



CERTIFICATIONS

Bootcamp Edition 2.0 is offered as a part of the following certifications:



Certified Operations
(Specialist/Expert)



Certified Analysis
(Specialist/Expert)



Certified Cyber Developer



Certified Cyber Scientist

ART OF EXPLOITATION™

BOOTCAMP EDITION 2.0

Art of Exploitation Bootcamp Edition 2.0 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 nine-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 9-day basic course, the modular design allows individual sections to be added, subtracted, or taught separately depending on the requirements of the audience.

TOPICS

1. Pre-operations and Legal Requirements
2. Basic Operating System Review
3. Methodology
4. Open Source and Network Discovery
5. Network Reconnaissance
6. Vulnerability Identification
7. Hacking Network Devices
8. Hacking Unix
9. Hacking Windows
10. Hacking an Intranet
11. Capstone Exercise

CONTACT US

1333 Ashton Road
Hanover, MD 21076

866.356.3535

www.artofexploitation.com



BOOTCAMP 2.0

MODULE TOPICS

CLASS LENGTH (HOURS)

NUMBER OF LABS

1 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.

8 BASIC OPERATING SYSTEM

This module covers basic Windows and UNIX 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; modifying permissions; system directories and their content; basic user and network commands; VI editor; and manipulating processes and files.

2 REVIEW 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.

8 OPEN SOURCE AND NETWORK DISCOVERY

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.
- Automating your collection determining.
- Analyzing IP registration information and assignments conducting DNS queries.
- Using various trace routes (ICMP, UDP and TCP)
- BGP queries
- Autonomous system analysis.

6 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.



1 VULNERABILITY IDENTIFICATION

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.

3 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.

12 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.

9 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.

6 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 internal reconnaissance to find other targets; from one domain to another; how to conduct the use of keyloggers and sniffers; and data-mining techniques that can be used to find all kinds of information.

16 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.



CONTACT US

1333 Ashton Road
Hanover, MD 21076

866.356.3535

www.artofexploitation.com