NOT SO SECURE
A Claranet Group Company

claranet cyber security

Hacking 101

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

- Attendees will gain understanding in the following topics:
- Understand different network topologies and addressing schemes
- Understand the properties and security of common network protocols and the network protocol stacks
- How to fingerprint, enumerate and exploit common Windows and Linux
- Misconfigurations and vulnerabilities
- Differentiate between types of wireless standards and understand the benefits and risks associated with these standards
- How to exploit common web application security flaws

Class Outline

MODULE 1. HACKING FUNDAMENTALS
- Hacking History 101
- Hacking in 2018
- CIA Triad
- Art of Hacking Methodology
- Introduction to Kali Linux

MODULE 2. 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

MODULE 3. 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

MODULE 4. WINDOWS SECURITY
- Windows Fundamentals
- Windows Password Hashing
- Workgroups vs Domains
- Windows Authentication
- Windows Exploitation 101
- Client-Side attacks
- Case Study: WannaCry

MODULE 5. HACKING CMS SOFTWARE
- Introduction to Content Management Systems
- Enumerating CMS Platforms
- Hacking WordPress
- Joomla Exploitation

MODULE 6. 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

MODULE 7. 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

Prerequisites

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

For more information contact
+44 1223 653193
contact@notsosecure.com