Author Details

- **Name:** Bharath, Tarun
- **Email:** sgowravam@albany.edu tkattasreenivasulu@albany.edu
- **Team Number:** 2
- GitHub

Questions

Answer the following questions about your tool. Your answers should be thorough and fully answer the question. Answers should be grammatically correct and be full sentences.

(8 points) What is the goal of this tool? What purpose does it bring to the competitions?

The goal of my script is to enable remote command execution and control over a network, providing an operator with the capability to interact with a target system. While acknowledging that such scripts are often associated with malicious activities, I built this tool with the intention of showcasing potential security threats and risks associated with unauthorized access. In the context of competitions, its purpose is educational, demonstrating the potential dangers of insecure remote command execution and the importance of securing systems against such threats.

(8 points) Did other tools influence your tool? If so, what are they? If not, what was your inspiration for the tool?

The script I developed draws inspiration from tools and techniques commonly associated with malicious activities, particularly those involving remote access and control. While I don't explicitly mention specific tools, the use of PowerShell for remote execution and network communication aligns with tactics observed in various remote access Trojans (RATs) and penetration testing frameworks. My inspiration for creating this script stems from the necessity to illustrate a covert and efficient method for controlling remote systems, a scenario commonly encountered in both malicious and security testing contexts.

(8 points) What is the feasibility of another team member quickly learning to use or contribute to your tool? What makes it easy or difficult to learn?

The feasibility of another team member quickly learning to use or contribute to this script depends on their familiarity with PowerShell, network protocols, and remote command execution concepts. Admittedly, the script currently lacks extensive documentation, making it challenging for a new team member to grasp its intricacies. The use of obfuscated code, network communications, and the implementation of a continuous loop for command exchange adds complexity. Insufficient comments and explanatory notes further hinder the learning process. To enhance feasibility, I acknowledge the need for comprehensive documentation, clear comments explaining each section, and adherence to coding best practices. This approach aims to facilitate quicker understanding and contribution, emphasizing ethical use in alignment with organizational security policies.