

Art of Exploitation: Bootcamp Edition



Developing Tomorrow's Security Experts Today.

Art of Exploitation Bootcamp Edition provides a comprehensive solution to Computer Network Operations (CNO) training in the fields of computer penetration testing, red teaming, vulnerability analysis, and exploitation.

The first offering in this series is the flagship course "Art of Exploitation Bootcamp Edition." Modular in design, and comprehensive in scope, the Bootcamp Edition is a 10-day, intense course of study with over 40 labs that provides an introduction to the basic tactics, techniques, and methodology required for a Network Exploitation Analyst or Operator.

In addition to the 10-day basic course, the modular design allows individual sections to be added, subtracted, or taught separately depending on the requirements of the audience.

Modules

- Introduction
- Pre-operations and Legal Requirements
- Windows Review
- UNIX Review
- Methodology
- Open Source Collection
- Network Discovery
- Hackers and Cyber Terrorism Brief
- Network Reconnaissance
- Identifying Vulnerabilities
- Hacking Network Devices
- Hacking Unix
- Hacking Windows
- Remote Host Forensics
- Hacking an Intranet
- Capstone Exercise

Module Descriptions: Bootcamp Edition

Pre-Operations Preparation and Legal Concerns

Covers recommended preparation steps that an operator or team should conduct prior to commencement of an operation. Also discusses various laws and regulations that an individual working in computer security must be aware of. Topics include pre-operations checklists, codes of ethics, assessment reports, operating platforms, and connectivity. Length is approximately 1 hour.

Windows Review

This module covers basic windows commands and tools that the student will be required to understand and use throughout the course. Topics include the use of the command shell and resource kit tools to conduct various administrative tasks locally and remotely. Length is approximately 4 hours and includes 5 labs.

Unix Review

This module covers basic UNIX commands, directory structure, files and administrative tasks that the student will be required to understand and use throughout other portions of the course. Topics include modifying permissions; system directories and their content; basic user and network commands; vi editor; and manipulating processes and files. Length is approximately 3 hours and includes 4 labs.

Methodology

Provides the basic building blocks that are used in all other modules. Covers tactics, techniques, procedures, and concepts that an exploiter must grasp in order to be successful. Information in this module includes "golden rules," various overflows, different types of attack concepts, and mitigation strategies to avoid detection. Length is approximately 2 hours.

Open Source Collection

Provides the student techniques to gather target information using tools and resources found via publicly available sites throughout the internet. Topics include using advanced operators from the Google search engine, creating and using a target template to catalog your information, discovering system information via the internet, and tools to automate your collection. Length is approximately 3 hours and includes 2 labs.

Network Discovery

Building upon information discovered during the previous module, this module covers tools and techniques to further refine your target information. Topics discussed include determining and analyzing IP registration information and assignments, conducting DNS queries, using various traceroutes (ICMP, UDP and TCP), BGP queries, and autonomous system analysis. Length is approximately 4 hours and includes 3 labs and 1 group exercise.

Hackers and Cyberterrorism Brief

Knowing the enemy has been essential to success since Sun Tzu wrote the Art of War. To be a successful exploiter, not only do you need to know the enemy, you also need to understand how to think like the enemy. The Hacker Brief covers not only the adversarial mindset but also the emerging threats of cyberterrorism. Length is approximately 1 hour 30 minutes.

Network Reconnaissance

This module builds upon information gathered during previous modules and discusses methods, tools, and techniques that can be used to refine target information. Topics include port scanning, how to determine firewall rules, discovering and using open proxies, and system fingerprinting using manual and automated tools. Length is approximately 6 hours and includes 5 labs.

Identifying Vulnerabilities

This module explores how to determine potential target vulnerabilities and then match those vulnerabilities to the appropriate tool. Topics include where to find vulnerability and exploit information, how to determine host patch levels, and the use of intrusion detection systems to help determine tool selection. Length is approximately 1 hour and includes 1 lab.

Hacking Network Devices

Covers various techniques and tools that can be used to gather information from and exploit network devices. Topics include ARP spoofing, using SNMP for exploitation, and cracking network device passwords. Length is approximately 2 hours and includes 3 labs.

Hacking Unix

This module covers various methods, tools, and techniques used to exploit Unix systems. Topics include the use of remote exploits; installing various backdoors and rootkits; hiding your tracks; privilege escalation; post hack system analysis and data-mining the system and network for information. Length is approximately 10 hours and includes 9 labs.

Hacking Windows

This module covers various methods, tools, and techniques used to exploit Windows systems. Topics include the use of remote exploits, installing various backdoors, and post-hack system analysis. Length is approximately 2 hours and includes 1 lab.

Remote Host Forensic

This module covers the initial steps you need to take once you get on a box for the first time. This will be a deeper analysis of programs running or present, patch levels, user information, and network information. The discussion topics will help determine the risk involved with continuing with your activity. Length is approximately 4 hours and includes 3 labs.

Hacking an Intranet

Most courses cover how to hack into a system remotely, but don't cover the "What's next." Well, welcome to "What's next!" This module discusses how to go from owning one host to an entire domain; how to move from one domain to another; how to conduct internal reconnaissance to find other targets; the use of keyloggers and sniffers; and data-mining techniques that can be used to find all kinds of information. Length is approximately 5 hours and includes 4 labs.

Capstone Exercise

Putting to use all of the methods, tools, and techniques that have been taught, students will work in teams to exploit a target network and find the key files. Length is approximately 12 hours.

Solvern Innovations - Main Office
5523 Research Park Drive, Suite 230
Baltimore, MD 21228

phone: 443.543.5760
www.solvern.com