

Beginners Guide | How To Become an Ethical Hacker



Hussnain Fareed [Follow](#)

Nov 24, 2017 · 5 min read



Are you tired of reading endless news stories about *ethical hacking* and not really knowing what that means? Let's change that!

This Post is for the people that:

- Have No Experience With Cybersecurity (Hacking)
- Have Limited Experience.

- Those That Just Can't Get A Break

OK, let's dive into the post and suggest some ways that you can get ahead in Cybersecurity.

I receive many emails on how to become a hacker. "I'm a beginner in hacking, how should I start?" or "I want to be able to hack my friend's Facebook account" are some of the more frequent queries. In this article I will attempt to answer these and more. I will give detailed technical instructions on how to get started as a beginner and how to evolve as you gain more knowledge and expertise in the domain. Hacking is a skill. And you must remember that if you want to learn hacking solely for the fun of hacking into your friend's Facebook account or email, things will not work out for you. You should decide to learn hacking because of your fascination for technology and your desire to be an expert in computer systems. It's time to change the color of your hat 😊

I've had my good share of Hats. Black, white or sometimes a blackish shade of grey. The darker it gets, the more fun you have. -MakMan

Introduction!

First off, let's just agree that saying 'a Career in Cybersecurity' is a bit like saying 'a Career in Banking', i.e. it's an umbrella term that incorporates dozens of niches within the industry. In Cybersecurity we can, for example, talk about digital forensics as a career, or malware/ software detecting, auditing, pentesting, social engineering and many other career tracks. Each of these sub-categories within cybersecurity deserves a separate blog post, but, for the purposes of this piece, let's focus on some important generic requirements that everyone needs before embarking on a successful career in IT Security.

If you have no experience **don't worry**. We ALL had to start somewhere, and we ALL needed help to get where we are today. No one is an island and no one is born with all the necessary skills. Period.OK, so you have zero experience and limited skills...my advice in this instance is that you teach yourself some absolute fundamentals.

Let's get this party started.

1. What is hacking?

Hacking is **identifying** weakness and vulnerabilities of some system and **gaining access** with it.

Hacker gets unauthorized access by targeting system while *ethical hacker* have an official permission in a lawful and legitimate manner

to assess the security posture of a target system(s).

There are some types of hackers, a bit of “terminology”.

White hat — ethical hacker.

Black hat — classical hacker, get unauthorized access.

Grey hat — a person who gets unauthorized access but reveals the weaknesses to the company.

Script kiddie — a person with no technical skills just used pre-made tools.

Hacktivist — a person who hacks for some idea and leaves some messages. For example strike against copyright.

Actually, a goal of ethical hacking is to reveal the system weaknesses and vulnerabilities for a company to fix them. Ethical hacker **documents everything** he did.

2. Skills required to become an ethical hacker.

First of all to be a Pentester you need to be willing to continuously learn new things on the fly and or quickly at home. Secondly, you need to have a strong foundational understanding of at least one coding/scripting language as well as an understanding of Network and Web Security.

So here are some steps if you want to start from now...

1. Learn To Code (Programming).

2. Understand basic concepts of Operating System
3. Fundamentals of Networking and Security
4. Markup and as many technologies as you can!

3. What Platform To Code In:-

That depends on what platform you'll be working on. For web applications, I suggest you learn *HTML*, *PHP*, *JSP*, and *ASP*. For mobile applications, try *Java (Android)*, *Swift (iOS)*, *C# (Windows Phone)*. For desktop-based software try *Java*, *C#*, *C++*.

I would like to recommend *Python* as well because its a general purpose language and getting more popular nowadays due to its portability.

But what really is necessary for every programming language is to learn the fundamentals of programming, concepts like the data types, the variable manipulation throughout the program at the OS level to the use of subroutines aka functions and so on. If you learn these, it's pretty much the same for every programming language except for some syntax changes.

ProTips:-

1. To be an expert at any programming language, understand the OS level operations of that language (varies in different compilers) or

- learn assembly language to be more generalized
2. Don't get your hopes high if you can't achieve results in a short span of time. I prefer the "Miyagi" style of learning. So keep yourself motivated for what comes next.
 3. Never underestimate the power of network and system administrators. They can make you their *hypothetical* slave in a corporate infosec environment 😊

Resources To Get Started:

I would like to share some resources that I found best in learning from scratch.

Breaking into Information Security: Learning the Ropes 101

All of the basic topics to get you from zero to junior pentester level - covering off everything you need to know

leanpub.com

Web Hacking 101

On December 22, 2015, Twitter paid over \$14,000 to ethical hackers for exposing vulnerabilities. This wasn't a...

leanpub.com

There is a whole list of resources I have created for your help 😊

(<https://github.com/husnainfareed/Resources-for-learning-ethical-hacking/>)

Another advice..... Regularly follow <http://h1.nobbd.de/> to b updated with **HackerOne** Public Bug reports You can learn a lot from them, Follow <https://www.owasp.org/index.php/Cat...>

Alternatively, You can Join Slack Community for Hackers

<https://bugbounty-world.slack.com/>

<https://bugbountyforum.com/>

| Also You should Consider practicing Your Skills on

<http://www.itsecgames.com/>

<http://www.dvwa.co.uk/>

<http://www.vulnerablewebapps.org/>

<http://hackyourselffirst.troyhunt.com/>

<https://github.com/s4n7h0/xvwa>

<http://zero.webappsecurity.com/>

<http://crackme.cenzic.com/kelev/view/home.php>

<http://demo.testfire.net>

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

HackerOne Public Reports!

These Reports might help you guys to get some in-depth idea of BugBounty hunting...

HackerOne Public Reports.csv

Some of the points to be noted:

- **By a Self-Learner:** Why? Because without it you won't learn from things you experience, you won't be able to solve your problems.
- **Educate your self on daily basis:** read articles, write-ups, videos or slides to educate yourself
- Know your target, before proceeding make sure to know your target. Invest most of your time in identifying your target identifying the services the target uses.
- **Map the target:** get a better view of the target's infrastructure in order to get a better understanding of what to target.

- **Walk the path no one travels:** Don't be the common dude out there. Think out of the Box, think what the developer missed think what common guys are targeting, depending on that choose your path.
- **Be a ninja:** You need to be fast and precise as a Ninja. Know, Map, Target your victim precisely and quickly. This only works if you are good are talking the different path and if you are unique.

If you want to know more about Recon and how to chase Bug Bounty read this article **“How To Do Your Reconnaissance Properly Before Chasing A Bug Bounty”**.

Let's hope you are not going to blacklist this post for the rest of your life. I have a lot of interesting stuff coming up. Ciao.

If you enjoyed this story, please click the 👏 button and share to help others find it. Feel free to leave a comment.