

Forum:[Hack Forums](#)

Thread: [What should be a top to learn when pentesting today?](#)

Biggy_Asian - October 6, 2024, 1:52 pm

I have had a thing for pentesting since I was younger (4-5) but feel I am missing out on some valuable information or am just missing something in my education.

I do get into a little HTB sometimes however I am fairly lost for what I should really learn and what would really benefit my self in the future to learn.

I really do yearn to keep learning and for in-depth/deep readings as I feel I actually learn something there instead of really just being given something that was just handed with the vague comment at the top here and there etc you get it.

I can learn from something being handed to me however with not much understanding of the true inner workings I wont feel satisfied.

Any kind of resources would help (links or just from here in general). I am constantly eager to learn and I feel the best way to ask is to throw my hand out to those who are a bit more technical than I.

Biggy_Asian - October 6, 2024, 2:20 pm

(Oct 6, 2024 02:17 PM)shatter Wrote: [\[CITE\]](#) Foundational bash scripting, networking, and Active Directory. Also mandatory to have basic web application knowledge, even though a lot of the OWASP Top 10 have changed over the years and many security tools and even modern browser implementations can help mitigate a lot of the easy wins, it's non-negotiable to understanding those vulnerabilities etc.

Thanks these will help a bit. Anything else you could recommend? Maybe any write-ups which would be useful to read or anything along those lines?

Biggy_Asian - October 6, 2024, 2:24 pm

(Oct 6, 2024 02:21 PM)shatter Wrote: [\[CITE\]](#) Not really, I do one-to-one mentorship for my clients for careers in penetration testing and cater it to people's individual learning style and pace. Everyone is different. (So I've learned)

Gotcha. I prefer self teaching tbh I feel its better although mentoring could help for some.

Kroshie - October 6, 2024, 10:41 pm

(Oct 6, 2024 01:52 PM)Biggy_Asian Wrote: [\[CITE\]](#) but feel I am missing out on some valuable information or am just missing something in my education.

Your not gonna learn much if you just read from the code.

(Oct 6, 2024 01:52 PM)Biggy_Asian Wrote: [\[CITE\]](#) I am constantly eager to learn and I feel the best way to ask is to throw my hand out to those who are a bit more technical than I.

Please go actually learn and read up on things.

(Oct 6, 2024 01:52 PM)Biggy_Asian Wrote: [\[CITE\]](#) I do get into a little HTB sometimes however I am fairly lost for what I should really learn and what would really benefit my self in the future to learn.

Because of this I truely believe you dont exactly understand computers or anything much when it comes to the realm of hacking and/or exploiting vulns...

Was any of that helpful? No? Funny, because I just copy/pasted your own replies you made to the request for knowledge I made in this very forum. I find it particularly amusing that you made this post but an hour after that little performance in which you set out to stroke your own ego by tearing down beginners.

Anyways, as a gesture of good faith and because offering actual help isn't beneath me, my suggestion would be to dive into the art that is social engineering. It's, in my opinion, an incredibly underrated practice with a kind of flexibility you simply don't find with other tools. When you run into a problem there is, with little exception, almost always a social-engineering based solution.

In addition to everything else that makes the Darknet Diaries podcast so great, it features many episodes that really dive into some of the more interesting and exciting ways social engineering can be used by a pentester. The many books on persuasion (Influence: The Psychology of Persuasion, The Art of Persuasion, The Science of Human Hacking...just a tiny selection of the many, many awesome books written on the subject) that are easily found in libraries are an excellent place to start diving into the subject. Then there are the infamous social-engineering competitions at Def-Con, clips of which can easily be found all over the web.

There is tons of knowledge to be hoovered up by anyone interested in the subject, and one of the great things about it is that you can practice and make use of the skills throughout your entire day and as you get on with life. Highly recommended!

plops - October 7, 2024, 6:30 am

(Oct 6, 2024 10:41 PM)Kroshie Wrote: [\[CITE\]](#) In addition to everything else that makes the Darknet Diaries podcast so great, it features many episodes that really dive into some of the more interesting and exciting ways social engineering

Great thing to point out IMO

In my journey, Darknet diaries has been a great way for me to get exposed to different concepts, practices and techniques that I would have never known to look up.

In addition to following free and paid curriculum, it keeps my mind busy and adds to the forever list of things to study.

Biggy_Asian - October 7, 2024, 7:46 am

(Oct 6, 2024 10:41 PM)Kroshie Wrote: [\[CITE\]](#) Your not gonna learn much if you just read from the code.

Please go actually learn and read up on things.

Because of this I truly believe you dont exactly understand computers or anything much when it comes to the realm of hacking and/or exploiting vulns...

Was any of that helpful? No? Funny, because I just copy/pasted your own replies you made to the request for knowledge I made in this very forum. I find it particularly amusing that you made this post but an hour after that little performance in which you set out to stroke your own ego by tearing down beginners.

Anyways, as a gesture of good faith and because offering actual help isn't beneath me, my suggestion would be to dive into the art that is social engineering. It's, in my opinion, an incredibly underrated practice with a kind of flexibility you simply don't find with other tools. When you run into a problem there is, with little exception, almost always a social-engineering based solution.

In addition to everything else that makes the Darknet Diaries podcast so great, it features many episodes that really dive into some of the more interesting and exciting ways social engineering can be used by a pentester. The many books on persuasion (Influence: The Psychology of Persuasion, The Art of Persuasion, The Science of Human Hacking...just a tiny selection of the many, many awesome books written on the subject) that are easily found in libraries are an excellent place to start diving into the subject. Then there are the infamous social-engineering competitions at Def-Con, clips of which can easily be found all over the web.

There is tons of knowledge to be hoovered up by anyone interested in the subject, and one of the great things about it is that you can practice and make use of the skills throughout your entire day and as you get on with life. Highly recommended!

Thanks for the info but coming here to just be petty somewhat after getting angered at an response in your thread is pretty childish. Grow up. ?

(Oct 7, 2024 06:30 AM)Robert Walker Wrote: [\[CITE\]](#) Great thing to point out IMO

In my journey, Darknet diaries has been a great way for me to get exposed to different concepts, practices and techniques that I would have never known to look up.

In addition to following free and paid curriculum, it keeps my mind busy and adds to the forever list of things to study.

I've always watched some John Hammond videos to understand what someone in his place (a blue teamer) might do to study and reverse programs. I have learnt some new things from those hour long videos too. I know theres other resource I have looked at which I have forgotten but additional ones do help. I sometimes take time to read indepth studies on exploits or other vulns or whatever else that is relevant and try my best to grasp what is being done etc.