



## Art of Exploitation – Bootcamp Edition

CSRgroup and our partner Solvern Innovations are proud to present the the Art of Exploitation – Bootcamp Course.

Committed to providing a comprehensive solution to the difficult problem of providing quality training in the fields of Penetration Testing, Red Teaming and Exploitation Operations; CSRgroup and Solvern Innovations has developed “The Art of Exploitation” curriculum.

Our flagship course “The Art of Exploitation – Bootcamp Edition”, is a ten day intense course of study that provides and introduction to the basic tactics, techniques, procedures and methodology required for a network exploitation practitioner.

### About AOE Courses

The Art of Exploitation is a series of courses on various segments of computer exploitation. All of the courses are modular, allowing portions to be moved, subtracted, added, or even combined with other AOE courses to create a custom offering specific to the needs of the target audience. All AOE courses are built on the “Practice by Doing” method of instruction and contain many practical application labs. All AOE courses share the same philosophy; Focus on Methodology and Techniques instead of “Toolology”. Tools come and go, but if the student can learn the proper techniques and methodology, they can use many different tools to accomplish their goals and objectives.

### Pre Requisites

Although this is a basic level course in computer exploitation, this is not a basic computer course. The student should be familiar with Linux and Windows administration, command line usage, possess an understanding of TCP/IP and of networking.

### Contact

For more information, contact CSRgroup LLC at 410-609-3157, or email [training@csr-group.com](mailto:training@csr-group.com)

### Target Audience

Individuals involved in Computer Network Security, Information Assurance, Network Defense, Penetration Testing, Red Teaming, Mangers or anyone else wishing to better understand the threats that may face their networks on a daily basis.

### Exercises

Most modules contain several practical application exercises allowing the student to retain their knowledge through hands-on practice. There is also a 2 day “capstone” exercise which allows the students to test their recently gained knowledge in a practical setting.



## MODULES OUTLINE

### Methodology

This module covers a high level overview of the Tactics, Techniques, Procedures, and Concepts that an exploiter must grasp in order to be successful. Information in this module includes:

- "Golden rules"
- Various overflows
- Attack concepts
- Mitigation strategies to avoid detection

### 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

- Windows command shell
- Making the most of native commands
- Use of resource kit tools for local and remote reconnaissance and exploiting

### Open Source Collection

This module provides the student techniques to gather target information using tools and resources found via publicly available sites throughout the internet. Topics include:

- Google - using advanced search operators
- Creating and using a target folders
- Hiding or disguising your activities from the target
- Discovering and fingerprinting targets using online tools

### Pre-Operations & 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
- Connectivity & Infrastructure

### 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
- Manipulating processes and files



## Network Discovery

Building upon information discovered during the previous module, this section covers tools and techniques to further refine your target information. Topics include:

- Target IP/Netblock discovery
- DNS queries
- Tracerouting (using ICMP UDP and TCP)
- Network enumeration
- BGP Queries and Autonomous System analysis

## Hackers & Cyberterrorism

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.

## Hacking Network Devices

This section 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
- Cracking network device passwords
- Cisco config files
- Exploiting Network Devices

## Network Reconnaissance

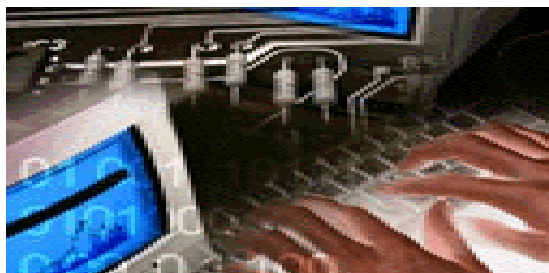
This module builds upon information gathered during previous modules and discusses methods, tools and techniques that can be used to refine target information. Topics include:

- Port scanning
- Banner grabbing
- Firewall interrogation
- Open proxies
- Interrogating mail servers
- Webserver fingerprinting
- SSL interrogation
- Discovering VPN's

## 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
- Analyzing your target folders and collected information to determine potential avenues of attack
- How to determine host patch levels
- The use of Intrusion Detection Systems to help determine tool selection





## Hacking Unix

This module covers various methods, tools and techniques used to exploit Unix systems. Topics include:

- Initial access with remote exploits
- Installing and using backdoors
- Rootkits
- Hiding your tracks
- Privilege Escalation
- Accessing and exploiting NIS and SAMBA
- Post hack system analysis
- Datamining and information extraction

## Hacking Internal Networks

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 covers:

- How to go from owning a host to an entire domain
- Using trusted relationships to exploit other domains
- Conducting internal reconnaissance
- Using keyloggers and covert packet sniffers
- Using LDAP and Active Directory to gather information.
- Datamining techniques that can be used to discover target information.

## Hacking Windows

This module covers various methods, tools and techniques used to exploit Windows systems. Topics include:

- Remote exploits,
- Choosing the right backdoor
- Covering your tracks
- Privilege escalation and token stealing
- Remote system forensics

## Capstone Exercise

Putting to use all of the methods, tools, and techniques that have been taught, the students will spend up to 2 days working in teams to exploit a target network and accomplish the given objectives.

