

# Hacking 101

1 day class

Get Certified



This 1-day course will teach you the foundations of Pen Testing and how to find and exploit vulnerabilities within different technologies. This introductory course will train attendees in understanding Pen Testing, and provide background information on risks and vulnerabilities associated with different systems and provide insight to how the mindset of a hacker works. Delegates will also get access to an online course environment platform which will be used to practice the concepts taught during the course.

## WHO SHOULD TAKE THIS CLASS

System Administrators, Web Developers, IT Managers, Security enthusiasts, anyone interested in Pen Testing and ethical hacking. (No prior experience is required to take this course)

## COURSE OUTLINE

### HACKING FUNDAMENTALS

- Hacking History 101
- Hacking in 2018
- CIA Triad
- Art of Hacking Methodology
- Introduction to Kali Linux

### NETWORK SECURITY

- Network Fundamentals
- MAC Addressing and Network Addressing
- Introduction to Port Addressing
- Understanding the OSI Layer and TCP/IP Model
- Domain Name System (DNS) Attack Surface
- TCP vs UDP
- Network Scanning
- Shodan

### LINUX SECURITY

- Introduction to Linux
- Linux Filesystem Hierarchy
- Linux File Permissions
- Berkeley Rsh/Rlogin Services
- Network File System (NFS) Security
- Missing Security Patches
- Vulnerability Identification
- Case Study: Shellshock
- Introduction to Metasploit

### WINDOWS SECURITY

- Windows Fundamentals

- Windows Password Hashing
- Workgroups vs Domains
- Windows Authentication
- Windows Exploitation 101
- Client-Side attacks
- Case Study: WannaCry

### HACKING CMS SOFTWARE

- Introduction to Content Management Systems
- Enumerating CMS Platforms
- Hacking WordPress
- Joomla Exploitation

### WEB SECURITY

- HTTP Protocol Basics
- Understanding Web Application Attack Surface
- SQL Injection
- Case Study: T alkT alk SQL Injection
- Command Injection
- Cross-Site Scripting (XSS)
- Open Redirect

### WIRELESS SECURITY

- WiFi Security 101
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- WPA2 Security
- Wi-Fi Protected Setup (WPS) flaws
- Rogue Access Points Attacks