

Persistent Attack and Exploitation: Network Defense

Course Summary

This hands-on class will empower students to understand the basics of network defense and introduce them to the fundamental tools and techniques used. Moreover, a solid foundation in methodology will be developed allowing step by step guides to be used in practical hands-on classroom situations to defend and harden the network in depth. This class is designed to give students an overall perspective on network defense. The offensive side of the equation is highlighted during the course to illustrate what attackers can and will do to compromise a network. The defensive side begins with edge security of the public facing interface and focuses on the various methods used for protection. The class progresses inward focusing on network security, host security, intrusion detection and touches on incident response. Tools, techniques and methodology are emphasized in an interactive environment where students will be exposed to various defensive guides and processes.

Course Outline

Edge Security – Practical application and hands on designing, implementing and managing resources and technologies that protect the perimeter of a network.

Network Security - Practical application and hands on designing, implementing and managing techniques, policies, and devices that detect and prevent malicious activity across a network.

Endpoint Security - Practical application and hands on implementing and managing software, configuration, process or policy to secure Endpoint devices.

Threat Monitoring and Response – Practical application and hands on designing, implementing and managing collection, analysis and response to security related events.

Examples of Exercises and Labs

- Edge Router Configuration
- Firewall Configuration
- DMZ Design & Implementation
- IDS/IPS Deployment
- Edge Security Challenge Lab
- Network Encryption
- Authentication, Authorization, & Accounting
- Network Access Control
- DNS Hardening
- Anti-Virus Management
- Host-Based Firewalls
- Host-Based IPS
- Linux Hardening
- Windows Hardening
- Windows Domain Hardening
- Certificate Authority Deployment
- Endpoint Security Challenge Lab
- Incident Response Process
- Security Information & Event Management
- Threat Monitoring & Response Challenge Lab
- Final Challenge Lab: Network Defense Simulation

Course Duration

4 Days

Delivery Modes

Onsite Instructor Lead Class

Pre-Requisites

Students should have a familiarity with basic operating system concepts (Windows and Linux/Unix), and a good knowledge of TCP/IP and associated networking concepts.

Who Should Attend

Junior system or network administrators or other junior positions with information security or network responsibilities including new auditors or new consultants.

Materials Provided

Student Manual
Student Lab Manual
Student Lab Solutions Manual
Accuvant gear

Next Steps

Persistent Attack and Exploitation:
-Offense
-Secure Coding
-Web Application Security

Course Details

Day 1 Edge Security

Day 1 starts off by identifying the methodology of the layered security model. At the outermost perimeter we focus on Edge Security. A variety of device types will be discussed, focusing on the best practices for strengthening a network perimeter. Simplicity and effectiveness will be the underlying factor as we cover designing and building a solid first line of defense.

MAJOR TOPIC AREAS

- Edge Routers
- Firewalls
- DMZ's
- IDS/IPS
- Edge Security Daily Challenge Lab

Day 2 Network Security

Day 2 continues with the layered security model as we look in-depth at internal network protection. In this module protecting data while it is in transit will be a topic focus. In addition, a comprehensive approach to controlling access to network traffic will be explored.

MAJOR TOPIC AREAS

- Infrastructure
- Encryption
- Access Control
- Domain Name System
- Security Daily Challenge Lab

Day 3 Endpoint Security

Day 3 explores the final layer of the layered security model covered in this course. During this module the focus will be protecting devices that serve the end user such as workstations, servers, and other peripherals. We will also cover integrating Endpoint Security with the other layers in order to provide a cohesive defense.

MAJOR TOPIC AREAS

- Endpoint Protection
- System Hardening
- Windows Domain
- Endpoint Security Daily Challenge Lab

Day 4 Threat Monitoring & Response

Day 4 uses SIEM technology to audit the effectiveness of the layered security model and protect assets by correlating security events across a network or an entire enterprise. Proper processes for identifying and responding to security breaches will be outlined, as well as vendor solutions managing this complex data.

MAJOR TOPIC AREAS

- Logging & Alerting
- Incident Response
- Security Information & Event Management
- Threat Monitoring & Response Challenge Lab

For More Information

For more information about Accuvant's global education services, please contact us at education@accuvant.com or visit our web site: www.accuvant.com.

About Accuvant

Accuvant is the only research-driven information security partner delivering alignment between IT security and business objectives, clarity to complex security challenges and confidence in enterprise security decisions. Accuvant delivers these solutions through three practice areas: Risk and Compliance Management, Accuvant LABS and Solution Services. Based on our clients' unique requirements, Accuvant assesses, architects and implements the policies, procedures and technologies that most efficiently and effectively protect valuable data assets.

Since 2002, more than 3,900 organizations, including 65 of the Fortune 100, as well as 20 major federal U.S. agencies and thousands of mid-market businesses have trusted Accuvant with their data security challenges. Headquartered in Denver, Accuvant has offices in 36 cities across the United States and Canada. For more information, visit www.accuvant.com.