

Hands-On Vulnerability Assessment: Protecting Your Organisation - 4 Days Exposing Network Weaknesses

Course 589 Overview

- You Will Learn How To**
- Detect and respond to vulnerabilities that put your organisation at risk using scanners
 - Employ real-world exploits and evaluate their effect on your systems
 - Configure vulnerability scanners
 - Analyse the results of vulnerability scans
 - Assess vulnerability alerts and advisories
 - Establish a strategy for vulnerability management
- Course Benefits** Knowledge of vulnerability assessment and hacking techniques allows you to detect vulnerabilities before your networks are attacked. In this course, you learn to configure and use vulnerability scanners to detect weaknesses and prevent network exploitation. You acquire the knowledge to assess the risk to your enterprise from an array of vulnerabilities and to minimise your exposure to costly security breaches.
- Who Should Attend** Security auditors, firewall/IDS personnel, PCI security testers, network managers and those involved in cybersecurity measures and implementation. Experience with network security at the level of Course 468, "System and Network Security Introduction", is assumed. A working knowledge of TCP/IP is also assumed.
- Hands-On Training** Exercises provide you with practical experience assessing vulnerabilities and include:
- Configuring scanners
 - Port scanning and enumeration
 - Scanning infrastructure, servers and desktops
 - Exploiting browsers, IDS, SQL and file services
 - Investigating and preventing spyware
 - Creating custom vulnerability tests
 - Performing a risk assessment
 - Interpreting scanning reports
 - Identifying false positives and negatives
 - Comparing scanner results

Hands-On Vulnerability Assessment: Protecting Your Organisation - 4 Days

Exposing Network Weaknesses

Course 589 Outline

Fundamentals

Introduction

- Defining vulnerability, exploit, threat and risk
- Identifying the goals of assessments
- Creating a vulnerability report
- Conducting an initial scan
- Common Vulnerabilities and Exposure (CVE) list

Scanning and exploits

- Vulnerability detection methods
- Types of scanners
- Port scanning and OS fingerprinting
- Enumerating targets to test information leakage
- Types of exploits: worm, spyware, backdoor, rootkits, Denial of Service (DoS)
- Deploying exploit frameworks

Analysing Vulnerabilities and Exploits

Uncovering infrastructure vulnerabilities

- Scanning the infrastructure
- Uncovering switch weaknesses
- Vulnerabilities in Ethereal and Wireshark
- Network management tool attacks

Attacks against analysers and IDS

- Firewall weaknesses
- Identifying Snort IDS bypass attacks
- Corrupting memory and causing denial of service

Exposing server vulnerabilities

- Scanning servers: assessing vulnerabilities on your network
- Uploading rogue scripts and file inclusion
- Catching input validation errors
- Performing buffer overflow attacks
- SQL injection
- Cross-site scripting (XSS) and cookie theft

Revealing desktop vulnerabilities

- Scanning for desktop vulnerabilities
- Client buffer overflows
- Silent downloading: spyware and adware
- Attacking design errors
- Identifying browser plugin weaknesses

Configuring Scanners and Generating Reports

Implementing scanner operations and configuration

- Choosing credentials, ports and dangerous tests

- Identifying dependencies
- Preventing false negatives
- Creating custom vulnerability tests
- Customising Nessus scans
- Handling false positives

Creating and interpreting reports

- Filtering and customising reports
- Interpreting complex reports
- Contrasting the results of different scanners
- Producing a filtered report

Assessing Risks in a Changing Environment

Researching alert information

- Using the National Vulnerability Database (NVD) to find relevant vulnerability and patch information
- Evaluating and investigating security alerts and advisories
- Determining vulnerability severity
- Employing the Common Vulnerability Scoring System (CVSS)

Identifying factors that affect risk

- Evaluating the impact of a successful attack
- Calculating vulnerability severity
- Weighing important risk factors
- Performing a risk assessment

Managing Vulnerabilities

The vulnerability management cycle

- Applying a vulnerability process
- Standardising scanning with Open Vulnerability Assessment Language (OVAL)
- Patch and configuration management

Vulnerability controversies

- Rewards for vulnerability discovery
- Bounties on hackers
- Markets for bugs and exploits