800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Hacker Methodologies for Security Professionals Training

Applied Technology Academy

This course teaches students the processes threat actors use to break into organizations' networks and steal their most sensitive data. Utilizing industry-standard penetration testing and auditing software, attendees will learn to identify, scan, and enumerate target systems; correlate services to vulnerabilities and exploits; employ exploits to gain access to the target systems; elevate privileges; propagate through the network; and cover their tracks within a target network. This course is focused primarily on Windows and Linux operating systems, so students should be comfortable with both.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**2 years: Command-line & TCP/IP**	**$120,000**	**Yes**

Course Overview

After successfully completing this course, students will be able to:

- Identify the classes of hackers, their motivations, and
- the methodologies employed by threat actors
- Use publicly available tools and open source
- intelligence techniques to develop a target footprint
- Scan and enumerate targets to identify underlying
- operating systems and services
- Research and leverage exploits for vulnerable services
- to achieve access to target systems
- Identify system configuration weaknesses and viable
- privilege escalation tactics
- Analyze exploited systems to identify and remove
- indicators of compromise
- Employ system tools to exploit additional targets
- within an internal network

Course Outline

- **Lesson 1 : Hacker Techniques and Tools**
- **Module One: Hacking: The Next Generation**
- **Module Two: TCP/IP Review**

- **Module Three: Cryptographic Concepts**
- **Module Four: Four Physical Security**
- **Lesson 2: A Technical and Social Overview of Hacking**
- **Module Five: Footprinting Tools and Techniques**
  - Module Six: Port Scanning
  - Module Seven: Enumeration and Computer System Hacking
  - Module Eight: Wireless Vulnerabilities
  - Module Nine: Web and Database Attacks
  - Module Ten: Malware
  - Module Eleven: Sniffers, Session Hijacking, and Denial of Service Attacks
  - Module Twelve: Linux and Penetration Testing
  - Module Thirteen: Social Engineering
- **Lesson 3: Incident Response and Defensive Technologies**
  - Module Fourteen: Incident Response
  - Module Fifteen: Defensive Technologies

Intended Audience

- Threat Hunters who need to understand hacker behavior and methodology
- Security Analysts and Incident Responders who need to identify signs of compromise
- New members of penetration testing or red teams

Prerequisites

- Familiarity with Windows or Linux command-line interfaces
- Knowledge of TCP/IP networking
- Successful completion of OS Internals for Security Professionals

Follow-On Courses

- EC-Council Certified Ethical Hacker (CEH)
- Certified Ethical Hacker Master

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.