

# ETHICAL HACKING AND SYSTEMS DEFENSE



Duration: 3 full days and evenings

Class Time: 8:00 AM – 5:00 PM

Open Lab Time: 6:00 PM – 9:30 PM on the first two evenings

Attack and Defense Competition: 6:00 PM – 9:30 PM on the final evening

## DESCRIPTION:

Ethical Hacking and Systems Defense is a hands-on, *intensive*, three-day workshop immersing students in the methodologies and application of hacking concepts and techniques. This workshop introduces students to footprinting, scanning, gaining and maintaining access, covering tracks, and securing their own systems. When students leave this class they will have hands-on experience and an understanding of hacking concepts and techniques.

## ATTACK AND DEFENSE COMPETITION:

On the final evening, students will work and compete in teams with a chance to both attack as well as defend a “commercial” network. This allows for the more advanced students in class to test their abilities and help lead those less experienced team members to apply what was learned. Teams will be judged on their ability to secure their network assets, detect and respond to outside threats, and maintain the availability of existing services (e.g., E-mail and Web servers). On the previous two evenings your instructor will be mentoring you in “open lab” time.

## INTENDED AUDIENCE:

This course will significantly benefit anyone who is concerned about the integrity of their network infrastructure and systems security. Designed for those interested in taking the **Certified Ethical Hacker (CEH) exam (312-50)**



## PRE-REQUISITES:

Familiarity with the core TCP/IP protocols (e.g., TCP, IP, ICMP, UDP, DNS, HTTP), how networking equipment works (especially layers 2 and 3), Windows and Linux command lines, and SQL-based databases.

by Casey W. O’Brien, Instructor

IT Training Solutions, L.L.C.

801-649-4030 / [matt@ittrainingsolutions.net](mailto:matt@ittrainingsolutions.net)

## COURSE OUTLINE:

Each topic and subtopic listed in the outline includes a brief theoretical discussion, hacking exercises and labs, as well as defensive countermeasures. Both Windows-based and Linux-based attack tools will be used.

### DAY ONE:

- I. **Introduction to Ethical Hacking:**
  - a. Course goals and objectives
  - b. Information security certification programs:
    - i. CEH
    - ii. OPST
    - iii. CISSP
    - iv. GIAC
    - v. OSCP
  - c. Various penetration testing lab environments and system configurations
  - d. Introduction to ethical hacking
  - e. Ethical hacking methodologies:
    - i. OSSTMM
    - ii. NIST
    - iii. OCTAVE
    - iv. TRAWG
  - f. Penetration testing models:
    - i. White box
    - ii. Black box
    - iii. Gray box
  - g. Hacking laws: U.S. Perspective
  - h. Additional resources (both online and print)
  
- II. **Footprinting:**
  - a. Introduction to footprinting
  - b. Footprinting objectives
  - c. Footprinting environments (Intranet, Internet, Remote Access, Extranet)
  - d. Footprinting analysis:
    - i. Scope of activities
    - ii. Proper authorization
    - iii. Publicly available information:
      1. Company Web pages

by Casey W. O'Brien, Instructor

IT Training Solutions, L.L.C.

801-649-4030 / [matt@ittrainingsolutions.net](mailto:matt@ittrainingsolutions.net)

2. Related organizations
  3. Location details
  4. Phone numbers, contact names, E-mail addresses, job titles, organizational charts
  5. Current events (mergers, acquisitions, layoffs, rapid growth)
  6. Privacy or security policies
  7. Technical details indicating the types of security mechanisms in place
  8. Archived information
  9. Disgruntled employees
  10. Search engines, discussion groups, resumes
- iv. WHOIS and DNS enumeration
  - v. Network reconnaissance

### III. **Scanning:**

- a. Introduction to scanning
- b. Scanning objectives
- c. Scanning techniques using nmap:
  - i. Ping sweeps (ARP and ICMP)
  - ii. Port scans (TCP and UDP)
  - iii. Protocol scans (IP)
- d. Introduction to banner grabbing
- e. Banner grabbing objectives
- f. Banner grabbing techniques:
  - i. Telnet
  - ii. Netcat
- g. Introduction to application mapping
- h. Application mapping objectives
- i. Application mapping techniques:
  - i. amap
- j. Operating systems detection through fingerprinting
- k. OS fingerprinting objectives
- l. Active and passive stack fingerprinting techniques
- m. Stack fingerprinting techniques:
  - i. nmap
  - ii. POF
  - iii. Ettercap
- n. Identifying vulnerabilities through network vulnerability scanning:

by Casey W. O'Brien, Instructor

IT Training Solutions, L.L.C.

801-649-4030 / [matt@ittrainingsolutions.net](mailto:matt@ittrainingsolutions.net)

- o. Vulnerability scanning objectives
- p. Vulnerability scanning techniques:
  - i. Nessus

## DAY TWO:

### IV. Enumeration:

- a. Introduction to enumeration
- b. Enumeration objectives
- c. Network service enumeration (services are discussed in numeric order according to the port on which they traditionally listen, whether TCP or UDP; focus is on those services that give up the lion's share of information):
  - i. FTP
  - ii. SMTP
  - iii. DNS
  - iv. SNMP
  - v. HTTP
  - vi. NetBIOS Name Service (NBNS)
  - vii. NetBIOS Session Service
  - viii. SMB/CIFS

### V. Windows Hacking:

- a. Introduction to Windows Hacking
- b. Windows hacking objectives
- c. Hacking Windows techniques:
  - i. Hacking Windows-specific services:
    - 1. Manual and automated remote password guessing
    - 2. Eavesdropping on authentication
    - 3. Attacking vulnerabilities in Windows-specific services
    - 4. Privilege escalation techniques:
      - a. Buffer overflows using Metasploit
      - b. DLL injection
      - c. Named Pipe Redirection
      - d. NetDDE requests
      - e. Debugger authentication flaws
      - f. WINS flaws

by Casey W. O'Brien, Instructor

IT Training Solutions, L.L.C.

801-649-4030 / [matt@ittrainingsolutions.net](mailto:matt@ittrainingsolutions.net)

- ii. Getting interactive:
  - 1. Determining and disabling auditing
  - 2. Command-line remote control techniques:
    - a. Remote.exe
    - b. PsExec
    - c. Netcat
  - 3. GUI remote control techniques:
    - a. RealVNC
    - b. Enabling RDP on target system
- iii. Maintaining access techniques:
  - 1. Creating rogue user accounts
  - 2. Planting backdoors
  - 3. Installing rootkits
- iv. Expanding influence techniques:
  - 1. Searching for sensitive files
  - 2. Combing the drive for hidden/protected files
  - 3. Extracting/cracking passwords
  - 4. Capturing keystrokes
  - 5. Capturing packets
  - 6. Attacking other systems
- v. Covering your track techniques:
  - 1. Erasing the logs
  - 2. Hiding files

## **DAY THREE:**

- VI. **Web Hacking:**
  - a. Introduction to Web application hacking
  - b. Web application profiling and scanning
  - c. Introduction to Hacking Web platforms
  - d. Hacking Web platform techniques:
    - i. Apache
    - ii. Internet Information Services (IIS)
    - iii. Hardening Web platform best practices:
      - 1. ModSecurity
      - 2. URLScan
  - e. Attacking Web authentication:
    - i. Common Web authentication threats

by Casey W. O'Brien, Instructor

IT Training Solutions, L.L.C.

801-649-4030 / [matt@ittrainingsolutions.net](mailto:matt@ittrainingsolutions.net)

- ii. Bypassing authentication techniques
- f. Attacking Web authorization:
  - i. Fingerprinting authorization
  - ii. Attacking access control lists (e.g., Directory Traversals) and tokens
- g. Input validation attacks:
  - i. Buffer overflows
  - ii. Canonicalization (e.g., dot-dot-slash)
  - iii. HTML injection
  - iv. Boundary checks
  - v. SQL injection and datastore attacks
  - vi. Command execution
  - vii. Encoding abuse
  - viii. PHP global variables
- h. Attacking Web Datastores:
  - i. SQL primer
  - ii. SQL injection discovery
  - iii. Exploiting SQL injection vulnerabilities
  - iv. Other datastore attacks
- i. Attacking Web Application Management:
  - i. Remote server management:
    - 1. Telnet
    - 2. SSH
    - 3. Proprietary management ports
    - 4. Others
  - ii. Web content management:
    - 1. FTP
    - 2. SSH/SCP
    - 3. FrontPage
    - 4. WebDAV

by Casey W. O'Brien, Instructor

IT Training Solutions, L.L.C.

801-649-4030 / [matt@ittrainingsolutions.net](mailto:matt@ittrainingsolutions.net)