Phase 1

Project Initiation (August 21 - September 8, 2023)

Backlog Items for Implementation:

Implant

- Basic Post-Ex Tactics: Implement basic post-exploitation tactics to demonstrate control over the compromised system. This can involve simple actions like listing processes, accessing files, or gathering system information.
- Implant Registration on Server
- Persistence Mechanisms: Implement a basic persistence mechanism, such as a scheduled task or registry key manipulation, to ensure the implant survives system reboots and remains active.
- Anti-Virtual Machine (VM) / Sandbox Techniques: Implement basic anti-VM and anti-sandbox techniques to evade detection and analysis during the development phase.
- Credential Harvesting: Implement a simple credential harvesting module to gather usernames and passwords from the compromised system.

Server

- Multiple Listener Creation for Multiple Implants: Allow the server to create and manage multiple listeners to handle connections from multiple implants simultaneously.
- Implant Registration on Server
- Pluggable Modules Architecture for Extensibility: Implement a basic framework for allowing the addition of new modules and functionalities to the server in a modular and extensible manner.

Interface

- Resizeable: Ensure that the interface is resizable to adapt to various screen sizes and user preferences.
- Tab for Listener Creation: Create a dedicated tab in the interface to allow users to create and manage multiple listeners easily.
- Real-time Implant Monitoring and Reporting: Provide real-time monitoring and reporting of implant activities, such as connections, received data, and executed commands.

Hardware

- Buy ESP32: Procure the necessary ESP32 hardware for testing and development.