

# Principles of Security Technologies Coursework

## EXAMPLE REPORT STRUCTURE

### Title Page:

- Report title
- Student ID
- Module: COS6025-B Principles of Security Technologies

### Executive Summary/Abstract

Provide a short summary of:

- The malware/attack analysed
- Key findings
- Main risks
- Key mitigation strategies

(This should be written so it could be readable by a non-technical manager.)

### 1. Introduction and Context

Discuss:

- The chosen malware or cyberattack. Briefly describe the attack type (e.g., ransomware, trojan, worm, etc.)
- When and where it occurred
- Who/what it targeted. Outline the impact on organisations or society
- Why it is significant

Avoid long history sections – stay focused on analysis.

### 2. Attack Overview and Threat Analysis

Describe how the attack works:

- Initial infection method, IOCs
- Propagation/lateral movement
- Payload behaviour
- Impact

Use frameworks where possible:

- MITRE ATT&CK techniques
- Kill chain model
- Incident lifecycle

You may include attack flow diagrams or a timeline of events.

### 3. Simulated Malware Analysis Process

You are **NOT** running malware, but you must explain how it *would* be analysed.

#### **3.1 Static Analysis**

Describe:

- File inspection techniques
- Hashing and signatures
- Strings analysis
- Metadata examination

Explain what analysts would expect to find.

### **3.2 Dynamic Analysis**

Describe:

- Behaviour monitoring
- Process activity
- Registry/file changes
- Network traffic

You may reference public sandbox reports (e.g. from Hybrid Analysis, VirusTotal, Any.Run, etc), as well as sample screenshots (clearly cited).

### **3.3 Tools and Methods**

Discuss tools that would be used:

- Wireshark
- ProcMon
- SIEM tools
- Sandboxes, etc...

Explain why these tools are appropriate.

## **4. Detection and Mitigation Strategies**

Explain how organisations could:

- Detect the attack
- Respond to it
- Prevent recurrence

For instance, through the use of security technologies like SIEM/IDS/IPS monitoring, endpoint detection, network segmentation, patch management, etc...

Explain how secure design/SDLC practices could reduce risk.

## **5. Ethical, Legal, and Social Considerations**

Discuss ethical issues, such as:

- Privacy implications of monitoring systems
- Ethical handling of malware data
- Responsible disclosure
- Legal obligations (e.g. GDPR, breach reporting)

Reflect critically:

- Trade-offs between security and privacy
- Societal impacts of surveillance technologies

## **6. Conclusion**

Summarise:

- Key lessons learned
- Most important risks
- Most effective defences
- What organisations should prioritise

Do not introduce new material here.

## **References**

Minimum **12 sources**. Use **ONE** consistent referencing style (e.g. Harvard, APA, IEEE).

Include academic sources, vendor reports, threat intelligence reports, official guidance (NCSC, CISA, MITRE ATT&CK).

### Appendices (Optional)

You may include:

- Diagrams
- Tables
- Screenshots from sandbox reports
- Example logs

Do **not** include executable malware or unsafe material.

Appendices do **not** count toward the word limit.