# [GUIDE] How to become a professional Pen-Tester

## First Steps Down a Lengthy Road

A pentester must know a lot about a lot, while specializing will be a goal after you are hired, you must be a general expert in many fields of study. It can be very daunting for a budding infosec student or hobbyist to look at everything a pentester should know. A lot I.T people will fantasize about being a pentester, but most of them won't even start the process because it seems very difficult and time consuming. And they are correct. If you don't absolutely love security testing, talking about security subjects, learning new techniques, and having to spend hours (if not days) to figure out a problem, then this is not for you.

Still here? Alright lets dig into what subjects make up the core knowledge an entry level pentester should be very well versed in.

### 1. Networking

One of the most essential skills for a penetration tester to learn is how computers talk to each other. Learn the ins and outs of TCP/IP, 3-way handshakes, protocols and packet inspection. Get to the point where you can go to a white board and map out a network communication using the OSI module and write in depth how it all works. Don't just know each level of the OSI module, fully understand each level, know every protocol associated with each level. This is crucial because analyzing traffic through packet dumps you will need to analyze every wrapper, every address, etc. An expert will be able to read and manipulate network traffic on the packet level, once you have that sort of understanding you are solid.

How to prepare:

* Study Network+, CCNA Security, read TCP/IP Illustrated Part 1.
* Practice with Wireshark, inspect traffic, understand how packets are created and transmitted.
* Study HTTP, know it inside and out. "HTTP The Definitive Guide" is a great resource.
* Use Burpsuite (more on this later) to proxy and inspect web traffic.

### 2. Understanding the Internet

In the networking section I mentioned HTTP and Burpsuite, so lets discuss that next. Most people think they understand the internet, they are wrong. Can you write out a full HTTP request and response? Do you know every HTTP verb? Do you know the difference between HTTP 1.0 and HTTP 1.1 and HTTP 2.0 or HTTP 0.9 without having to research it? Do you know most of the HTTP response codes, not just general information but specific codes. Do you know how a CDE works?

Ok lets assume the answer to most of that is no because most people don't actually study how the internet works. When you are performing web application testing, code review, and API review, you will need to know how it all works.

How to prepare:

* Read "HTTP The Definitive Guide"
* Read "The Tangled Web"
* Be familiar with RFC 2616 and other related RFCs.
* Practice inspecting web-traffic with both Wireshark and Burpsuite.

## 3. Operating Systems

As a pentester you will have to test all operating systems. You don't get to choose only Windows environments running only Windows 7 and below. You will run into many different types of environments, running Linux and Macs as well and Windows. You should be comfortable with all types of operating systems and how to enumerate information, use of command line (CMD, Powershell, Bash), and how to download/install and execute programs. Looks simple but that is a lot of knowledge. If you got access to Windows Server 2012, could you change roles, add a new admin, push updates etc? If you got on a Ubuntu Box as a webuser, can you enumerate to find insecure files or permissions? Of course you don't need to memorize everything, Google is your friend, but you should have a general knowledge of how to do everything and use Google as a backup for the fine details.

How to prepare:

* Create a VM of at least one Linux distro and one Windows Server. A Mac VM would be handy, but it is similar enough to Unix that knowing Linux commands will at least help. With those VM's or using them as hosts, attain admin level knowledge of their functionality. There are many web courses, books, and websites that will provide you with great knowledge.

## I Have the Core Knowledge, Now What?

Congratulations, if you attained all the core knowledge listed above, you are no longer a noob. That is a lot of knowledge to have about technology and with it you can probably get a decent entry level tech job. Now it is time, if you haven't already, to get a job. Most pentesters come from varying backgrounds such as Network Admin, I.T Helpdesk, Security Analyst, Web Development, Programmers, and more. The point is, get a job in technology, doesn't need to be security related immediately though that is a bonus. At this point you should also look at getting a few certs, Network+ and CCNA would be great for getting into a networking job. MCSA is good for geting into a System Admin role. If you mastered the core knowledge then you should have no issues getting a few of the entry level certs.

You may be asking, why wasn't programming listed as core knowledge. There is a good argument that it should be but I think programming should be part of the next step. Mastering everything in the first section will take at least a year or two depending on how fast you can learn, your current background in technology, etc. Adding programming on top of that immediately will take up even more time, and if you don't have a reason to learn coding yet then you are likely to forget a lot.

Ok so now you have a job in I.T, it pays Clay Davis but it looks good on the resume. Every job you have from now on will be a stepping stone. Don't expect to remain at any one job for more then two years because the way to the top is a ladder and getting complacent will get you stuck on a lower rung. Of course if you do find that you really enjoy being a Network Admin, System Admin, Security Analyst and don't feel like pursuing Penetration Testing, that is perfectly fine. Those jobs are great and will provide you with a good future.

Now though, for those who want to keep climbing the ladder, we start to dig deep into security.
How to Become a Hacker?

1. Learn Defensive Security

Probably one of the most asked questions on HF is how to become a hacker. Well to start off if you mastered those core topics you are well on your way. Now we can apply security to each of those core topics. I find it best to learn Blue Team (Defensive Security) before jumping into Red Team (Offensive Security). Because while studying defensive security first you will also learn about offensive security. And any pentester should know what kind of defenses may be in place to prevent a reverse shell, code execution, logging, standard AV behavior and more. Also going down this route can lead to a security analyst position which is a great lead into penetration testing. Of course you can skip this step if you want, learn the advance subjects listed later, and you probably can still get into penetration testing. This is only my recommendation.

How to Prepare:

* Study: Security+ and CISSP (don't have to get cert but at least study).
* Understand common defense techniques such as how Anti-Virus works, how Web Application Firewalls work, how Firewalls/IDS/IPS work and where they are installed in networks.
* Create your own lab setup, play with setting up Splunk and other free security tools.
* Study compliance such as HIPPA, PCI DSS, and FedRAMP. Study standards such as ISO 9000 and NIST.

At this point you should be able to design, at least on paper, a fully secured network and understand each type of security device you put in place for the layered security. You also should be able to write a Security Policy and understand different security controls based on the compliance or security standard any company may want to utilize.

If you are not a Security Analyst or on an I.T Security team at this point, start applying. You now have the knowledge to get at least a level 1 security position.

2. Can I Start Coding Yet?

Yes, now it is time to learn how to write programs. One thing to keep in mind is that you don't

**need to be a programmer to be a penetration tester. In fact, unless you already are a programmer, studying to become one would be a waist of time. What you should know though is the basics of computer science and how to write at least basic scripts/programs for security testing. We want to know how to test applications, find insecure code and exploit it, but we don't need to be dev ops to do that. Of course the more you know about programming the better you will be at testing it, but that is only one of many areas a pentester needs to know. If programming is your thing then you should start that much earlier in the training, add it to your core knowledge set, go to school for it, and make that your job. You can later move to penetration testing if you want but there are better jobs in my opinion, such as Malware Analyst (reverse engineer) or Security Researcher (finding and creating zero days exploits). Both of which rely heavily on being an expert at programming and are also awesome jobs.**

**For penetration testers though we want to keep it simple. Python is a great language to learn and master. You can learn about computer science with Python, write custom security tools etc. Python runs natively on Linux and Mac and soon Microsoft will be adding it natively on Windows. I recommend learning Python 2.x first but also know how to write in Python 3.x. There are a ton a great free resources for learning Python but the one I found most useful for starting out is "Learning Python the Hard Way". After that you can move to books like "Black Hat Python" and "Violent Python".**

**While I recommend sticking with one language until you truly mastered it, there are other languages that will be valuable to learn, at least to the point where you can read source code and understand it.**

*** C and ASM for exploit development.**
*** PHP for server side.**
*** HTML for web development.**
*** JavaScript for client Side.**

**By no means is this a complete list of languages to be familiar with but it is a great start. Once you understand programming basics it really comes down to learning different syntaxes. Of course there are many differences between Python and C (not to mention ASM) but you should be able to jump into C and be able to apply some previous knowledge to it. Once you know the basics, one of the best ways to learn coding is to review source code found on github and other places.**

**3. Learn Offensive Security**

**At this point you should be level 2 or 3 in whatever security job you chose. You know all the security lingo, you can program, you can develop security policies and perform risk analysts etc. You are comfortable and an above average user on any operating system. You should also have at least two to four certifications. So lets get into the nitty gritty of popping shells. Once you start really digging into security testing you will understand why you had to learn so much other information first. Imagine attempting a reverse shell from a friends computer to your local host, and nothing happens. You don't understand, the software worked in your personal lab so whats wrong? Well that is where networking knowledge comes in. Maybe the program does not have the correct permissions, maybe an AV is blocking it, there are many possibilities and if you lacked the above knowledge you would be stuck, probably writing a post on HF asking for help. But because you followed this tutorial and you studied hard for the last few years, you can easily**

troubleshoot the problem. Now it is time to learn about the art of hacking.

How to Prepare (in no particular order):

** Highly recommend reading "Web Application Hackers Handbook". Know it inside and out.
* Pick up a book on the basics of hacking. The material will be very out dated but it will provide you solid knoweldge.
* Use YouTube and other sources to learn about: getting shells such as php shells, reverse shells, bind shells, etc.
* Learn about enumerating a host, port scanning, manual and automated methods of searching for security vulnerabilities.
* Learn how to exploit well known vulnerabilities, such as MS08-067 and MS17-010.
* Learn basics of privilege escalation methods, both manual and automated.
* Learn how to enumerate hosts in a network, capturing packets in wireshark, doing broadcast scans with nmap, using netbios and smb to enumerate hosts etc.
* Learn how to research for vulnerabilities.
* Be able to modify scripts to fit your needs. And be able to troubleshoot older exploits to work with more modern libraries.

Truly there is a lot that I didn't cover. This section is more about organic learning then a strict regiment. You will bounce from topic to topic. As you learn more about one subject you will find something you don't understand and you will study that as well. For a more controlled learning environment I would suggest some online courses. They are expensive but they will provide a more comprehensive and structured form of learning. The PWK is good for those who are already advanced with the core hacking subjects. While elearnsecurity is very good for those who need a bit more hand holding to learn the same (and more) skills that the PWK teaches. Your goal now is to get the OSCP but you can get something like PPTP first to help prepare you for PWK.

4. Practice Practice Practice.

Now its time to put all that information to practicle application. Time to practice your skill set. There are a couple of methods to practice legally.

1. Build your own lab.
2. Use an online lab.

In this day and age there is no reason not to use online labs except if you want to be familiar with how to set up a virtual lab. There are many free labs online including "hackthebox.eu" and "hackthissite.com" as well as others. Then there are paid for labs which are very beneficial such as "pentesterlabs.com". You can also look into Vulnhub.com to find pre-made insecure vm images to practice on. The point is, you should be actively practicing security testing in lab environments, this is the best way to learn.

Steps 3 and 4 will take you at least one year, especially if you are actively working full time. Once you have a couple of advance certs like the OSCP, it is time to move on.

Time to Become a Penetration Tester

**If you followed the steps I provided then going from a complete noob (knew nothing about security, networking etc) to penetration tester will take around 5 to 7 years. This time will obviously be shorter if you are already in the IT field, have gone to college for computer science or related field etc. So if you start at the age of 16 you can probably get a penetration tester job by 23 or so, not bad. I started much later in life and it took me about 6 years from starting college to getting hired as a penetration tester. By now you will be very versed in infosec and related technologies. Your resume will be great, multiple certs, multiple jobs showing a clear climb in expertise and desire to improve yourself. You will be more qualified then most people who are applying to Penetration Tester jobs. 100% if you apply to enough places you will get a job.**

**I recommend applying to places that are entry level friendly. Because even with the jobs you had and the expertise you have in labs...that is not practical experience. You will start as a level 1 (or whatever they call it) for at least the first year. But once you have one year of real experience you are golden. If after two years you are not making $100k, look for a new job because you are worth it.**

## Conclusion

**I never expected the post to be so long, it was some task summarizing a road-map to becoming a penetration tester. For all of you that stuck to it and read the entire post, my hats off to you, and I believe you have what it takes to succeed. Researching will be long and arduous, you will be baffled, confused, and read stuff so dry that that every distraction would be welcomed. But that is what it means to be a professional and not just a hobbyist.**