How to Learn Penetration Testing: A Beginners Tutorial

Katerina Borodina Mar 15 *Updated on Mar 20, 2019* • 9 min read

#security #beginners #webappsecurity #webdev

❤ 185 🦄 41 336 DISCUSS ■■■

Disclaimer: Hacking is a difficult skill to learn. You will not become a good pentester by just doing a few online courses. You will not become a good pentester by just installing Kali Linux and learning how to use the tools. This is a challenging path, wrought with endless frustrations, and you will not learn how to travel it well within a day - a month - or even a year. However, if you're determined, you'll find pentesting to be an incredibly rewarding field and you might never want to leave.

*In this tutorial, I'll specifically cover the **web application hacking** side of penetration testing. This is a guide for ethical hacking. If you're doing the unethical sort, I'd really rather you not. Or at least give me part of your profits, please.*

Assumed knowledge:

- *Basic technical background (Unix commands, some software development skills)*
- *Intense desire to break things*

❤ 185 🦄 41 🔖 336

0 - The Background Knowledge

Some CS101 knowledge is a must. Trying to learn how to hack without even being comfortable with Unix commands wouldn't just be like trying to run before you can walk. It'd be like flying an A380 without knowing which direction up is.

If you try to jump into pentesting without the necessary prior knowledge and

How to Linux: The main power of Linux/Unix for coding and pentesting comes from the terminal and the sheer number of tools available. You can *try* to do everything you need in Windows, but it's not going to be easy - and if you're getting into pentesting, you'll need to know some Linux eventually. Trust me: if you get a job in security and your coworkers find out you've never used Linux, they'll laugh at you forever.

You have three main options here:

- Get an install of a Linux distribution (such as Ubuntu). Your best option for this is to download a virtual machine software where you can contain your Linux install (links down below).
- Keep using macOS, if you have it. You can make do with this since the terminal and tools on Macs are pretty much the same as Linux.
- Use Ubuntu on Windows 10. I'd consider this the worst option for a beginner because it can be pretty unreliable when it comes to installing tools, and getting the GUI to work can sometimes be a nightmare.
- VirtualBox: Free virtual machine software
- Ubuntu: Decent Linux starting distro

❤ 185 🦄 41 336

- Unix commands for Beginners

How to Code: Now that you have your environment set up, we can get to the fun bit! Learning some basic coding skills is essential to pentesting. If you want to learn how to break it, first learn how to make it. For web application pentesting, you'll want to learn some full stack stuff such as HTML, CSS, Javascript, and Python. Python has the added benefit of being a great language for scripting and will allow you to write your own pentesting tools (exciting!).

- Learn front-end
- Learn Python

1 - Set up Your Environment

If you're a dev, you probably have your perfect setup already. Gratz! The way to go here is usually Linux or Mac. Personally, I use Ubuntu on Windows 10

❤ 185 🦄 41 🔖 336

Many beginners start with Kali, but I recommend against this. Part of becoming a confident pentester is building your library of tools. Kali hands you a bunch of tools, none of which you'll really understand and appreciate.

But whatever you're doing, it's *absolutely crucial* that you have a comfortable setup. Take some time now to fix any issues you might have in your setup (like bootloaders, window managers, GUI, etc). Pentesting can get messy when you have countless windows and complicated tools open, and the last thing you need is your own environment working against you.

2 - Learn the Theory

No way around this one. Even in just web application hacking, there's a whole breadth of knowledge you need to know. I'd split web hacking knowledge into two categories: The Basics, and the Nifty Tricks. The Basics are what you should learn first from books, videos, online tutorials, etc.

Unfortunately, given how quickly the world of hacking moves, most to know them!). The Nifty Tricks are the real moneymakers. You'll learn these later through browsing experienced pentesters blogs, joining ethical hacking communities, and obscure Youtube videos. If you're the first to discover a Nifty Trick, you get a place in The Hall of Fame and maybe lots of money.

Here are some great resources for The Basics:

- The Web Application Hacker's Handbook: This is a great starting point. This covers almost all the basics you need. But don't bother with the "lab" that comes with the book.
- OWASP's Testing Guide: OWASP is a key player in web application hacking, and this guide is *immense*. It has a lot of what you'd need to know.
- LiveOverflow on Youtube: This guy is great - he covers a lot of The Basics and also plenty of Nifty Tricks.
- Hacksplaining: Lots of info on different vulnerabilities.
- SecHub: A compilation of a bunch of different exploits, with writeups too! Super cool

❤ 185 🦄 41 ⚡ 336

- Learn the HTTP TCP/IP Model, basic networking, and packets. You'll need this, trust me.

Once you've learned and practiced The Basics (more on how to practice in the next section), you can move on to learning some Nifty Tricks. Some resources:

- DEF CON videos are great.
- Vulnerability writeups: There's a lot of places to find them, and Medium can be a good one. Check out r/Netsec too. Also Google the vulnerability you want to learn more about with the word "writeup" or "POC" appended, e.g. "XSS writeup". You'll find posts from very clever people about new ways they've found to exploit stuff.
- Look for pentesting communities and join them. Hacking, surprisingly, is a very social field, and a lot of cool tricks can be learned just by talking to other pentesters.

3 - Practice with CTFs and Wargames

❤️ 185 🦄 41 336

This is the fun bit. Once you have some theory down, you can start practicing by doing hacking challenges. These are vulnerable web applications with hidden "flags" that you find by exploiting the application.

CTF (Capture the Flag) competitions are live events with scoreboards and teams, while wargames are less competitive and are more like playgrounds to practice your skills on.

Check out CTFtime for current and upcoming CTFs, although most of these will be too difficult for a beginner. Good wargames are OWASP's WebGoat and OverTheWire. Also check out OWASP's Juice Shop, Hacker101 CTF, Hack The Box, and Google's XSS game.

While fun and a great way to learn, note that the skills you need for wargames/CTFs are somewhat different from the skills you need for real-life applications such as bug bounties. It's possible to be a top scorer in CTFs, but be utterly incapable of doing bug bounties (this was me for a while) and vice versa.

❤ 185 🦄 41 🔖 336

Wargames are to bug bounties what Civ5 is to running an actual country. Wargames teach you some excellent strategy and puzzle solving skills, but real life is a different landscape - more on this in Section 5.

4 - Get Good at Scripting

This will make your life much, much easier. Python is amazing as a scripting language, especially for hacking. A lot of CTFs and bug bounties will require brute force actions such as sending many packets and hashing, all of which can be done easily by writing your own Python scripts.

Check out pwntools, a Python CTF framework. It simplifies exploit writing! Here's how you send packets.

I recommend making a folder where you keep your own Python scripts and build on them over time. I really can't understate how much time this will save you.

❤️ 185 🦄 41 🔖 336

5 - The Real World and Bug Bounties

At some point, you'll get the flag for your first moderately difficult CTF challenge without having to Google the solution. And you'll feel amazing. Likely, you'd have spent hours and hours on it, and finally figuring out the answer on your own will be a feeling that'll get you hooked on pentesting forever.

You're a hunter now. Fierce. Unstoppable.

You might even think that you're ready to start making money now. But once you check bug bounty sites, you'll realize you have no idea what you're doing. There are no clues telling you where vulnerabilities are. There's such a wide attack surface that you don't even know where to start. And thousands of better hackers have already wiped the site clean.

As disheartening as it might be, this is the point where the fun really starts. You're out of the playground and ready to play with the big kids now. A good starting point is watching this DEF CON video I linked earlier and digging into finding good tools and more Nifty Tricks.

Now is the time to start learning web reconnaissance. It's covered well in the DEF CON video, and you'll learn more about it as you build your library of recon tools.

6 - Know thy Tools

Tools don't make a hacker. But you're probably not going to get too far

I recommend starting off with just downloading a couple of the "mandatory" tools like Nmap and Burp Suite. Nmap is a discovery tool that finds hosts and open ports on domains, generally giving you a good feel for what the network looks like. And Burp Suite is your new best friend. Seriously. It's the #1 multitool of web hacking. Its main use is capturing and editing packets, but it does so much more. I really can't give it justice in this blog post - just google it and watch some tutorial videos.

After those two, it's up to you to find (or make) the tools that suit you best. Here are some of my favorites:

- Sublist3r: I'm absolutely in love with this subdomain enumerator. It's crazy quick and finds a bunch of stuff.
- Aquatone: Similar to Sublist3r but much more robust. Trades speed for power; I usually run Sublist3r first and then keep Aquatone in the background.
- dirsearch: Directory bruteforcer.
- LinkFinder: Discovers endpoints in Javascript files.
- recon-ng: An entire framework for web reconnaissance that does pretty

❤ 185 🦄 41 336

if you find the right setting.

- SecLists: Not a tool per se, but a collection of lists for bruteforcing. Pretty much a staple of web pentesting - I'd almost put it in the mandatory section.
- Spotify hacking mixtapes for feeling cool

7 - Keep Hacking

I told you it'd be difficult, didn't I?

Pentesting is challenging, confusing, and overall just frustrating. But if this is something you really want to do, you'll find ways to overcome all of that.

Try to join communities, such as the ones on Twitter and Bugcrowd, since the journey is always more fun with others.

And remember: this is a field that *really* matters. It's rewarding, and you'll be doing legitimate good for the world. Blackhat hackers are learning every

❤ 185 🦄 41 336

day too, and the ethical hacking community needs all the help it can get. Good luck, and godspeed!

This post was originally published on explainhownow.com

✋ **Hey dev.to reader.**

Do you prefer **sans serif** over **serif**?

You can change your font preferences in the "misc" section of **your settings**. ❤

Katerina Borodina **+ FOLLOW**

I do cyber security, particularly web application testing.

@kathyra_ kathyra_ www.explainhownow.com

Add to the discussion

❤ 185 🦄 41 336

PREVIEW SUBMIT

▼

Alexander Khovansky

Mar 15

Great article! Many useful tools listed.
That Civ5/real country analogy made me chuckle, so true.
Too often on HackTheBox labs you find something conveniently hidden in plain sight that contains plaintext password, or weak password hash from the top of rockyou.txt wordlist in Kali.
Haven't had this much luck with real world environments so far.

♡ 5

REPLY

▼

Katerina Borodina Author

Mar 15

Thanks Alexander! :)
Yeah I was a little iffy on whether to add HTB at all but I figured it was probably good for beginners, to at least build up confidence.
I was definitely in for a shock when I went from ctfs to the real world!

♡ 3

REPLY

▼

❤ 185 🦄 41 336

I just turned 31 and have been doing internet marketing (mostly SEO) for the last 10+ years. I’m ready for a career change.

I’m fascinated by this kind of stuff but it feels like I’m too late and too old to start now. Any advice?

♡ 3 REPLY

▼ Katerina Borodina Author Jun 30 ▪▪▪

No way you are NOT too old!! Hacking might seem like an intimidating field to enter, especially because so many of the "pros" have been doing it since they were kids. But there's just as many amazing pentesters who entered the field later in their career.

Plus, security is such a diverse area, with so many people from different backgrounds. Having experience in internet marketing could give you a totally different, very valuable perspective that others don't have.

♡ 2 REPLY

▼ Garrett Jun 30 ▪▪▪

I have found my SEO experience has made me particularly good at OSINT.

❤ 185 🦄 41 336

Katerina Borodina Author

Jun 30

Hell yeah!! That's awesome!

♡ 1

REPLY

▼

Adam Duncan

Mar 18

I’m interested in ethical hacking and this was a really great intro piece. Thanks for taking the time to do it!

♡ 4

REPLY

▼

Katerina Borodina Author

Mar 18

Awesome! Good luck :)

♡ 1

REPLY

▼

Ari Kalfus

Mar 18

❤️ 185 🦄 41 336

guardrails. And you get infinite time to play on it. I'm sure you're aware of juice shop but I was surprised it wasn't mentioned here.

♡ 2 REPLY

Katerina Borodina Author Mar 18

Good call. Added Juice Shop!

♡ 3 REPLY

Peter Ellis Mar 24

What I would add is that all of this exercise and tool knowledge is also very useful for every single web developer who builds customer-facing applications.

♡ 3 REPLY

Katerina Borodina Author Mar 24

Absolutely! I think security is a pretty neglected side of development. Then again, if web devs followed security practices, I probably wouldn't have a job.

❤ 185 🦄 41 🔖 336

almokhtar bekkour

Mar 15

Thanks, that was useful!

♡ 3

REPLY

Katerina Borodina Author

Mar 15

So glad to hear that! :)

♡ 2

REPLY

Abdur-Rahmaan Janhangeer

Mar 19

```
#AMostUseful
```

♡ 2

REPLY

code of conduct - report abuse

❤ 185 🦄 41 336

Classic DEV Post from May 21

Ten Cognitive Biases to Look Out For as a Developer

Frank Rosner

Cognitive biases can be viewed as bugs in our thinking. In this blog post we want to take a look at ten cognitive biases to look out for as a developer.

❤ 140 💬 16

Frank Rosner

+ FOLLOW

From one of our Community Sponsors

How to Use Git to Manage Your Writing Project

Brian P. Hogan

DigitalOcean

+ FOLLOW

❤ 185 🦄 41 🔖 336 🐦

changes, view the difference between those changes, and review the previous version.

❤ 180 💬 12

Another Post You Might Like

I left my job today after 7 years

James Turner

Sometimes you need to risk it to get the biscuit...

❤ 118 💬 29

James Turner

+ FOLLOW

Another Post You Might Like

❤ 185 🦄 41 336

What’s an unpopular software opinion you have?

Ben Halpern

Please share! ...

❤ 77 💬 322

Ben Halpern

+ FOLLOW

What are debounce and throttle functions, and how do you write them in JavaScript and React?

Lee Warrick - Oct 18

Awesome Frontend Security

Nazym J - Oct 18

Cutting Azure Costs 💰

Aaron Powell - Oct 18

Svelte 3: Usando blocos "if"

Eduardo Rabelo - Oct 18

❤ 185 🦄 41 🔖 336

❤ 185 🦄 41 🔖 336