

Forum:[Hack Forums](#)

Thread: [New To Hacking And Pentesting](#)

Digital Whispers - September 18, 2016, 6:12 am

A little introduction. For the last ten years I've been working as a network engineer. Before that, I did general IT work, installing, repairing, and upgrading hardware and software. It was ten years ago that I was introduced to the world of Cisco. Now I have my CCENT, CCNA, and I passed the CCNP ROUTE. Now, along with studying for the CCNP SWITCH exam, I'm also teaching myself Python (using Python Crash Course), I'm reading through The Hacker Ethos, and I'm studying for the Security+ exam. I figure the Security+ exam is the best place to start getting Security/Pentesting certs.

My question is this. Am I approaching it the right way? Is starting with Python a good idea? Should I eventually go for Offensive Security certs and eLearn Security certs? There is so much to learn to be a master pentester so I just want to opinion of others with experience. If there was an ultimate checklist of things to know, what would be on it? I know it would be ridiculously long, but if that's what is needed then that's what needs to be done. I'm exceedingly focused and inspired so when I have my mind set on something, I accomplish. Being stubborn helps with that as well. ?

Faith Connors - September 18, 2016, 6:32 am

Well it's good to hear that you're dedicated to all that stuff, as most people decide to give up after we tell them that hacking a facebook account doesn't have a 100% success rate.

Python is a good place to start if you don't really have any experience with any other languages, but it also kinda depends what kinds of stuff you want to do. If you want to try exploiting websites, maybe PHP or SQL would help more than knowing C, or if you want to write malware, something like C would be better than something like Python, whereas writing an exploit or just a quick script to deliver a payload might be more practical in Python/Ruby/Perl.

As for certifications, OSCP is the widely acclaimed "best" cert you can go for, it's a lot more prestigious and generally a lot harder to complete. That applies to most of OS's certs, and for one of them I believe you have to hack a site to even find the registration page. So yeah, OSCP would be a good goal to move towards, but it's good that you already have experience with networks and IT, because if you understand how all that stuff works it'll make your life much easier.

So yeah, Security+ is a great place to start as it's not very hard, doesn't really have any prerequisites and teaches a good chunk of knowledge, although you might already know some of it. I think network engineer experience counts as infosec experience, so after Security+ CEH would be good, as you need at least 2yrs infosec experience to take the exam (or you take their official training for a few months.) After that, maybe you could look into CISSP or just look to better improve your skills and get ready for OSCP, although I wouldn't recommend jumping into OSCP right after CEH.

Digital Whispers - September 18, 2016, 6:55 am

Thanks for the advice. Believe me, I would love to be able to hack Facebook pages, just for the entertainment of it, not to mess with my ex or anything. ? Like I said, I'm stubborn enough to learn what it takes to do anything, and I don't want to be a skid. I'd like to learn everything down to the nuts and bolts. For now, I use tools within Kali to practice pentesting, but I'm the kind of person who wants to know why it worked, and if I can manipulate the code more to make it do other things.

As far as programming, I'm learning Python first because I read in a few places that it's the best language to learn for networking exploits and whatnot. I do want to learn C eventually and hopefully even Assembly one day. I know I would need to know those for reverse engineering, right? Obviously I would need to know some web scripting languages to be able to do web pentesting. That's something else I'm using Kali programs to do for now.

I've read quite a few people saying that CEH isn't good for hands on learning. They said that it teaches you more about the knowledge you need and not about how to actually perform any work. Is that true? I suppose to be a master at pentesting, one needs to study both aspects - the theoretical and then being able to apply it.

Faith Connors - September 18, 2016, 7:19 am

(Sep 18, 2016 06:55 AM)Digital Whispers Wrote: [\[CITE\]](#) Thanks for the advice. Believe me, I would love to be able to hack Facebook pages, just for the entertainment of it, not to mess with my ex or anything. ? Like I said, I'm stubborn enough to learn what it takes to do anything, and I don't want to be a skid. I'd like to learn everything down to the nuts and bolts. For now, I use tools within Kali to practice pentesting, but I'm the kind of person who wants to know why it worked, and if I can manipulate the code more to make it do other things.

As far as programming, I'm learning Python first because I read in a few places that it's the best language to learn for networking exploits and whatnot. I do want to learn C eventually and hopefully even Assembly one day. I know I would need to know those for reverse engineering, right? Obviously I would need to know some web scripting languages to be able to do web pentesting. That's something else I'm using Kali programs to do for now.

I've read quite a few people saying that CEH isn't good for hands on learning. They said that it teaches you more about the knowledge you need and not about how to actually perform any work. Is that true? I suppose to be a master at pentesting, one needs to study both aspects - the theoretical and then being able to apply it.

Mmm, CEH is rather hypothetical, you're right. It teaches you what things do, but not quite how to use them in an actual pentesting scenario. Don't get me wrong though, it's still good to know all that stuff, but if you were to actual try pentesting with only that, you'd have to figure out what your action plan is on your own. But IMO, the best way to learn is just by doing, so practicing the techniques used helps, and then maybe trying a CTF-style virtual machine from Vulnhub would be good too, just to see how you actually perform.

JudoWannaKnow - September 18, 2016, 7:48 am

Just to kind of jump on this, I am doing a similar path. Just less networking experience and more medical knowledge which i know means nothing. But I was reading how OSCP and SEC+ are similar normally if you can pass the former the latter is easier, or so I have been told. I am intrested in learning more to do CTF.

I am currently teaching myself Python. Currently studying up to get Network+ in the next few months. Other then that my plans consist of Python, C++ and SQL in the next few years. As well as CEH, SEC+/OSCP, maybe pick up A+ if someone who works in the industry can tell me if it really is worth anything?

Digital Whispers - September 18, 2016, 9:50 am

To say OSCP and Security+ are similar in any way is like saying it's just as easy to draw stick figures as it is paint the Mona Lisa because they both involving a drawing utensil. ? Security+ is an easy exam regardless because it just covers the basics of networking and some security concepts. You should have no problem with it.

JudoWannaKnow - September 18, 2016, 3:01 pm

Like I said that is what some of my research pointed too. Some of the test prep I have been doing for it has also hinted to it in a degree.

ThisIsCyn - September 18, 2016, 3:03 pm

Op should also read the thread in my description will add some valuable detail

skelly76 - September 18, 2016, 4:03 pm

(Sep 18, 2016 03:03 PM)ThisIsCyn Wrote: [\[CITE\]](#) Op should also read the thread in my description will add some valuable detail
Lol.

Faith Connors - September 18, 2016, 4:56 pm

(Sep 18, 2016 03:03 PM)ThisIsCyn Wrote: [\[CITE\]](#) Op should also read the thread in my description will add some valuable detail
Yeah, lol.

No offense, but it's not very in-depth and doesn't really cover that much. There are much better written guides on here.

Digital Whispers - September 18, 2016, 7:33 pm

I need to keep a schedule of everything. I am attacking so much at once that I want to make sure I appropriate time to each topic carefully. I'm actually excited that I'm finally learning a programming language.

Earlier today, I set up part of my GNS3 network to study for the CCNP SWITCH exam. I came across an excellent video tutorial that incorporates GNS3 into all of the topics necessary. I have until December to study and pass it since my certifications expire in December. After I passed the ROUTE exam the plan was to move directly to the SWITCH exam, but personal issues arose so everything got put on hold. Now I'm cutting it really close, but the SWITCH exam is the easiest of the three needed for the CCNP certification so I have confidence that I'll be alright. Plus, I've been doing more VLAN configs at my job so it has been exceedingly helpful with committing it to memory.

Sorry, I'm rambling. I'm a complete introvert, unless you find the right topic for me to digress into. ? I almost forgot one more think. Along with the networking topics, I'm also learning Wireshark. ?

(Sep 18, 2016 03:03 PM)ThisIsCyn Wrote: [\[CITE\]](#) Op should also read the thread in my description will add some valuable detail
Thanks. Every little bit helps.

JudoWannaKnow - September 18, 2016, 9:42 pm

(Sep 18, 2016 07:33 PM)Digital Whispers Wrote: [\[CITE\]](#) I need to keep a schedule of everything. I am attacking so much at once that I want to make sure I appropriate time to each topic carefully. I'm actually excited that I'm finally learning a programming language.

Earlier today, I set up part of my GNS3 network to study for the CCNP SWITCH exam. I came across an excellent video tutorial that incorporates GNS3 into all of the topics necessary. I have until December to study and pass it since my certifications expire in December. After I passed the ROUTE exam the plan was to move directly to the SWITCH exam, but personal issues arose so everything got put on hold. Now I'm cutting it really close, but the SWITCH exam is the easiest of the three needed for the CCNP certification so I have confidence that I'll be alright. Plus, I've been doing more VLAN configs at my job so it has been exceedingly helpful with committing it to memory.

Sorry, I'm rambling. I'm a complete introvert, unless you find the right topic for me to digress into. ? I almost forgot one more thing. Along with the networking topics, I'm also learning Wireshark. ?

Thanks. Every little bit helps.

Please continue, I am actually interested. It will help me when I get there.

Cimex - September 18, 2016, 10:05 pm

(Sep 18, 2016 03:03 PM)ThisIsCyn Wrote: [\[CITE\]](#) Op should also read the thread in my description will add some valuable detail

Thank you. That thread really did unskid me