What I learned-

This week, I was introduced to several ethical frameworks that guide decision making in the field of cybersecurity. The one I found most interesting was Deontological Ethics, which focuses on duty and the inherent rightness of actions rather than the outcomes. This aligns with the ideas presented in Chapters 2–4 of the eBook, especially the emphasis on integrity and consistent ethical action. According to deontology, some actions are simply right or wrong, regardless of the consequences. This mindset is especially important when handling sensitive data or enforcing security protocols. This framework connects closely with the (ISC)2 Code of Ethics, particularly the directive to “protect society, the common good, necessary public trust and confidence, and the infrastructure.” Deontology helps reinforce the idea that ethical behavior should not depend on whether we get caught or praised, but whether the action respects rights and follows accepted rules. I also learned how personal lenses, such as my background, experiences, and education, can influence how I interpret ethical scenarios. The difference between what is ethical and what is legal stood out as especially important for cybersecurity professionals, since many unethical behaviors in tech are still technically legal.

How I’ll apply it-

One real world example that I can think of of applying Deontological Ethics is in the context of a university IT helpdesk(which was kind of an example we used in class). If a technician is asked to reset a student’s password by someone claiming to be a parent or relative, the technician must follow established rules around “explicit authorization”. Even if the parent is being persistent and seems trustworthy, sharing account access without verified consent would violate both university policy and ethical duty. According to Deontological Ethics, the right action is to deny access unless formal authorization is provided, no matter how inconvenient that may be for the requester. This approach ensures privacy and security are respected, and aligns with professional standards like the code of ethics that are in the (ISC)2.

Muddiest point-

One part I’m still unsure about is how to decide when something that is unethical but legal should be reported or challenged. For example, if a company collects user data in a way that complies with the law but feels invasive, do cybersecurity professionals have an obligation to speak up? How do we balance professional duties with personal values in these situations? I'm still trying to understand how ethical responsibility applies when there is no clear legal violation.

Portfolio note-

- I will add a section titled "My Ethical Lens" that explains why I chose Deontological Ethics and how it connects to cybersecurity decisions. This helps show my foundational understanding of ethics and how I plan to apply it in real-world scenarios.

- I’ll also include a practical example in the "Authorization Principle" section about how important it is to get permission before accessing student accounts. This demonstrates my ability to connect ethical concepts to specific actions on campus or in the workplace.

- Including these sections matters because they show my growth in thinking about ethics in a structured way and help build a portfolio that reflects my development as a responsible cybersecurity professional.

AI Use Note

AI Use: I used ChatGPT to help brainstorm and organize my reflection based on the course slides and assignment instructions. I edited the content to reflect my own understanding and added my own examples.