💯 eCPPTv2_Exam_Review 2021 💯

First and foremost, avoid stressing yourself before the exam by reading numerous write-ups from others. This can be overwhelming, as people tend to share their personal experiences and may exaggerate their success. Everyone loves discussing their achievements, especially when they feel like they've "conquered" the challenge.

Here are my key pieces of advice:

1. If you're not yet a professional, take the course and lab exercises with INE. It's best to start from scratch with the eJPT certification and work your way up.
2. If you're not in a rush, consider completing the entire "Offensive Learning Path" on TryHackMe.
3. Prepare for the challenge with some snacks and chocolates. Think of it like you're gearing up for a battle — it'll be a few intense days.
4. Create your Cheat Sheet. You can use mine: Pentest-CheatSheet.xlsx.
5. The first target you need to exploit will be outlined in the engagement letter. Don't overthink it. If you don't immediately get a Meterpreter session, try resetting the lab and re-initializing your Metasploit Database or use MSF5 (I personally use MSF5).
6. Meterpreter is the ideal tool for pivoting. Other techniques, like Chisel, may waste valuable time. Double pivoting is a strong strategy.
7. Be aware that MSF6 no longer supports SOCKS4A and instead supports "socks_proxy" for exploitation.
8. Enumeration is crucial. Thoroughly enumerate each target, as it can provide access to other systems. Proxychains is also essential.
9. Simplify your exploitation process. Sometimes, the same technique can be applied to exploit different elements.
10. Don't skip buffer overflow testing. It's critical to understand this, especially "Brainstorm" CTF from Tryhackme and the "Offensive Penetration Testing - Module 6" from Cybrary.
11. Resetting the lab is not always the solution for buffer overflow. Think carefully about what resetting accomplishes if the target is already running. Instead, try different ports on your listener side and refine your exploit code.
12. When tackling the final target, don't overthink the privilege escalation. The solution will usually become apparent as soon as you gain access to the machine.
13. Reporting is key. I recommend using these resources for reporting: reporting guide, RandoriSec, TCM-Security.
14. The exam is not just about exploiting and escalating targets (or simply catching flags). It's equally important to use both Windows/Linux enumeration techniques and possibly some automated tools to identify vulnerabilities across all targets.
15. Finally, join the eLearnSecurity Discord community. Install the app and enjoy engaging with fellow students and hackers. It's a great place for discussions and support.