Presentation outline:

1. Title of project and presenters
2. Project goal
   1. Create a tool for scanning devices in a given network
   2. Scan for open ports and potential vulnerabilities in the services running
   3. To be used by team members to scan networks for potential vulnerability points of entry
3. Project background info: Mentions that it primarily uses Nmap and Pyqt
   1. Frontend – GUI with PyQt5
   2. Backend
      1. Nmap commands for scanning range of IP’s
      2. Asynchronous support for scanning without blocking
      3. Access NVD API to search for CVE’s of selected ports
4. Nmap in depth (pyqt?)
   1. Flowchart or diagram of program flow?
   2. Ping scan to expose all devices in the network (returns list of IP’s)
   3. Port scan on given IP to expose all listening ports
   4. Version scan to show which service and version is running on selected port
      1. Use NVD API to get CVE’s for the selected port’s service and version
5. Installer
   1. Python program and its module dependencies packaged into an executable (using pyinstaller)
   2. Can be ran on any device with Python3 (included in Ubuntu out of the box)
   3. Depends on nmap being installed on system
      1. When launching, application checks if nmap is installed
      2. If not installed, prompts the user to install on their behalf.
6. Demonstration slides. Screenshots and explanation
7. Final slide of demo shows CVEs, brief explanation of the CVE
8. Issues (past and current?)
   1. Portability (installer)
   2. Hanging due to synchronous functions
   3. General bugs
      1. Managing dynamically created elements in PyQt
9. Future direction(s)
   1. Network mapper topology
   2. Report generation and export in pdf format
   3. Bypassing anti-virus and firewall