Initial Backlog

Implant

- Advanced Evasion Techniques
  - Module Stomping
  - Reflective DLL Injection
  - PE Loading
  - Heap Encryption
  - Thread Call Stack Encryption
  - PPID Spoofing
- Basic Post-Exploitation Tactics
- mTLS Authentication with Server
- Custom COFF Loading
- C2 Communication Encryption
- Anti-Debugging Techniques
- Process Injection (e.g., process hollowing, atom bombing)
- Anti-Virtual Machine (VM) / Sandbox Techniques
- Credential Harvesting
- Persistence Mechanisms (e.g., Scheduled tasks, registry keys)
- Data Exfiltration Methods (e.g., DNS tunneling, exfiltration over covert channels)
- Exploitation of Zero-day Vulnerabilities

Server

- Multiple Listener Creation for Multiple Implants
- Authorization
- mTLS Authentication with Implant
- Load Balancing for Multiple Implant Connections
- GeoIP-Based Routing of Implant Connections
- Pluggable Modules Architecture for Extensibility

Interface

- Resizeable
- Dark Theme
- Tab for Listener Creation
- Tab for Implant Setting Customization

- Tab for Security Customization
- Real-time Implant Monitoring and Reporting
- Integration with Threat Intelligence Feeds
- Multi-User Support
- Automated Response and Remediation Actions

Hardware

- Buy ESP32
- Customize to Download Implant Code