Certified in The Art of Hacking

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Day**

Overview

Securing customer data is often crucial when deploying and managing web applications and network infrastructure. As such, IT administrators and web developers require security knowledge and awareness in order to secure their environment. Due to this requirement, operational staff often require hands-on training and experience to identify, control and prevent organisational threats. This introductory/intermediate technical class brings together Infrastructure Security and Web Application Security into a 5-day “Art of Hacking” class designed to teach the fundamentals of hacking. This hands-on training was written to address the market need around the world for a real hands-on, practical and hacking experience that focuses on what is really needed when conducting a penetration test.

This class teaches attendees a wealth of techniques to compromise the security of various operating systems, networking devices and web application components. The class starts from the very basic and builds up to the level where attendees can not only use the tools and techniques to hack various components involved in infrastructure and web hacking, but also gain solid understanding of the concepts on which these tools are based. This class combines a formal hacking methodology with a variety of tools to teach the core principles of ethical hacking.

- Approaches attackers take when targeting organisations
- Conducting penetration testing engagements step by step and leveraging open source and publicly available tools to gain access to vulnerable systems
- Understanding how to exploit your own network before attackers do

Target Audience

- System Administrators who are interested in learning how to exploit Windows and Linux systems
- Web Developers who want to find and exploit common web application vulnerabilities
- Network Engineers who want to secure and defend their network infrastructure from malicious attacks
- Security enthusiasts new to the information security field who wants to learn the art of ethical hacking
- Security Consultants looking to relearn and refresh their foundational knowledge

Prerequisites

- Basic familiarity with Windows and Linux systems e.g. how to view a system’s IP address, installing software, file management
- Basic understanding of Network fundamentals e.g. IP addressing, knowledge of protocols such as ICMP, HTTP and DNS
- Basic understanding of HTTP fundamentals e.g. Structure of an HTTP request, HTTP method verbs, HTTP response codes

The above requirements are not mandatory but are recommended due to the pace of the class. The Kali 101 course can be undertaken as a prerequisite to this course.

What You Will Learn

- You will be able to discover and fingerprint systems and services available within their infrastructure
- You will be able to discover and exploit Windows and Linux operating systems through a variety of well-known vulnerabilities
- You will be able to conduct password brute force attacks to compromise services and gain access to a host
- You will discover the techniques for hacking application servers and content management systems to gain access to customer data
- You will be able to conduct client-side attacks and execute code on a victim’s machine
- You will be able to identify common web application vulnerabilities and introduce security within their software development lifecycle in a practical manner

FAQs

- The Art of Hacking (QATAOH) course written and updated for 2019 and benefits from the latest vulnerabilities in current and future platforms /systems. E.g. we do not talk about hacking windows XP and 2003 servers (unlike CEH) but talk about circumventing controls in Modern OS such as Windows 2012 / 16 servers. High impact vulnerabilities such and or mass compromise vulnerabilities are taught in the class.
- Unlike CEH, where the focus is to run a tool to achieve an objective which helps attendees pass the exam, we focus on the underlying principles on which tools work and provide attendees an understanding on what is the root cause of the vulnerability and how does the tool work to exploit it. We also talk about how the vulnerability should be mitigated.
- The class benefits from a hands-on lab which is hosted in the NotSoSecure cloud. Every attendee gets their own dedicated Virtual Machines upon which they practice each and every vulnerability in detail.

- In terms of reputation, this course remains one of the most popular class's at BlackHat and other major events. The course is written and taught by pen testers and the training is based on real-life pen testing experience. The Infrastructure component of the class is featuring this year at BlackHat Las Vegas.

Outline

Day 1

- TCP/IP Basics
- The Art of Port Scanning
- Target Enumeration
  - Exercise - ARP Scan (Enumeration)
  - Exercise - Port Scanning (Service Enumeration)
- Brute-Forcing
  - Exercise - SNMP (Brute Force Attack)
  - Exercise - SSH
  - Exercise - Postgres
- Metasploit Basics
  - Exercise - Metasploit Basics

Day 2

- Password Cracking
  - Exercise - Password Cracking
- Hacking Unix systems
  - Exercise - Heartbleed
- Hacking Application Servers on Unix
  - Exercise - Hacking Application Servers (Tomcat)
  - Exercise - Hacking Application Servers (Jenkins)
- Hacking Third Party CMS Software
  - Exercise - PHP Serialization Exploit
  - Exercise - Wordpress Exploit

Day 3

- Windows Enumeration
  - Exercise - Windows Host Enumeration
- Client-Side Attacks
  - Exercise - Hacking Third Party Software
- Hacking Application Servers on Windows
  - Exercise - Hacking Application Servers on Windows
- Post Exploitation
  - Exercise - Windows Hacking - Password Extraction
- Hacking Windows Domains
  - Exercise - Hacking Windows Domains

Day 4

- Understanding the HTTP protocol
  - Exercise - Burp Demo
  - Exercise - Manipulating Headers
- Information gathering
  - Exercise - Information Gathering
- Username Enumeration & Faulty Password Reset
  - Exercise - Username Enumeration
  - Exercise - Password Brute-force Attack
  - Exercise - Forgotten Password Functionality
- SSL/TLS related vulnerabilities
  - Exercise - TLS
- Authorisation Bypasses
  - Exercise - Authorization Bypass via Parameter Manipulation
  - Exercise - Authorization Bypass
  - Exercise - Arbitrary File Download

Day 5

- Cross Site Scripting (XSS)
  - Exercise - XSS (reflective)
  - Exercise - XSS Session Hijacking
  - Exercise - Stored XSS
- Cross Site Request Forgery (CSRF)

    - Exercise - CSRF (Demo)
- SQL Injection
    - Exercise - SQLite (Manual and slap based exploitation)
- XML External Entity (XXE) Attacks
    - Exercise - XXE
- Insecure File Uploads
    - Exercise - Insecure File Upload

End of Course Exam

GCHQ Certified Training (GCT) Exam:

- Online proctored exam taken in class on the final day of the course
- Duration - 70 minutes
- Questions 50, multiple choice (4 multiple choice answers only 1 of which is correct)
- Pass Mark 50%