Advanced Computer Network Security
Assignment

The purpose of Assignment is to help students understand the mechanisms of malware operation and use tools for analyzing malware activity.

Question 1: Use tools to create malware for research purposes.

Types of malware focused on in this course:

- Trojan
- Virus
- Worm
- Bot
- Rootkits
- Ransomware

Malware Repository: theZoo: A live malware repository

Question 2: Use malware analysis tools to analyze the behavior of malware upon activation.
List of tools for analyzing malware behavior:

- 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

Notes:

- Only create malware for research purposes and delete the malware immediately after completing the research process.
- Each group needs to create one type of malware (as assigned by the instructor) and use one of the tools listed in the question to analyze behavior (suggestions for additional tools are welcome).