Network System Security – Reflection – Week 04

Key Learning Outcomes

Understanding Malware Taxonomy and Behaviour

Understanding the different types of malware and their behaviours is essential because each requires distinct defence strategies. Effective cybersecurity must address both technical vulnerabilities and human factors like social engineering.

File Integrity Monitoring as a Defence Mechanism

Building a file integrity checker demonstrated how cryptographic hashes provide reliable file verification, showing that hashing is far more secure than relying on file metadata because even tiny changes are detectable and cannot be easily forged.

Signature-Based Detection

Signature-based malware detection, while historically important, is ineffective against modern adaptive threats like polymorphic and metamorphic malware. This highlights the need for behaviour-based and machine learning–driven security approaches.

Worm Propagation Dynamics

Simulating worm propagation illustrated how quickly self-replicating malware can spread across networks, emphasising that early detection and rapid containment are crucial because infections grow exponentially once a worm reaches critical mass.

Detecting Unauthorised File Modifications

Implementing change detection demonstrated how file integrity monitoring supports intrusion detection and forensic analysis

Layered Defence Architecture (Defence in Depth)

Designing a multi-layered monitoring system reinforced the principle of defence in depth, showing that effective cybersecurity requires integrating prevention, detection, containment, and recovery measures across hosts, networks, and users.

Network Anomaly Detection

Monitoring network activity revealed how anomaly detection distinguishes normal from malicious behaviour, emphasizing that effective detection depends on carefully balancing sensitivity to avoid false positives or missed threats.

Technical Skills Developed

- Cryptographic hashing using Python's hashlib library for integrity verification
- File system operations for scanning, monitoring, and baseline comparison
- Regular expression pattern matching for signature-based detection
- Network simulation to model propagation dynamics

Challenges and Critical Insights

False Positives vs. False Negatives

Effective detection systems require balancing sensitivity and specificity, because too many false positives overwhelm administrators, while too few detections allow attacks to go unnoticed, highlighting the need for awareness.

Human Interaction

Users are often the weakest link in cybersecurity, and effective protection requires combining technical defences with user education to prevent attacks like phishing and social engineering.

Moving Forward

Practical Applications

This workshop has equipped me to:

- Implement file integrity monitoring in personal or professional projects
- Evaluate antivirus and endpoint detection solutions
- Recognise red flags in code or system behaviour that indicate potential compromise