George Theodorakopoulos

CMT118 Malware Analysis and Vulnerability Assessment

Malware Analysis

- Malware analysis
  - How does a piece of malware work?
  - What is it trying to achieve?
- Static and Dynamic analysis
- Static
  - Analyze without executing the malware
  - Safe but limited
- Dynamic
  - Run malware and observe its behavior
  - Can learn more, but need to keep it contained

Vulnerability Assessment

- Reconnaissance
  - Sniffing Networks
  - Scanning Hosts (Computers)
- Attacks
  - Web application vulnerabilities
    - Cross-site scripting, SQL Injection
  - Buffer Overflow, Denial of Service
  - Social engineering

Assessment

- Coursework (30%)
  - Analyse a piece of malware
  - Perform penetration testing on a vulnerable application
  - Write a report on the process and the findings
- Exam (70%)
  - Both malware analysis and vulnerability assessment

Background

- Useful to know:
  - Networking (wireshark)
  - Programming (C, Python)
  - Operating systems (memory management, stack, heap)
  - Command line (Linux)