Week 7 Reflection

This week's lectures focused on **penetration testing (pen testing)**, providing insight into how organizations proactively identify and address security vulnerabilities. The topics included fundamentals of pen testing, its purpose and limitations, types of tests, planning and scoping engagements, managing test processes, and follow-up strategies.

What I Learned

- I gained an understanding of **penetration testing fundamentals**, including its role in evaluating system security by simulating attacks.

- The **purpose of pen testing** was highlighted: to identify vulnerabilities before attackers can exploit them, while acknowledging the **limitations**, such as not guaranteeing complete security.

- I learned about **different types of penetration tests**, including black-box (tester has no prior knowledge), white-box (tester has full knowledge), and grey-box (partial knowledge).

- **Planning and scoping** a test engagement involves setting objectives, defining boundaries, and ensuring legal and ethical compliance.

- I understood the importance of **managing test processes and outcomes**, including documenting findings and communicating results effectively.

- **Follow-up and remediation strategies** ensure that identified vulnerabilities are addressed and mitigated to improve overall security posture.

Challenges Faced

- Grasping the differences between **black-box, white-box, and grey-box testing** and when each is appropriate required careful consideration.

- Understanding how to **effectively plan and scope engagements** while staying within legal and ethical boundaries was initially complex.

Reflection and Personal Growth

- This week emphasized that cybersecurity is **proactive**, and pen testing is a key tool for anticipating and preventing attacks.

- I realized that **thorough documentation and communication** are just as important as technical testing for effective remediation.

- The lectures highlighted the need for **ethical responsibility and careful planning** when performing security assessments.

Next Steps

- I plan to **explore practical pen testing labs** in controlled environments to gain hands-on experience.

- I will study **common pen testing tools and frameworks** to understand their applications in real-world scenarios.

- I aim to **connect pen testing knowledge with previous lessons on vulnerabilities and web security** to see how testing fits into a broader security strategy.