Môn An Toàn Mạng Máy Tính Nâng Cao

Bài tập 2

Mục đích bài tập 2 sẽ giúp sinh viên tiếp cận cơ chế hoạt động của mã độc và sử dụng công cụ để phân tich hoạt động của mã độc.

Câu 1: Nhóm sử dụng công cụ để khởi tạo mã độc với mục đích nghiên cứu.

Các loại mã độc tập trung trong môn học

* Virus
* Trojan
* Worm
* Bot
* Rootkits
* Ransomware

Kho Malware: theZoo: A live malware repository

Câu 2: Sử dụng các công cụ phân tích mã để phân tích hành vi của mã độc khi nó được kích hoạt.

Danh sách các tools để phân tích hành vi của mã độc

* Cuckoo: Sandbox
* capa: Automatically identify malware capabilities
* FLARE Obfuscated String Solver
* Ghidra Software Reverse Engineering Framework
* Malcom: Malware Communication Analyzer
* Mobile Security Framework (MobSF)
* Pafish: Testing tool
* Radare2: The Libre Unix-like reverse engineering framework

|  |
| --- |
| Ghi chú:   * Chỉ tạo mã độc với mục đích nghiên cứu và Xoá ngay mã độc ghi hoàn tất quá trình nghiên cứu. * Mỗi nhóm chỉ cần tạo 1 loại mã độc (Thầy sẽ chỉ định) và sử dụng 1 trong những công cụ trong câu hỏi để phân tích hành vi (Các bạn có thể đề xuất thêm) * Thời điểm nộp bài: 23:00, 29.Apr.2023 |