

Persistent Attack and Exploitation: Offense

Course Summary

This course examines offensive hacking techniques as a step in understanding Network Defense. This process is explored using a Penetration Testing framework and uses current hacking tools and techniques. Footprinting a target is step one and focuses on gathering information in the public arena that is freely available and not always recognized as dangerous. Enumeration, step two, is based on discovered targets and provides more in-depth and potentially damaging information for use against the target. Step three, Attack, is based on vulnerable and exploitable targets identified in steps one and two. Automated tools and simple, basic attack techniques are combined to totally compromise vulnerable targets on the network. The final step, Escalation, is designed to solidify the hold on the target and pilfer and extract maximum information from the compromised targets. During the course simple but effective countermeasures are offered as steps in improving the Network Defense of the target.

Course Outline

Footprinting	Enumeration	Attack	Escalation
Public Information	Traffic Analysis	Password Cracking	Maintain Access
Search Engines	Raw Communications	Misconfigurations	Escalate Privileges
Public Postings	Host Discovery	Exploitation	Leverage Weakness
Maltego	Port Scanning	Active Attacks	Pilfer Data
	Service Enumeration	Social Engineering	Vulnerability Scanning

Examples of Exercises and Labs

- Whois and ARIN
- Search engine use
- Email harvesting
- Other public information and Metadata
- Using tools like Maltego
- Major Footprinting Lab
- Traffic Analysis and Sniffing
- Raw Communications
- DNS insecurities
- Port scanners
- Vulnerability scanners
- Major Enumeration Lab
- Password security and attacks
- Exploiting misconfigurations
- Vulnerability exploit tools like metasploit
- Active network attacks
- Man in the middle attacks
- Major Attack Lab
- Escalation of privileges
- Compromising local executables
- Pilfering and scraping information
- Major Escalation Lab

Course Duration

4 Days

Delivery Modes

Onsite Instructor Lead Class

Pre-Requisites

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

Who Should Attend

System or network administrators or others with information security responsibilities including auditors or consultants.

Materials Provided

Student Manual
Labs and Lab Solutions
Checklists and guides
Tools and installers
Accuvant gear

Next Steps

Persistent Attack and Exploitation:
-Network Defense
-Secure Coding
-Web Application Security

Course Details

Day 1 Footprinting

Day 1 introduces methods of gaining open source information on a designated target. The importance of a methodical and complete process for gathering information and keeping it organized is discussed. Day 1 also reinforces the thorough and organized manner required for successful information gathering.

MAJOR TOPIC AREAS

- Public Information
- Search Engines
- Mining Public Postings
- Maltego
- Footprinting Daily Challenge Lab

Day 2 Enumeration

Day 2 focuses on more active and less passive methods and tools used to further investigate the target and begin to focus the attack on discovered weaknesses. Basic concepts of how communication occurs on the network will be explored enabling a better understanding of how to compromise it. Tools and techniques to discover weaknesses and exploitable targets is discussed and demonstrated.

MAJOR TOPIC AREAS

- Traffic Analysis and Sniffing
- Raw Communications and Connections
- Host Discovery
- Port Scanning
- Service Enumeration
- Vulnerability Scanning
- Enumeration Daily Challenge Lab

Day 3 Attack

Day 3 focuses on taking advantage of the information found during Day 2 and using that to find and use exploits to penetrate target machines. A variety of exploit sources and exploit types are explored and tested and alternate methods of penetration are discussed. Social engineering will be touched on and web attack methods will be explored.

MAJOR TOPIC AREAS

- Password Cracking
- Leverage Misconfigurations
- Exploit Vulnerabilities
- Active Network Attacks
- Social Engineering
- Attack Daily Challenge Lab

Day 4 Escalation

Day 4 focuses on strengthening our hold in the network by fundamentally understanding the basic architecture of Windows and Unix/Linux hosts and networks. We will use this understanding to our advantage to escalate privilege levels and expand our hold in the network.

MAJOR TOPIC AREAS

- Maintain Access
- Leveraging Local Vulnerabilities
- Pilfering Data
- Escalation 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.