

## **Session 1**

### Section A: Introduction

- CD Tour
- Certifications
- Security Intro
- Resource Types
- Risk

### Section B: Hacking Fundamentals

- Exploiting Weaknesses
- Exploit Process
- Threat/Vulnerability Types
- White-Hat vs. Black-Hat
- Persistent vs. Casual
- Motivations

### Section C: Methodologies

- Overview
- Reconnaissance
- Scanning
- NMap Scan
- Enumeration
- Penetration
- System Elevation
- Network Elevation

### Section D: Methodologies (cont.)

- Pilfer
- Expansion
- Housekeeping
- Common Tools
- Other Tools

### Section E: Network Scanning Phases 1 & 2

- Overview
- Network Topology
- Network as a Target
- Discovery
- Scanning the Network
- Scanning Tools

### Section F: Network Scanning Phases 3 & 4

- Enumerating
- Packet Analyzers
- CDP
- CDP Demo
- Weak Passwords
- Common Conventions

## **Session 2**

### Section A: Management/Physical Threats

- Device Management
- Design Errors
- SolarWinds
- Physical Security
- Physical Tools

### Section B: Routers

- Router Components
- Routers & Domains
- Dynamic Routing
- Tools
- Attacks
- RIP

### Section C: Bridges & Switches

- Concepts
- Root Bridges
- Vulnerabilities/Attacks
- ARP Poisoning

### Section D: Firewalls

- Firewall Concepts
- Vulnerabilities
- Design Vulnerabilities
- Firewall Setup
- Firewall Traversal

### Section E: Wireless

- Wireless Concepts
- WEP
- Management Console
- Wireless Security
- Wireless Modes
- Wireless Vulnerabilities
- Attacks
- Warchalking/WarDriving

### Section F: W2K Hacking Phases 1 & 2

- Overview
- Discovery/Reconnaissance
- Scanning

### Section G: Enumerating Servers

- Overview
- Database Servers
- Mail/IM Servers
- Network/Web Servers
- Syslog/IAS Servers

## **Session 3**

### Section A: Enumeration Strategies & Tools

- Tool Concepts
- Terminal Services
- General Banner Grabbing
- Assorted Tools
- Anonymous Connections
- Browser/Client
- Net Commands
- LDAP Query Tools

### Section B: Using Enumeration Tools

- NetCat
- Cain & Abel
- Null Session
- DumpSec

### Section C: Penetrating Windows 2000/NT

- Identification
- Weaknesses
- Default Configuration
- Default Accounts
- Account Management
- Inherent OS Weaknesses
- NetBIOS API
- Tools

### Section D: Penetration Tools & Strategies

- LSA

- Sniffer
  - Password Cracker
  - Notepad Execution
- Section E: Elevation on Windows 2000/NT
- Overview
  - SAM Dump
  - Tools/Vulnerabilities
  - L0phtCrack
  - SAM File
  - Registry
- Section F: Pilfering
- Permissions
  - Use Data
  - Targets
  - More Targets
- Section G: File Permission Auditing
- Folder Permissions
  - Registry Permissions
  - File Delete Child
  - File Delete Child Process

## **Session 4**

- Section A: Expansion
- Scanning/Enumeration
  - Authentication
  - Relays & Proxies
  - Service Accounts
  - User Rights
  - Account Policies
  - Local Policies
- Section B: Housekeeping
- Cleaning Up
  - Reentry
  - File Header
  - Tools
  - Strategies
- Section C: Event Log Management
- Log Utilities
  - Set Up Audits
  - Audit Object Access
- Section D: Terminal Server
- Vulnerabilities
  - Detection Tools
  - Monitoring Tools
  - Attack Applications
  - Pipeupadmin
- Section E: IIS
- Evaluation
  - Weaknesses
  - Input Validation
  - Permissions
  - Application Analysis
  - Tools
- Section F: Exploiting IIS
- File Traversal
  - View Results
- Section G: Securing IIS
- Directory Structure

- IDS
- Internet Service Manager
- DLLs
- ISAPI Filters
- Directory Browsing
- Authentication
- Lockdown

## **Session 5**

### Section A: Securing Windows 2000/NT

- Analyze
- Best Practices
- Communication
- User Education
- Penetration Analysis
- Backups
- Tools
- Restriction

### Section B: Baseline Security Analysis

- Security Analyzer
- Security Report
- Score & Templates
- Options
- Reports

### Section C: UNIX Hacking Phases 1-3

- Versions
- Usage
- Discovery/Reconnaissance
- Scanning
- Enumeration

### Section D: UNIX Hacking Phases 4-7

- Concepts
- Brute Force Attack
- Dir. Serv./Remoting
- Pilfer Points
- Expansion
- Housekeeping
- UNIX Resources

### Section E: Security Policies

- Adapt to Security
- Security Plan
- Risk Assessment
- Cost
- Personnel/Culture

### Section F: Prevention Strategies

- Passive/Proactive Plan
- Testing & Documentation
- Fall Back Plan
- When it Happens!
- Discovery
- Reaction