Robert Deal
Senior Design
October 1, 2023

Milestones:

- Selection/setup of environment
  - Approx 10% of total time
  - This involves putting together a network to test on which will include any devices that will be used for exploits later
- Creation of first example exploit
  - Approx 15% of total time
  - A single exploit for a single device to function as an example for further down the line and to build the rest of the system around
- Backdoor in exploit handler framework
  - Approx 25% of total time
  - This will consist of a handler that will send and manage a connection with custom backdoor devices so the user can interact with them with comparatively low effort
- Log management ability
  - Approx 25% of total time
  - The ability of the framework to manage and update any user logs on the target system in order to halt discovery by system admins and the like
- Frontend interface for user access
  - Approx 10% of total time
  - This will consist of a user interface, likely graphical web server based, that will allow for a simple and concise use of the functions of the system in order to effect a result for the user on the target
- Expansion of exploit devices
  - Approx 15% of total time (larger share if the previous ones take less time)
  - This will simply be adding more exploits to the system library in order to encompass move devices or other sorts of effects

Timeline Estimate:

- 1st week:
    - Create a real world physical network example so as to easily show the full capabilities of the project as well as an administrator's view
    - Create a virtual environment for the tool to be tested on in order to safely and quickly develop the following capabilities
- 2nd week:
    - Write a target handler that will create and manage backdoors or other sorts of connections established by the exploit crafter
- 3rd week:
    - Implement a way for the user to scan targets for exploitable vulnerabilities
- 4th week:
    - Write an exploit crafter that will load, assemble, and send payloads/exploits
- 5th week:
    - Write a target handler that will create and manage backdoors or other sorts of connections established by the exploit crafter
    - Build a framework that can manage the various different systems and processes of the tool
- 6th week:
    - Write a user interface that can call the various functions of the manager
- 7th week:
    - Create a system that can show all active logs on the target device and manipulate them to remove user activity
- 8th week:
    - Reinforce the handler to handle errors, crashes, and the ability to reupload code to the device
- 9th week:
    - Write a library of various exploits and payloads that can be used to compromise devices
- 10th week+:
    - Test and widen the library to function on as many devices as feasible

Effort Matrix:

- All tasks by Robert Deal