Week 6 Reflection

This week's lecture focused on **malware analysis**—a deeper and more technical area of cybersecurity. We explored what malware analysts actually do, the complete workflow of analysing malware, the skills and tools required, and career tips for entering the field.

What I Learned

- I learned that malware analysts play a crucial role in **understanding, dissecting, and responding to malicious software** that threatens systems and networks.
- The lecture broke down the **end-to-end malware analysis workflow**, including:
    - **Static analysis** (examining malware without running it, e.g., strings, file headers)
    - **Dynamic analysis** (observing behavior in a sandbox)
    - **Reverse engineering (RE)** (decompiling/disassembling to understand logic)
    - Identifying **IOCs (Indicators of Compromise)** such as IPs, hashes, domains, and behavior patterns.
- I now understand how these steps help analysts discover how a malware sample works, what it targets, and how to defend against it.
- The lecture also highlighted the **skills and tools** needed: programming knowledge, assembly basics, debuggers, disassemblers (like IDA Pro or Ghidra), virtual machines, and sandbox environments.
- We finished with **career tips**, explaining how to break into malware analysis through continuous learning, lab practice, and building a strong portfolio.

Challenges Faced

- The idea of **reverse engineering** seemed particularly complex due to its low-level focus on machine code and system internals.
- Understanding the full workflow from static to dynamic to RE required careful attention, as each step builds on the previous one.

Reflection and Personal Growth

- This week gave me a much clearer picture of what a malware analyst actually does—it's not just running tools but understanding behavior and patterns deeply.

- I realised the importance of **structured analysis workflows** in order to avoid mistakes and maintain safety when working with live malware.

- The career advice was motivating, showing that with consistent practice and curiosity, it's possible to enter this specialized field even as a student.

- Overall, the week strengthened my appreciation for the **defensive side of cybersecurity**, especially how essential analysis is for preventing large-scale attacks.

Next Steps

- I plan to experiment with **safe malware labs**, such as using REMnux or a Windows VM for learning the basics of static and dynamic analysis.

- I want to begin learning **Assembly language** and **low-level programming concepts**, which will help with reverse engineering.

- I will explore resources like Malware Traffic Analysis, The Zoo, and practical tutorials to gain hands-on experience.

- My goal is to connect what I've learned this week with earlier topics like malware types and countermeasures to build a more complete understanding.