dostoevskylabs / dostoevsky-pentest-notes

Notes for taking the OSCP in 2097. Read in book form on GitBook https://dostoevskylabs.gitbooks.io/do…

pentesting methodology oscp enumeration exploitation buffer-overflow

346 commits **1** branch **0** releases **1** contributor

Branch: **master** New pull request Find file Clone or download

dostoevskylabs Updates chapter-2.md ··· Latest commit `878a6f2` on Feb 18

.gitignore	GitBook Example	2 years ago

README.md	Updates README.md	3 months ago
SUMMARY.md	Updates SUMMARY.md	3 months ago
chapter-1.md	Updates chapter-1.md	3 months ago
chapter-2.md	Updates chapter-2.md	3 months ago
chapter-3.md	Updates chapter-3.md	3 months ago
chapter-4.md	Updates chapter-4.md	6 months ago
chapter-5.md	Updates chapter-5.md	6 months ago
chapter-6.md	Updates chapter-6.md	3 months ago
chapter-7.md	Updates chapter-7.md	3 months ago
chapter-8.md	Updates chapter-8.md	7 months ago
chapter-9.md	Updates chapter-9.md	3 months ago

README.md

Dostoevskylabs's PenTest Notes

This is my attempt to not suck at pentesting by organizing my learning. I have very briefly covered various concepts related to penetration testing, but more importantly I have linked a large array of resources that you can source deep knowledge from.

Still a work in progress, expect regularly updates.

Table of Contents

What have I learned so far?

1. Security is a constantly evolving landscape and it's hard to keep up if you try to learn everything at once; try to stick to one focal point at a time. There is plenty of time to dive into all the interesting concepts, but you need to build fundamentals first (walk before you run)
2. It pays off to take your mind off of the problem sometimes - don't neglect the people in life who care about you. It's easy to get obsessed with this field and get sucked into a rabbit hole of endless learning, but put it down sometimes and go crack a beer with the wife/husband/gf/bf/friend. Pet your cat sometimes.
3. **Network. Network. Network.** LinkedIn and Twitter are amazing to network with your industry. This may seem obvious but it took me a really long time to come out of my shell and start talking to people. However, this industry is more about the people you know than anything else. It's tight-knit and your geek network can land you in some really favorable

situations. Get to know people, engage with them. **Take an interest in what they are doing (it's probably pretty cool)**. If you're an introvert take a few steps out of your shell, don't worry you can always run back in to recharge ;)!

4. Bounce your ideas off people! - find people you can speak with on any given topic because there will be times when you have specific questions you won't be able to google for and even if you can it's more important to talk with someone who understands it at or above your level. That conversation starts a critical dialogue that will get your brain to take that step to the next level.
5. **Exploit development is hard. **Most of the people out there releasing really groundbreaking exploits are far smarter and have been doing this far longer than you or I. They are legends that make it possible for us to learn by sharing what they have researched/developed. With every new concept I learn I understand I am only scratching the surface and that it will take decades to get to that level; respect the time that has to be put into this and it will pay off, but don't be discouraged if it takes you a while to get anywhere. Our senses aren't able to natively perceive things in the context of programs running in memory, so it requires a perceptual switch (and a difficult one at that) to be able to really work out all the moving pieces of any exploit, and **that's okay**.
6. There is no feeling greater than basking in the glory of shell.
7. **In short, I've learned nothing. (Except how to use bold)**