

Forum:[Hack Forums](#)

Thread: [Ethical Hacking/PenTesting CompTia Question](#)

CrouchingTig3r - January 10, 2020, 4:15 pm

I was wondering what would be the appropriate route to go down to get into pen testing , ethical hacking when you're beginning or starting out.

Would it looking like this ?

Networking+ ---> Security+ ----> OSCP ??

Or what should be the exact time line or route

Fladrif - January 11, 2020, 12:20 am

If you want to be the best, work in IT (network / server admin or development) for 10 years then get a job in infosec

CrouchingTig3r - January 11, 2020, 5:03 am

(Jan 11, 2020 01:20 AM)Fladrif Wrote: [\[CITE\]](#) If you want to be the best, work in IT (network / server admin or development) for 10 years then get a job in infosec
doesn't sound right but thanks for the comment .

Fladrif - January 11, 2020, 5:34 am

Sorry but it is right, its not easy, but thats life :)

If you just want to be another junior pentester with specific skills in one area i.e. web pentesting then yeah maybe there are some shortcuts and OSCP/hackthebox/vulnhub are some of them, but youll never be as good as that person that spent 10 years developing web apps or managing a network and then moved into security...

CyberStrike - January 11, 2020, 7:32 am

That is how old school InfoSec professionals did it, like you went from tech support to jr admin to admin (of course you get certs and all that jazz). In truth and speaking from that school there are things I immediately think of which others may not. Security+ will teach you how an administrator thinks which is important but it's no where near what you need to know to tackle an actual pentesting cert, unless CEH or something.

CrouchingTig3r - January 11, 2020, 7:52 am

(Jan 11, 2020 08:32 AM)CyberStrike Wrote: [\[CITE\]](#) That is how old school InfoSec professionals did it, like you went from tech support to jr admin to admin (of course you get certs and all that jazz). In truth and speaking from that school there are things I immediately think of which others may not. Security+ will teach you how an administrator thinks which is important but it's no where near what you need to know to tackle an actual pentesting cert, unless CEH or something.

This field will make you go far through experience but when starting out what should one know and obtain to get your foot even In the door.

Fladrif - January 11, 2020, 8:38 am

Quick mode -> download Kali, sign up for hackthebox, watch ippsec videos, profit.

Yeah you'll learn how to compromise web servers and escalate privileges in very specific circumstances, but it won't do you a huge amount of good in the real world of infosec.

doth3righthong - January 11, 2020, 10:48 am

You could also work your way into the skill with bounties. Find bugs and exploits as a side hobby.

CrouchingTig3r - January 11, 2020, 12:42 pm

(Jan 11, 2020 09:38 AM)Fladrif Wrote: [\[CITE\]](#) Quick mode -> download Kali, sign up for hackthebox, watch ippsec videos, profit.

Yeah you'll learn how to compromise web servers and escalate privileges in very specific circumstances, but it won't do you a huge amount of good in the real world of infosec.

If Kali Linux didn't take so much of my space on my Mac I'd begin learning.

Fladrif - January 11, 2020, 1:51 pm

You don't necessarily need Kali. A browser and a copy of Burp will get you a fair way on a lot of CTFs and web challenges.

Bugsplat - January 11, 2020, 1:56 pm

Kali is just an OS with a bunch of shit you probably won't use. Just download what you need.

CrouchingTig3r - January 11, 2020, 2:00 pm

(Jan 11, 2020 02:51 PM)Fladrif Wrote: [\[CITE\]](#) You don't necessarily need Kali. A browser and a copy of Burp will get you a fair way on a lot of CTFs and web challenges.

I've been trying to follow this TUT

<https://www.youtube.com/watch?v=3Kq1MlftWCE>

Fladrif - January 11, 2020, 2:07 pm

It's a 14 hour long video, I'm not sure what you want from me but I'm not watching it all ?

Just keep doing your research, don't ask questions that a million people have already asked, watch loads of tutorial videos and you'll be on the right track. It looks like quite a generic vid which is good when you're starting out, but you could also start looking at more specific attack types. And watch some blackhat/defcon videos and some sans instructional videos too. You'll be pwning in no time...

Bass_Reeves - January 11, 2020, 2:38 pm

(Jan 10, 2020 05:15 PM)CrouchingTig3r Wrote: [\[CITE\]](#) I was wondering what would be the appropriate route to go down to get into pen testing , ethical hacking when you're beginning or starting out.

Would it look like this ?

Networking+ ---> Security+ ----> OSCP ??

Or what should be the exact time line or route

The Cyber Mentor has literally answered your question -

<https://www.youtube.com/watch?v=dRTqRJsr1ss>

Apparently took him just over 2 years from help desk - pentester.

CrouchingTig3r - January 11, 2020, 2:49 pm

(Jan 11, 2020 03:38 PM)Bass_Reeves Wrote: [\[CITE\]](#) The Cyber Mentor has literally answered your question - <https://www.youtube.com/watch?v=dRTqRJsr1ss>

Apprently took him just over 2 years from help desk - pentester.
2 years isn't long, time isn't what im worried about, more so developing the skills to even get to the point where I want to be and mapping everything out.

Bass_Reeves - January 11, 2020, 3:34 pm

(Jan 11, 2020 03:49 PM)CrouchingTig3r Wrote: [\[CITE\]](#) 2 years isn't long, time isn't what im worried about, more so developing the skills to even get to the point where I want to be and mapping everything out.

I hear if you, if you watch the video he tells you how he done it.

He didn't have any skills in IT before he started at help desk. Earned his certs along the way.

ITlorty - January 12, 2020, 4:27 pm

IMHO just studdy and go for the oscp. CEH is a joke, and compTIA test arent all that impressive either.

Polymath - January 13, 2020, 7:57 am

(Jan 10, 2020 05:15 PM)CrouchingTig3r Wrote: [\[CITE\]](#) I was wondering what would be the appropriate route to go down to get into pen testing , ethical hacking when you're beginning or starting out.

Would it looking like this ?

Networking+ ---> Security+ ----> OSCP ??

Or what should be the exact time line or route
Firstly, I recommend you to read this high quality thread: <https://hackforums.net/showthread.php?tid=5788781>

Secondly, it depends on what your current experience/qualifications are. Do you have a degree? What certs do you have? How many years of experience in IT or IT security related jobs have you had?

(Jan 11, 2020 01:20 AM)Fladrif Wrote: [\[CITE\]](#) If you want to be the best, work in IT (network / server admin or development) for 10 years then get a job in infosec
This is not good advice. This may be good for old timers who already have experience in the IT industry and want to move to cyber security. But for someone who is young and has potential, it would be better to do a Computer Science degree, and pick up some certs along the way which will make you employable and possibly get you an entry Cyber Security role from where you can work your way up

ropslide - January 13, 2020, 8:00 pm

In this world you will get a job quick with the right degrees. Any other than that you will have to be outstanding at what you are doing to succeed in any sector.

Then also it depends which path of security you're actually choosing, rather be an expert in a niche, than a fool on all levels. It's unlikely that you will always be a master of everythng, much more importantly you got to have the understanding to work yourself into any field of security quick. Once you obtained that, you can work yourself through the levels to the extend of interest you're having.

Realistically: Get a degree and work yourself up.

Utopistic: Become extraordinary good at security and prove your skills to a company by revealing

security holes. (This is not as rare as many would believe)

To answer your question more precisely:

Networking+ ---> Security+ ----> OSCP ??

Prepend:

Coding: Understand how bugs are created, learn how to spot them, then learn how to exploit them.

(This would automatically lead to understanding Stack/Heap, and prior to that -eventually- even ASM, while it is worth mentioning that there are many good exploiters that don't know ASM)

Once you exploited, you'll automatically come up to the next question which most likely turns out to be: Networking.