

## Advanced Ethical Hacking

### Overview

Advanced Ethical Hacking Boot Camp aims to train you on how to successfully attack fully patched and hardened systems, how to circumvent common security controls, and how to get to confidential data.

### Target Audience

### Course Objectives

The goal of this course is to help you master a more efficient and effective penetration testing process. By learning how to fully utilize 0day attacks that replicate an APT attack, you become a very valuable member of any penetration testing team. This course also supports and prepares you for the CEPT and ECSA certification exams.

### Course Outline

[Register Online](#)

### Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"  
ILT = "Instructor-Led-Training"

*This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.*

## Course Outline

Black Hat hackers are always changing their tactics to get one step ahead of the good guys. InfoSec Institute updates our course materials regularly to ensure that you learn about the most current threats to your organization's networks and systems. This course focuses on advanced exploitation techniques. A brief introduction to system exploitation theory and process will be covered, the rest of the course covers advanced topics, such as:

- Attacking fully patched systems
- Attacking DMZs & other secured infrastructure
- Using egghunter & meterpreter shellcode
- Running exploits in RAM vs. on disk
- Privilege Escalation attacks on Windows 7
- Hijacking SSL encrypted sessions
- 0day vuln discovery process
- Writing Windows Shellcode
- Fuzzing with peachfuzz and SPIKE
- Using a Disassembler
- Attacking SafeSEH
- XSS Attacks & XSS Redirection
- Buffer Overflows against Windows 2008 Server, Windows 7 clients
- Port Redirection
- Metasploit scripting & automation
- Hiding from IDSs
- Advanced Man in the Middle Attacks
- MITM VoIP attacks
- Format String attacks
- Heap Spraying/JIT Spraying
- Binary Auditing with IDA Pro
- Anti-disassembling Detection circumvention
- Defeating ASLR, DEP
- RFI & Source Code Injection Attacks
- 0day attacks
- Compromising secured infrastructure
- NMAP automation
- Covert Channels
- Traffic interception
- Intercepting VoIP traffic & attacking Ethernet enabled PBXs
- Windows SEH Stack Overflows
- Fuzzer selection & comparison
- Portable Executable (PE) Compression & Encoding
- Egghunter & ROP payloads
- Cross Site Request Forgery Attacks
- Proxy cache poisoning