Course	COMP 8003
Program	Applied Computer Science, Network Security Applications Development Option
Term	September 2024

- This is an individual assignment.

Objective

- Develop a simple Command and Control (C2) system that:
    - Implements both an attacker and a victim component.
    - Allows the attacker to send commands to the victim, which executes the command and returns the result.
    - Supports command execution with arguments (e.g., ls, ls -l, ls -l /etc).
    - Optionally, it uses either TCP or UDP for communication.
    - Includes a secondary task of using John the Ripper to crack a password.

Learning Outcomes

- Understand the basics of command and control systems and their potential risks.
- Gain hands-on experience with network programming using sockets (TCP/UDP).
- Develop skills in secure coding practices and ethical considerations when creating network tools.
- Learn how to use John the Ripper for password cracking in a controlled environment.

Assignment Details

Part 1: Command and Control (C2) System

- Create two components: an attacker and a victim.
- The victim program must:
    - Run indefinitely, listening for commands.
    - Execute received commands and return the output to the attacker.
- The attacker program must:
    - Take a command as an argument when executed.
    - Connect to the victim, send the command, and print the output received from the victim.
- Command Requirements:

    - Support commands with arguments (e.g., ls, ls -l, ls -l /etc).
    - Do not implement redirection (<, >, >>) or pipes (|).
- Communication Protocol:
    - You may choose either TCP or UDP.
    - Consider how you will handle dropped packets or connection issues, particularly with UDP.
- Reliability:
    - Ensure your attacker program handles potential errors gracefully, such as unreachable victim.

Part 2: Password Cracking with John the Ripper

- Create a new user on your system with a simple password.
- Use John the Ripper to crack the password and document your process.
- Try to crack your password.
- You can give this a reasonable number of hours.
- It is unlikely that you will be able to crack it in a reasonable amount of time.

Report Requirements

- C2 System Design:
    - Explain your design choices, including the protocol (TCP/UDP) and error-handling mechanisms.
    - Provide a brief analysis of the potential risks associated with a C2 system and how this tool could be used maliciously.
- John the Ripper Analysis:
    - Describe the process of setting up the user account and cracking the password.
    - Discuss the time taken and any observations from using John the Ripper.

Constraints

- You can use any programming languages(s) of your choice.
- You cannot use existing C2 frameworks; you must implement the attacker and victim components yourself.
- All code must be your work. Collaboration is not allowed.
- You must not use any privileged or destructive commands during testing.
- Ensure compliance with legal and ethical standards when implementing and testing your solution.

Resources

- You may refer to class notes and resources.
- Your work must be substantially your own for tutorials or external references.

Submission

- Ensure your submission meets all the guidelines, including formatting, file type, and submission.
- Follow the AI usage guidelines.
- Be aware of the late submission policy to avoid losing marks.
- ***Note: Please strictly adhere to the submission requirements to ensure you don't lose any marks.***

Evaluation

Topic	Value
C2 System	40%
Design	20%
Testing	20%
Report	20%
Total	100%

Hints

- Consider how you will manage the connection between the attacker and victim, especially if using UDP.
- Think about error handling if the victim process crashes or is unreachable.
- Explore extending your C2 system to support additional commands or features.
- For the password cracking task, choose a simple password for the new user to ensure the process is completed in a reasonable time.