

Forum:[Hack Forums](#)

Thread: [how to start a new career](#)

0x00 - April 4, 2018, 12:52 pm

This is my first post here, so first of all, hello world.

I know u are sick of this type of post but i need a piece of advice from you, it doesnt matter if that hurts, be honest.

I work as a developer in a big company meanwhile im finishing my degree in computer science, but i dont want to work as a developer anymore im trying to focus in security.

I want to start a new carreer in cybersecurity maybe as an ethical hacker, but i dont know if im in the right path or how to start properly. I was always interested in security but i didnt realize that it can be my job too. I always read security books, i read about new bugs, new issues,etc. when i code, and i always think if my code could be broken or if someone can bypass my programs, and of course i think how to break other people programs/code but i didnt started to hack anything seriously.

I know C,C++,Java,Python,JS and derivates,PHP and a others languages.

About databases, I know MySQL, Oracle SQL, SQLite and Im familiar with Mongo and lucene sintax.

In terms of servers mainly Linux iptables,SELinux etc. Debian and Red Hat, so i know Apache,Tomcat and a little bit of Node, about Windows servers i dont know too much because when i worked with Windows server all was working fine and all i did was maintenance. About bash i used to write my own scripts.

I have some knowledge of how to stay anonymous things like Proxies,VPN and tor but i didnt used that for anything more than privacy and curiosity.

About programs i dont know too much, just a little about Kali Linux in basic things like Nmap, Wireshark, volality and Aircrack. I think i need to learn more tools.

Related to networking i used to open/close ports and config network adapters i feel like i need more knowledge here too.

About cryptography i know what i learned in the university and a little by my own.

I solved some CTFs but i didnt be the first and played some hackathons.

So im thinking to get some certifications like CEH or offensive security, do you think this is usefull or required to get a job?

I know that i will be a noob again if a start a new job in cybersecuty and what i lose so, do you recomend me to move or maybe it is too late for me ? how is the salary in similar jobs?

thanks in advance

CyberStrike - April 5, 2018, 12:06 am

Never too late, I have seen people getting into pentesting at 54 read a story once about a grandma learning C++ for her grandkids to make them an app, so never too old. You are actually in a pretty good spot to change up you seem to have the coding/linux get a bit more familiar with Windows not

just server but also look at the end user solutions (7-10). You probably already know that you are going to encounter Windows 7 although pretty soon Windows 10 within a year or so should be at about 57% .. and God help us if it's Windows 10s. I would hit up even just a simple Network+ book just to help you in that area, I tend to see most "security" issues that give us access or the opportunity for further exploitation once inside of the network are just bad configs in either networking or in the OS.

Now this is just opinion, but CEH at best is a primer, I would honestly read and understand what they are talking about, although they seem to have gotten a bit more than just surface in v9.. But check out ELearnSecurity (<https://www.elearnsecurity.com/certification/>) EJPT/ECPPT are not too shabby, the most important thing is that you must really do lots of hands on. Vulnhub they have tons of vulnerable VM's that you can practice against. OSCP is not the easiest cert out there but by far you will find it puts other certs such as CEH/CPEH to shame, and if you plan on working for a company that specifically does pentesting you will find that with a CEH you honestly are looking at a bit of catchup time, that'll happen with OSCP as well soon as you hit a company, but you would probably have a little less of that learning curve.

You know being that you already are a coder you will find that several times in your security career you will find a client who doesn't want a pentest instead they would prefer a code review so believe me it's not the last time you will be looking through tons of src code. Also exploit development/DFIR (malware triage)/ Reverse Engineering that is a lot of things to explore.

0x00 - April 6, 2018, 2:33 am

You are right maybe some books/training about windows or powershell can be good.

I didn't know nothing about ELearnSecurity but look awesome.

About CEH and OSCP, in this day I have got some books for preparing CEH and look ok to start/read. I agree with you OSCP is more hard and professional but is not at my range now.

Thanks for the response!

CyberStrike - April 7, 2018, 10:43 am

You should also give the following a look <https://hackforums.net/showthread.php?tid=5788781> it's pretty much what you need to focus on to become a pentester, it's quite good.

0x00 - April 9, 2018, 12:29 am

Thanks!, great info I will check it out