COMPX508 – Malware Analysis

Week 9

Lecture 2

Outline

- Dynamic analysis
- Cuckoo – A sandbox
  - Architecture
  - Webserver (GUI)
  - Uploading the malware
    - GUI
    - Shell
  - Analysis – Reports

Topics discussed before

- Static analysis
  - Basic file investigation
  - Ghidra
  - x86
- Dynamic analysis
  - Registry functions
  - Windows processes
  - DLL injection (Not covered yet)

Indicators of Compromise (IoCs)

- Pieces of data, such as URLs, IPs, filenames, log entries, etc. that indicate malicious activity
- Host Based Indicators
  - Indicators found within a victim machine
  - E.g. files created by the malware, registry entries written, URLs in strings etc.
- Network Based Indicators
  - Indicators obtained from network activity or on the wire
  - E.g. URLs/IP addresses
  - Information in packets etc.

Tools - FlareVM

- Process and Thread information
  - Process Explorer
- System Logs
  - Process Monitor
- API calls
  - API Logger
- Static Strings
  - Strings
- TCP connections
  - TCP View

Tools - REMnux

- Network Protocol Simulation
  - INetSim
- Packet Capture and Analysis
  - Wireshark
- Read/Write network connections
  - Netcat
- Encryption/Decryption
  - CyberChef

Sandbox

- All-in-one software (Virtualized environment)
  - Multiple VMs (kind of hosts) to run malware
  - A server to record events (including static and dynamic behavior)

- Fingerprinting (May not reveal real intent)

Cuckoo

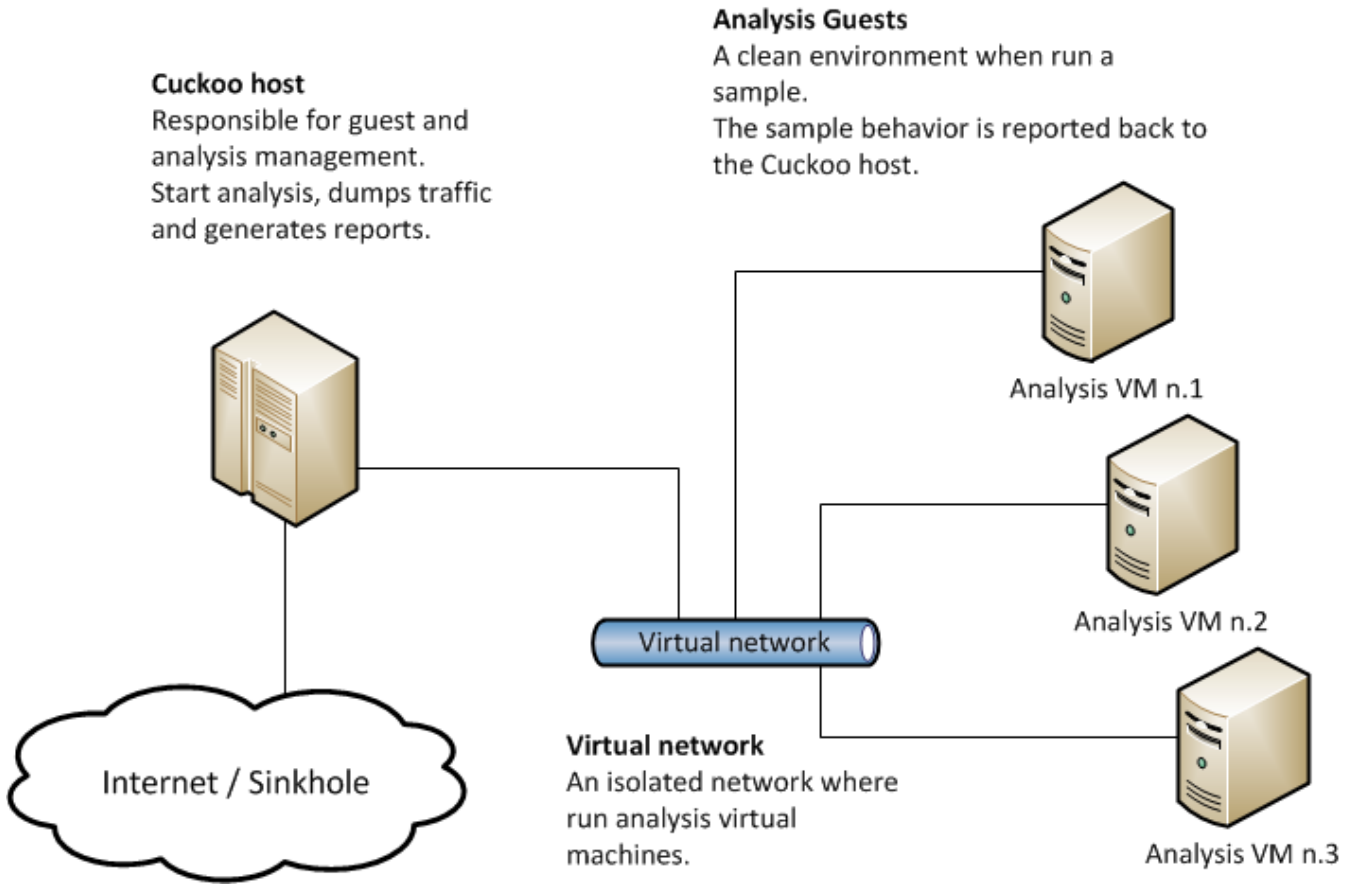
- A sandbox
  - Supports virtualization
    - Providing isolated environment to run malware
  - Allows data collection – recording events
    - Processes information
    - File system actions
    - Network traffic
    - System changes
    - …
  - Reporting

  - Open source

https://cuckoo.readthedocs.io/en/latest/

https://github.com/cuckoosandbox

Cuckoo



https://cuckoo.readthedocs.io/en/latest/introduction/what/

Other tools

- CAPE
- Any.Run
- …

- Tutorial