The Art of Hacking Bootcamp

5 Days

2021 EDITION

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 course and experience to identify, control and prevent organisational threats.

This introductory/intermediate technical course brings together Infrastructure Security and Web Application Security into a 5-day "Art of Hacking" course designed to teach the fundamentals of hacking. This hands-on course 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 Pen Testing.

This course teaches attendees a wealth of techniques to compromise the security of various operating systems, networking devices and web application components. The course 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 course combines a formal hacking methodology with a variety of tools to teach the core principles of ethical hacking.

Who Should Attend

- **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 want to learn the art of ethical hacking**
- **Security Consultants looking to relearn and refresh their foundational knowledge**

Attendees will be able to:

- Discover and fingerprint systems and services available within their infrastructure
- 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
- Hack 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

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 course. The Hacking 101 course by NotSoSecure can be undertaken as a prerequisite to this course.

Hardware Requirements: Delegates 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 course. Delegates 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 course.

Delegates Receive

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

NotSoSecure part of claranet cyber security®

For more information:

UK: +44 (0)1223 653 193
US: +1 (628)200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com

The Art of Hacking Bootcamp

5 Days *Continued*

2021 EDITION

Course Outline

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

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®

For more information:

UK: +44 (0)1223 653 193
US: +1 (628)200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com