HACKING POINT

CHECK POINT

STARTING A CAREER IN WEB HACKING
BOOT CAMP

This 3-day course begins by teaching you the foundations of Pen Testing and how to find and exploit vulnerabilities within different technologies (web applications and underlying infrastructure) and provide insight to how the mindset of a hacker works and leads on to look at the basics of web application and web application security concerns. A number of tools and techniques, backed up by a systematic approach on the various phases of hacking will be discussed.

This course then familiarises the attendees with a wealth of tools and techniques required to breach and compromise the security of web applications. It discusses the very basics of web application concepts, and gradually builds up to a level where attendees can not only use the tools and techniques to hack various components involved in a web application, but also walk away with a solid understanding of the concepts on which these tools are based. The course will also talk about industry standards such as OWASP Top 10 and PCI DSS which form a critical part of web application security. Numerous real-life examples will be discussed during the course to help the attendees understand the true impact of these vulnerabilities. If you would like to step into a career of Ethical Hacking / Pen Testing with the right amount of knowledge, this is the right course for you.

During the course delegates will have access to an online environment platform to practice their new skills.
Attendees will leave with a wealth of hacking tools and techniques crucial in getting started in this dynamic field of hacking

This course is a combination of our Hacking 101 course and our Web Hacking course.

WHO SHOULD ATTEND

- Web Developers
- IT Managers
- Security enthusiasts, anyone interested in Pen Testing and ethical hacking
- Security enthusiasts
- Anybody who wishes to make a career in this domain and gain knowledge of networks and applications
- System Administrators
- SOC Analysts
- Pen Testers who are wanting to level up their skills

PREREQUISITES

Delegates should bring their laptop with windows operating system installed (either natively or running in a VM). Further, Delegates must have administrative access to perform tasks such as installing software, disabling antivirus etc. Devices that don't have an Ethernet connection (e.g. MacBook Air, tablets etc.) will not be supported during the course.

CLASS CONTENT

HACKING FUNDAMENTALS

- Hacking History 101
- Hacking in the modern era
- CIA Triad
- Art of Hacking Methodology
- Introduction to Kali Linux

NETWORK SECURITY

- Network Fundamentals
- MAC Addressing and Network Addressing

NotSoSecure part of claranet cyber security

HACKING POINT

CHECK POINT

- 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: TalkTalk 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

UNDERSTANDING THE HTTP PROTOCOL
- HTTP Protocol Basics
- Introduction to proxy tools

INFORMATION GATHERING
- Enumeration Techniques
- Understanding Web Attack surface

ISSUES WITH SSL/TLS
- SSL/TLS misconfiguration

USERNAME ENUMERATION & FAULTY PASSWORD RESET
- Attacking Authentication and Faulty Password mechanisms

AUTHORIZATION BYPASS
- Logical Bypass techniques
- Session related issues

CROSS SITE SCRIPTING (XSS)
- Various types of XSS
- Session Hijacking & other attacks

CROSS SITE REQUEST FORGERY (CSRF)
- Understanding CSRF attack
- Various impacts of SSRF attack

SQL INJECTION
- SQL Injection types
- Manual Exploitation

XML EXTERNAL ENTITY (XXE) ATTACKS
- XXE Basics
- XXE exploitation

DESERIALIZATION VULNERABILITIES
- Serialization Basics
- PHP Deserialization Attack

INSECURE FILE UPLOADS
- Attacking File upload functionality

COMPONENTS WITH KNOWN VULNERABILITIES
- Understanding risks known vulnerabilities
- Known vulnerabilities leading to critical exploits

INSUFFICIENT LOGGING AND MONITORING
- Understanding importance of logging and monitoring
- Common pitfalls in logging and monitoring

MISCELLANEOUS
- Understanding formula Injection attack
- Understanding Open Redirection attack

NotSoSecure part of
claranet cyber security