# assignment

1. This internship requires 2–3 hours daily (Mon–Fri) for at least 6 months. Describe a situation where you maintained long-term consistency despite challenges. Why did you continue?

ans: I am currently maintaining a consistent routine of investing 3–4 hours every day in learning and practicing penetration testing and I am doing this for a year now. I practice on TryHackMe and use it on real targets listed on HackerOne.

and I have also maintained consistency while learning blue teaming from Let's Defend. For this period of time I dedicated 4–5 hours daily to study blue teaming,  Incident response and related labs.
The main challenges were time management especially during busy weeks. I continued the practice because I really wanted to know how the blue team works. I invested 2 months in this practice.

2. Pick one real CVE related to privilege escalation or lateral movement and explain how attackers exploit it, in simple terms for a technical audience.

ans: CVE-2021-4034 is a privilege escalation vulnerability in the linux pkexec.

pkexec is used to run a normal user to run root commands safely.
so before running any command as root it simply removes GCONV_PATH, LD_*, PATH variables so it can be run safely.

but to exploit it we need to know how this works, there are two main parts of it first is argc and second is argv, argc is the number of arguments user passes and argv is those values in a array form, so if user runs pkexec id, then the values will be argc = 2, argv[0]= "pkexec" and argv[1]="id", so when the developer developed this tool, they never thought about the value of argc as 0 and argv as NULL.

So what CVE-2021-4034 does, it invokes the pkexec via kernel to run without any argument, so the values become 0 and NULL so the variable cleanup gets skipped and when it comes to importing libraries, system import it from library that attacker controls.

So because the pkexec is already running as root, the loaded library code runs with root permission.

3. Are you familiar with SEO and on-page optimization (headings, keywords, internal linking)? Briefly explain your experience, or confirm your willingness to self-learn (2–3 hours).

ans: I don't have direct experience in SEO yet but I am familiar with medium blogs and reports.
Additionally I run a youtube channel which helps me to understand how title, keywords affects the reach. So I am confident that I can understand it quickly, I am fully willing to dedicate 2-3 hours daily to self-learn.