THE COMPLETE ROADMAP TO BECOME

ETHICAL HACKER

~ TheGeekyBoy | Telegram

INTRODUCTION

Are you: a student trying to break into cyberse curity? A tech professional looking to transition into a role in security? Or simply, someone who is interested in hacking and doesn't know how to get started? If so, this post is for you!

Almost all the messages I receive on social media is about becoming an ethical hacker. The road to becoming an ethical hacker is indeed convoluted: there are no colleges offering a "hacking" major and there seems to be an ever-growing list of skills that need to be mastered.

In this post, I am going to outline the skills one needs to become an ethical hacker, and how to go about mastering them. This will give you a good framework on how to get from infosec newbie, to master hacker.

WHO IS AN ETHICAL HACKER

First off, what exactly is an ethical hacker?

A hacker is someone who gains unauthorized access to computer systems using their technical knowledge.

This is illegal and fuels a large part of modern criminal activity.
However, thanks to the change in the landscape in the infosec industry, is it now possible to make a living as a hacker legally. Those who do are referred to as "ethical hackers".
An ethical hacker is someone who attempts to penetrate computer systems and networks with the permission of their owners in order to find security vulnerabilities that a malicious hacker could exploit. This helps organizations strengthen their systems against cyberattacks.

ROADMAP OF AN ETHICAL HACKER

You need to know these skills before getting into Ethical Hacking :-

- Programming and CS Fundamentals
- Networking and OS Fundamentals
- Security Fundamentals
- Pick your Specialisation
    i) Binary Security
    ii) Web Application Security
    iii) Mobile Application Security
    iv) Network Security
- Communication Skills
- Understanding Cryptography
- Practicing Anonyminity
- Practicing These more.

PROGRAMMING AND CS FUNDAMENTALS

Strong skills come from good fundamentals. The best hackers often come from a CS/programming background, because knowing how to build software gives you a comprehensive perspective about how the software works and helps you break them. In addition, an ethical hacker often has to automate large parts of their workflow and programming skills are required for that.

So the first thing to master is basic programming skills. I recommend using Codecademy for this. Codecademy will teach you the basics of how to program. A good general-purpose language to learn is Python. It is easy to learn and great for quickly automating security tasks.

WHY TO LEARN PROGRAMMING FOR ETHICAL HACKING ?

Hackers are the problem solver and tool builders, learning how to program will help you implement solutions to problems. It also differentiates you from script kiddies.

Writing programs as a hacker will help you to automate many tasks which would usually take lots of time to complete.

Writing programs can also help you identify and exploit programming errors in applications that you will be targeting.

You don't have to reinvent the wheel all the time, and there are a number of open source programs that are readily usable. You can customize the already existing applications and add your methods to suit your needs.

WHICH PROGRAMMING LANGUAGE TO LEARN ?

Language : HTML

Purpose : Web Hacking

Login forms and other data entry methods on the web use HTML forms to get data. Been able to write and interpret HTML, makes it easy for you to identify and exploit weaknesses in the code.

Language : JAVASCRIPT

Purpose : Web Hacking

JavaScript code is executed on the client browse. You can use it to read saved cookies and perform cross site scripting etc.

Language : SQL

Purpose : Web Hacking

Using SQL injection, to by-pass web application login algorithms that are weak, delete data from the database, etc

WHICH PROGRAMMING LANGUAGE TO LEARN ?

Language : Python, Ruby , Bash , Perl
Purpose : Building Tools and Scripts

They come in handy when you need to develop automation tools and scripts. The knowledge gained can also be used in understand and customization the already available tools.

Language : C/C++
Purpose : Writing Exploits, Shell Codes etc.

They come in handy when you need to write your own shell codes, exploits, root kits or understanding and expanding on existing ones.

Language : Java , C# , Visual Basic , VB script
Purpose : Other uses

The usefulness of these languages depends on your scenario.

NETWORKING AND OS FUNDAMENTALS

It is also important to understand how computer networks and operating systems work. This will help you understand how a lot of modern exploits work, and how systems are protected against these exploits. To learn computer networking and operating systems, I recommend following college course recordings on Youtube.

SECURITY FUNDAMENTALS

There are a few more things that are helpful to all ethical hackers.

First, make sure you are proficient in using the Linux command line. The command line is the most efficient way of interacting with computer systems, and as an ethical hacker, you will spend a lot of time there. To learn the command line, use LinuxCommand.org.

An understanding of the basics of cryptography is also critical since it is used to protect almost every single digital system out there. A quick read on GeeksforGeeks should give you a good overview.

PICK YOUR SPECIALISATION

There are many specializations you can focus on as an ethical hacker, and they all require expertise in their own set of domain knowledge. You should gain a general understanding of all of these fields and find out which you are more interested in. Then, you should pick one and focus on gaining expertise in that field.

1) Binary Security

Binary security is the field of attacking and protecting binary applications. Binary exploitation is attacking a compiled application to elevate privileges or perform arbitrary actions on a targetted system.

2) WEB APPLICATION SECURITY

You could also focus on the vulnerabilities that commonly affect web applications. As web applications become more complex, securing web applications has evolved into a field of its own. A good way of learning about web applications is by starting with the OWASP top ten vulnerabilities. Then, dive deeper into the architecture and development process of web applications and how they affect security.

3) MOBILE APPLICATION SECURITY

In this field, you learn how to hack and secure applications on different platforms such as Android and IOS. You should focus on learning about the security features and limitations of modern mobile operating systems and the vulnerabilities commonly found on popular platforms.

4) NETWORK SECURITY

Dig deeper into the field of network security, and learn about the vulnerabilities that affect fundamental network technologies. A good place to start is NullByte's posts on Wifi hacking.

COMMUNICATION SKILLS

Communication skills are extremely important for an ethical hacker. Writing and communicating your findings to your clients will be a big part of your job.

Focus on being detailed in your writing, and be as clear and concise as possible when communicating.

Learn to communicate your technical knowledge to different audiences by keeping a technical blog, or by contributing to Wikis or online learning sites

UNDERSTANDING CRYPTOGRAPHY

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.

These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

PRACTICE THESE MORE !!

Lastly, it is not enough to just understand how thing work. It is also important to understand what these theoretical vulnerabilities and defenses look like in real-world applications. So, you should practice hacking and defending

Practice by playing CTFs. A good one to start with for beginners is OverTheWire.

Another good way to practice is by building vulnerable applications with minimal protection, breaking it yourself, and finally implement fixes to protect against the vulnerabilities that you've found. This way, you learn to both hack and protect an application at the same time.

Bug bounties are also a great way to practice. HackerOne and Bugcrowd are two of the biggest platforms, with a wide variety of clients.

Pick a program related to your chosen field of expertise and hack away! On bug bounty programs, you are hacking actual targets instead of simulated ones like in CTFs. So it will be a lot harder, but a lot more realistic.

RESOURCES :- (BOOKS)

-The Hacker Playbook 2: Practical Guide To Penetration Testing

-The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy

-Breaking into Information Security: Learning the Ropes 101

-Penetration Testing: A Hands-On Introduction to Hacking

-Social Engineering: The Art of Human Hacking

-Hacking: The Art of Exploitation, 2nd Edition

-Web Hacking 101

-OWASP Testing Guide (A must read for web application developers and penetration testers)

-The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws

-The Basics of Web Hacking: Tools and Techniques to Attack the Web

VULNERABILITY DATABASES AND RESOURCES

http://www.exploit-db.com/

http://1337day.com/

http://securityvulns.com/

http://www.securityfocus.com/

http://www.osvdb.org/

http://www.securiteam.com/

http://secunia.com/advisories/

http://insecure.org/sploits_all.html

http://zerodayinitiative.com/advisories/published/

http://nmrc.org/pub/index.html

http://web.nvd.nist.gov

http://www.vupen.com/english/security-advisories/

http://www.vupen.com/blog/

http://cvedetails.com/

http://www.rapid7.com/vulndb/index.jsp

http://oval.mitre.org/

http://sploitus.com/

http://cxsecurity.com/

LINUX PENETRATION TESTING OS

Kali Linux

the infamous pentesting distro from the folks at Offensive Security

Parrot Os

Debian includes full portable lab for security, DFIR, and development

Android Tamer

Android Tamer is a Virtual / Live Platform for Android Security professionals.

Blackarch

Arch Linux based pentesting distro, compatible with Arch installs

LionSec Linux

Linuxpentesting OS based on Ubuntu

LEARNING PLATFORMS TO SHARPEN YOUR SKILLS

- CTF Hacker 101
- CTF 365
- Hack The Box : Penetration Testing Labs
- Hack.me
- CTFLearn
- OWASP
- Root-me.org
- Vulnhub.com
- CybersecWTF
- Hacking Articles
- Windows/ Linux Local Priviliges Workshop
- Rafay Hacking Articles
- PentesterLabs
- PentestitLabs

NOTE :

All references taken from Internet and shared on internet .

Thanks to those who shared their opinion before that helped me learn.

Thanks for reading this short summary of some very long books.

MANY THANKS

For reading this Ebook .

THE GEEKY BOY

Telegram | Instagram