

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 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.

Modules

- Pre-operations and Legal Requirements
- Basic Operating System Review
- Methodology
- Open Source and Network Discovery
- Network Reconnaissance
- Vulnerability Identification
- Hacking Network Devices
- Hacking Unix
- Hacking Windows
- 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 and includes 1 lab.

Basic Operating System Review

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. Length is approximately 8 hours and includes 8 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 and includes 1 lab.

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, tools to automate your collection determining, 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 8 hours and includes 5 labs.

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.

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. 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 3 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 12 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 9 hours and includes 5 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 6 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 16 hours.

See TCS' complete line of products and services at www.telecomsys.com.

Your Established Partner

TCS is a leading provider of software and solutions to government customers requiring high reliability and security. TCS has been providing premier IT and wireless communications solutions to the U.S. Government since 1987.

TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401 USA
Toll Free: 1.888.728.8797
Outside US: +1.410.263.7616
www.telecomsys.com

TCS Cyber Intelligence Group - Main Office
1333 Ashton Road
Hanover, MD 21076-3120
phone: 866.356.3535

Enabling Convergent Technologies® is a registered trademark of TCS. All other trademarks are the property of their respective companies. Information subject to change without notice.
| NasdaqGM: TSY5 | 100113