Cybersecurity series

The Art of Hacking Bootcamp

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 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.

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.

CLASS NAME

The Art of Hacking Bootcamp

CONTEXT

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.

This class will teach students:

- 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

- 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

claranet cyber security

PREREQUISITES

Prerequisite knowledge

- 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 Hacking 101 class by NotSoSecure can be undertaken as a prerequisite to this class.

Hardware requirements

Students should bring their own laptop, and must have administrative access to perform tasks such as software installations, disable antivirus etc. Devices that don't have an Ethernet connection (e.g. MacBook Air, tablets etc.) are not supported.

Software requirements

Windows 7 or 10 operating systems are recommended for the class. Students will be required to install OpenVPN client, an SSH client such as Putty and Mozilla Firefox. Installation instructions will also be provided on the first day of the class

GENERAL OBJECTIVES

On Completion of this class Attendees will be able to:

- Discover and fingerprint systems and services available within their infrastructure
- Be able to discover and exploit Windows and Linux operating systems through a variety of well-known vulnerabilities
- Conduct password brute force attacks to compromise services and gain access to a host
- Hacking application servers and Content Management systems to gain access to customer data
- Conduct client-side attacks and execute code on a victim's machine
- Identify common web application vulnerabilities and introduce security within their software development life-cycle in a practical manner

CLASS OUTLINE

Module 1

- TCP/IP Basics
- The Art of Port Scanning
- Target Enumeration
- Brute-Forcing
- Metasploit Basics

Module 2

- Password Cracking
- Hacking Unix systems
- Hacking Application Servers on Unix
- Hacking Third Party CMS Software

Module 3

- Windows Enumeration
- Client-Side Attacks
- Hacking Application Servers on Windows
- Post Exploitation
- Hacking Windows Domains

Module 4

- Understanding the HTTP protocol
- Information gathering
- Username Enumeration & Faulty Password Reset
- SSL/TLS related vulnerabilities
- Authorisation Bypasses

Module 5

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- SQL Injection
- XML External Entity (XXE) Attacks
- Insecure File Uploads

claranet cyber security

MATERIALS

Students will receive:

- A PDF copy of all class materials used during the class including instructor slide deck, tool cheat sheets and walkthrough guides
- Access to NotSoSecure's Art of Hacking lab for 30 days after class completion