Comps Project Proposal:
Francisco, Ekow, Isha

Project Idea #1: <u>Project FIE</u> (Browser Extension Scanner)

- **Rough description (1 paragraph should be enough)**
  - Browser extensions are used to add features and customize web browsing, but they can also present a security risk. Many extensions request permissions (some more than needed) that allow them to read user data, monitor browsing behavior, inject scripts into web pages, or communicate with external servers. Malicious or poorly designed extensions can exploit these permissions to steal sensitive info, track users, or deliver malware.
  - The goal of this project is to study how malicious browser extensions operate and develop a security scanner that analyzes browser extensions and produces a security report.
- **List of potential deliverables**
  - **A website to search for browser extensions that returns security information about that extension**
    - **Code to**
      - Enumerates installed/searched browser extensions.
      - Extracts metadata such as permissions, background scripts, content scripts, and network access (API calls)
    - A rule-based or heuristic analysis engine that flags:
      - Excessive or dangerous permissions.
      - Use of obfuscation or dynamic code execution.
      - Suspicious network endpoints or behaviors
    - A scoring system to rate extension risk levels.
  - **Documentation**
    - A written report explaining:
      - Common attack techniques used by malicious browser extensions.
      - The design and architecture of the scanner.
      - Limitations of the approach.
    - A user guide explaining how to run the scanner and interpret its reports
  - **Data**
    - A dataset of known malicious or suspicious extension patterns.
    - Lists of dangerous permissions and API calls.
    - Sample benign and malicious extensions for testing.

- **Description of how you would test your project**
  - We could have a set list of browser extensions that we would know are risky
- **Potential barriers to success, questions you don't yet know the answer to, biggest worries, etc.**
  - Finding malicious browser extensions and getting access to their code or enough data to analyze

- **Anything else you want to say**
    - WE ARE EXCITED!

Project Idea #2: YARA-FIE SCANNER (YARA Rules)

- Rough description (1 paragraph should be enough)
    - YARA is a pattern-matching tool used to identify and classify malware. We would create a scanner using YARA rules built around shared malicious characteristics of old malware samples.
- List of potential deliverables
    - Project Proposal
    - Create a Virtual Machine
    - Build a collection of old malware samples to create simple YARA rules around
    - Create a base YARA tool with basic rules to identify sample malware files
    - Improve our tool by developing auto-detection malware patterns for our tool.
    - Run YARA rules with auto-detected patterns on new samples

- Description of how you would test your project
    - We would create and verify the Virtual Machine Setup
    - Safely execute the malware program to ensure isolation
    - Test the base YARA tool by running predefined YARA rules against a sample of malware
    - Measure the accuracy and false positives of this tool
    - Add an auto-detection component and compare results against the base rules
- Potential barriers to success, questions you don't yet know the answer to, biggest worries, etc.
    - Executing malware samples safely
    - Creating and understanding a YARA tool complex enough to avoid high false positive rates
    - Finding large data sets
- Anything else you want to say
    - We are interested in introducing YARA rules to our browser extension project idea, to automatically categorize specific types of browser extensions