to identify signs of compromise
- New members of Penetration Testing and Vulnerability Assessment Teams

Prerequisites

Although no specific courses are required, students should have some level of experience with Microsoft Windows and Linux operating systems as well as a basic understanding of TCP/IP networking.

Duration

Five days

ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

Hacker Methodologies for Security Professionals

Course Outline

I. Footprinting
- A. WHOIS and DNS Enumeration
- B. DNS Interrogation
- C. Open Source INTelligence (OSINT)

II. Scanning
- A. Host Discovery
- B. Service Discovery

III. Enumeration
- A. Banner Grabbing
- B. Operating System Detection
- C. Vulnerability Scanning

IV. Web Hacking
- A. Web Application Architecture
- B. HTTP(S) Primer
- C. Discovery
- D. Configuration Management
- E. Authentication
- F. Authorization
- G. Session Handling
- H. Data Validation
- I. OWASP Top 10

V. System Hacking (Windows)
- A. Domain Enumeration
- B. User Enumeration
- C. Penetration
- D. Privilege Escalation
- E. Pillaging
- F. Expanding Influence
- G. Local Access

VI. System Hacking (Unix)
- A. User Enumeration
- B. Penetration
- C. Privilege Escalation
- D. Pillaging
- E. Expanding Influence
- F. Local Access