HACKINGPOINT

CHECK POINT

START A CAREER IN INFRASTRUCTURE 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 and infrastructure) and provides insight to how the mindset of a hacker works. It moves on to provide you with the basics of network hacking, laying a foundation by discussing the basic concepts and gradually builds up to the level where attendees not only use the tools and techniques to hack various components involved in infrastructure hacking, but also walk away with a solid understanding of the concepts on how these tools work and therefore ready to face the real world.

A number of tools andtechniques, backed up by a systematic approach on the various phases of hacking will be discussed during this course. 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 Infrastructure Hacking course.

WHO SHOULD TAKE THIS CLASS

- 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
- Network Engineers
- Pen Testers who are wanting to level up their skills

PREREQUISITES

The only requirement for this course is that you bring your laptop with an admin/root access. VPN access to our state-of-the-art hacklab, which is hosted in our data centre in the UK where required tools/virtual machines (VMs) will be found, will be provided during the course. We also provide a dedicated Kali VM to each attendee on the hacklab, so you don't need to bring any VMs with you, all you need is to install the VPN client and you are good to go!

COURSE OUTLINE

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
- 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

NotSoSecure part of claranet cyber security

HACKINGPOINT

CHECK POINT™

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

THE ART OF PORT SCANNING
- Basic concepts of Hacking Methodology
- Enumeration techniques and Port scanning

THE ART OF ONLINE PASSWORD ATTACKS
- Configure online password attack
- Exploiting network service misconfiguration

THE ART OF HACKING DATABASES
- Mysql, Postgres
- Attack chaining techniques

METASPLOIT BASICS
- Exploitation concepts, Manual exploitation methodology
- Metasploit framework

PASSWORD CRACKING
- Understanding basic concepts of cryptography,
- Design offline brute force attack

HACKING UNIX
- Linux vulnerabilities, misconfiguration
- Privilege escalation techniques

HACKING APPLICATION SERVERS ON UNIX
- Web server misconfiguration
- Multiple exploitation techniques

HACKING THIRD PARTY CMS SOFTWARE
- CMS Software
- Vulnerability scanning & exploitation

WINDOWS ENUMERATION
- Windows Enumeration techniques & Configuration Issues
- Attack chaining

CLIENT-SIDE ATTACKS
- Various Windows client-side attack techniques

PRIVILEGE ESCALATION ON WINDOWS
- Post exploitation
- Windows Privilege escalation techniques

HACKING APPLICATION SERVERS ON WINDOWS
- Web server misconfiguration
- Exploiting Application servers

POST EXPLOITATION
- Metasploit Post exploitation techniques
- Window 10 Security features & different bypass techniques

HACKING WINDOWS DOMAINS
- Understanding Windows Authentication
- Gaining access to Domain Controller

NotSoSecure part of claranet cyber security