HACKER
HOUSE

Hands-On Hacking™

Course Syllabus

Table of Contents

Course Syllabus

Course Description

Hacker House Hands-On Hacking course is a 4 day intensive introductory course that teaches applied hacking methodologies in a hands-on practical orientated approach. Our course is engineered from decades of experienced cyber security practitioner's knowledge to educate students on common cyber security tasks. Our course is delivered by expert hackers to prepare students on adversarial thinking and equip them for tasks conducted in a number of different cyber security roles. Our team is dedicated to ensuring that each student is adequately prepared and capable of performing several applied hacking concepts to real-world problems. We teach the theoretical concepts required for each assessment activity, provide instructor led demonstrations and then tutor assisted hands-on practical labs to be completed by each student. Our course lab contents and modules are downloadable and can be re-used by students to continue learning beyond the course.

Our labs are provided as an educational resource to further enhance student learning and as a reference material for on-the-task assessment activities in future. We teach you how to hack into computers so you can better defend against and understand the methodologies used by hackers to breach systems.

Student Pre-requisites

We teach students from a grounds-up approach meaning you are not necessarily an expert in the technology field. Our students have come from all manner of technical environments or are currently attempting to enter industries in technical job roles. We however do require that students can demonstrate technical proficiency and are comfortable with computing tasks. To benefit the most from our course as a student you should be comfortable with the following topics:

- Basic TCP/IP networking
- Comfortable using Linux and performing general computer administration tasks
- Knowledge of programming languages are an advantage but not essential

As this is an introductory course designed for training people into junior and mid-level positions in the cyber security field, you should be competent with configuring your computers network interfaces and doing routine administration tasks beforehand.

If you do not understand basic concepts of computers and networking such as "what is an IP address", "how to list files and processes" or "what is a firewall" then it is advised to take a course in Linux fundamentals and TCP/IP networking before approaching our course. If you can answer the example questions above then this course is likely suitable for you. Typical students attending our course are working in or towards jobs within IT and technology realms.

Laptop Requirements

You will need to bring a laptop that meets the following recommended minimum technical specifications to complete our course:

- 2 or more CPU cores (Intel i3 & above recommended)
- At least 2-4gb of RAM
- Approximately 40-50gb free hard disk space (you may be ok with less)
- Virtual Box (https://www.VirtualBox.org)

You can try a sample of our practical components to assess your suitability before attending for free on the Hacker House website (https://hacker.house/training). This module is intended to be challenging to our students and so do not be worried if you do not complete all of the module, it is intended as a guide to show you what the course is about. There will be plenty of time during the course to sharpen your skills and ask questions of tutors.

Objectives

We teach how to conduct network and application security assessments from a real-world scenario driven hacker's approach. Students who complete our course leave with a core competency of skills that are applicable to many cyber security roles. Students will have performed a number of practical hands-on assessment activities covering different network perspectives and aimed at understanding the how's and why's of how breaches occur. Students completing this course will leave with an understanding of performing the following assessment activities:

- Open-source Intelligence Review
- External Infrastructure Assessments
- Internal Infrastructure Assessments
- Web Application Assessments
- Perform a Penetration Test

Our course will leave students with a clear understanding of the fundamentals in performing security assurance exercises against a range of technologies. This can help assist you with deploying secure platforms, assessing company infrastructure for weaknesses and defending assets such as databases or servers.

Code of Conduct

Hacker House strives to provide an environment that encourages student growth and enables efficient learning. A code of conduct will be provided to students that outlines our anti-harassment policies and expected behaviour of all course attendees. We will not teach students who wish to use the course material to engage in unlawful conduct.

Course Schedule & Format

Hacker House Hands-On Hacking course is divided into twelve modules, these modules are designed to teach fundamental concepts through both theory and practical approaches. Each module will begin with a tutor lecture introducing the necessary technical concepts and background for the practical module. A demonstration will then be performed of the practical lab components. Students are then tasked with completing the module themselves, allowing for one-on-one direct tutoring and assistance with understanding any concepts. The course is taught over a four-day period and at the end of each day a quiz will be used to assess student progress.

This course is not for the faint of heart; we work hard and fast to ensure you get all the concepts and materials you need to learn and begin a career in ethical hacking.

Provided Learning Materials

Students are provided with electronic and paper based learning materials, including lecture notes, configuration guides and command set references. Labs and module materials are provided in electronic formats. Course material can be downloaded onto the student laptop either from a network or through removable media. Notebooks and pens are provided.

Day One

Ethics & Legalities

Description

A module with focus on the ethical and legal issues around network breaches. We delve into a number of legislative issues and viewpoints on ethics. This module is a theory based module that teaches the best practice guidelines when dealing with issues such as vulnerability disclosure, bug bounty programs, laws when hacking and where to seek guidance from.

Objective

- Student will demonstrate an understanding of legal responsibilities
- Student will demonstrate an understanding of ethical practices
- Student will know where to seek legal advice and support

Open-Source Intelligence

Description

Our OSINT module focuses on exposing vulnerabilities and gathering information that is useful to an attacker. We will introduce all the necessary concepts on how to perform wide-reaching intelligence gathering for assisted intrusions into networks. We perform analysis on leaked intelligence and show how you can leverage public data sets to identify weaknesses and better secure organisations.

Objective

- Student will be able to demonstrate practical use of OSINT
- Identify vulnerabilities and weaknesses through OSINT
- Identify exposed accounts and data leaks through OSINT

DNS & Domain Hacking

Description

We explore DNS and associated technologies from the perspective of an attacker. Perform passive reconnaissance and enumeration against a fictional target environment and gain a better understanding of the types of records in use by DNS. We teach how to probe DNS servers for reconnaissance purposes and also how to misuse insecure configurations to perform attacks. Students will compromise and target a misconfigured DNS server.

Objective

- Student will be able to assess domain technology for common weaknesses
- Student will be able to identify misconfigurations and weaknesses in DNS
- Student will conduct vulnerability analysis against and exploit a DNS server
- Student will understand and perform DDoS attacks using DNS

E-Mail attacks & Mail Infrastructure

Description

We review common e-mail server technologies and use in delivering/receiving email. Methodologies on targeting e-mail environments will be presented and assessment activities will be performed to target mail server systems. We will identify and tear down several popular mail server attacks and their use to breach network perimeters. Common protocols such as SMTP, POP3, IMAP and integration with web mail are explored in detail.

Objective

- Student will be able to assess e-mail technology for common weaknesses
- Student will be able to identify misconfigurations and weaknesses in e-mail
- Student will understand and perform attacks against e-mail infrastructure
- Student will compromise an email server

Day Two

Web Server Infrastructure Hacking

Description

Web servers are explored in-depth in this module, covering the basics of web technologies and supporting infrastructure. We review common server side scripting capabilities, application server usages and everything in between. This module will have also serve as an introductory focus on common injection attacks that can be leveraged to gain access to the server. Examples of how to target and exploit common web infrastructure is covered in detail. We look at several high profile vulnerabilities in a real-world scenario with the goal of providing hands-on experience identifying and exploiting such situations.

Objective

- Student will be able to assess web server technology for common weaknesses
- Student will be able to identify misconfigurations and weaknesses in web servers
- Student will understand and perform attacks against web infrastructure
- Student will compromise a web server and perform privilege escalation activities

Virtual Private Networking Attacks

Description

VPN servers are used by individuals and businesses all over the world to secure network endpoints and data in-transit. This module will introduce the methodologies used to expose weaknesses in the initial VPN connectivity, exploit these weaknesses to compromise a VPN end-point and then conduct further analysis on secondary stage authentication processes. We will explore network topologies and designs that can result in significant weaknesses in VPN deployment.

Objective

- Student will breach a VPN environment through common attacks
- Student will explore secondary stage authentication attacks
- Student will demonstrate proficiency in performing analysis of VPN technology

Day Three

File Servers & Internal Infrastructure Attacks

Description

This module marks a shift in learning, moving from external network perimeter assessments and moving towards internal network resources. Students will review common internal network protocols such as FTP, SMB, CIFS, SNMP, TFTP and others to highlight ways in which centralised file storage repositories can be compromised. We cover a range of commonly seen vulnerabilities and misconfigurations that can result in data loss from internal file servers. File permissions and their security models are explored in this module.

Objective

- Student will be able to probe internal servers for common weaknesses
- Student will leverage weaknesses in file servers for unauthorised access
- Student will be able to probe and identify technology in use for file sharing
- Student will demonstrate an understanding of file permission attacks
- Student will be able to use privilege escalation attacks against file servers

UNIX Server Infrastructure

Description

UNIX technology is often found in use through many businesses. This module will explore in detail common attack methodologies used to target UNIX server estates. We will explore numerous protocols and configurations in technologies such as SSH, RPC & X11. This module will explore dozens of common UNIX attacks from both a remote and local perspective. This module will teach how to preform common audit activities against UNIX environments to identify vulnerabilities.

Objective

- Student will compromise a UNIX server through misconfigured services
- Student will gain a detailed understanding of targeting RPC and associated services
- Student will demonstrate ability to exploit UNIX environments for privilege escalation
- Student will be able to audit UNIX environments for weaknesses

Databases

Description

This module deals with database servers and database technologies. We will demonstrate common attack methodologies against a range of different database environments, ranging

from MySQL & Postgres to NoSQL services. We will review common misconfigurations that can be misused by attackers to gain elevated positions within database servers. We teach the core concepts of how to breach a database server for the purpose of extracting information and accessing network resources.

Objective

- Student will be able to identify insecure databases and configurations
- Student will be able to extract sensitive information from databases
- Student will be able to exploit and target database servers
- Student will be able to abuse database configurations for privilege escalation attacks

Day Four

Web Application Assessments

Description

This module builds on the topics explored in earlier modules to present a common network perimeter breach scenario. We explore typical application layer security weaknesses such as Cross-Site Scripting attacks, SQL injection vulnerabilities and XML entity injection flaws. We review typical CMS and deployed web applications to identify vulnerabilities that can be leveraged to gain unauthorised access to data. Identification and exploitation of common flaws and how to leverage them are explained.

Objective

- Student will be able to conduct a basic web application assessment
- Student will be able to identify common OWASP top 10 vulnerabilities
- Student will be able to leverage vulnerabilities to access data and network resources

Windows Enterprise Environments

Description

We present an introductory assessment of a Windows Enterprise architecture, leveraging many popular tools for exploiting Windows environments. The module will help assist in identification of missing patches, misconfigured Active Directory environments, trust and boundary issues as well as common privilege escalation attacks. This course will demonstrate how to leverage common Windows assessment tools and PowerShell to perform hacking attacks against Windows systems.

Objective

- Student will demonstrate how to compromise Windows servers
- Identification of vulnerabilities in common Windows enterprise technologies
- Perform basic lateral movement and privilege escalation attacks on Windows servers
- Audit Windows servers for common attack weaknesses

Art of Password Cracking

Description

This module explores passwords and attacks in detail. We explore concepts such as accelerated password cracking, word list compilation, identification of hash types and algorithms in use.

Objective

- Identify hashing and encryption algorithms
- Extract password hashes from common locations
- Use appropriate tools to target and recover plain-text passwords
- Perform password complexity analysis

Additional Information

Exam & Certificate

Hacker House does not provide a formal examination, instead students are assessed throughout the training to ensure topics and concepts are being learned thoroughly. End-of-day quizzes are assigned to validate student progress and to assist tutors in understanding learning needs. At the end of the course a certificate is presented to students who demonstrate sufficient competency of the course material. Taking the course does not guarantee a certificate and you may not be presented with a certificate if you are unable to demonstrate successful understanding of practical or theory components. Most students who attend our course are able to demonstrate such understanding and providing you have read the pre-requisites this should not be a concern.

Further Reading & Resources

Students attempting our course are often self-motivated learners and ask us for recommended reading guidelines. We have short listed here several books which our tutors and colleagues have found both enjoyable and relevant to the course.

1. NMAP Network Scanning – Gordon Fyodor Lyon (ISBN-10: 0979958717)
2. Silence on the Wire - Michal Zalewski (ISBN-13 978-1-59327-046-9)
3. Network Security Assessment – Chris McNab (ISBN-13: 978-1491910955)
4. Hacking Exposed 7: Network Security – Stuart Mcclure (ISBN-13: 978-0071780285)
5. Hacking Exposed Web Applications - Joel Scambray (ISBN-13: 978-0071740647)

There are a number of websites and resources online which can help students learn Linux fundamentals. Our tutors recommend that you should install Linux and use it as your daily computer for a few weeks to easily grasp the basics. Here are some of our favourite Linux distributions for beginners and general hacking use:

- Ubuntu for Desktops - https://www.ubuntu.com/desktop
- Kali Linux - https://www.kali.org
- Pentoo Linux - http://www.pentoo.ch
- BlackArch Linux - https://blackarch.org

We look forward to seeing you at one of our course events soon! If you have any questions or would like further information then contact the team through our website https://hacker.house. Happy Hacking!