Plan (Non-Technical Version)

Tuesday, January 14, 2025 8:00 AM

End goal:

- AI model based on NIST SP 800-40 R4
- Collect update and patch information from Windows and Debian systems
- Analyze collected update information to assess vulnerabilities, patch status, and compliance with NIST 800-40 R4
- Generate report based on NIST guidelines, inventory, prioritization, compliance status

Required components:

- Agent running on Windows / Debian systems to gather OS update data and send to centralized server

- Centralized server
    - Collect / aggregate OS update data
        - Data to send to server (no AI involved):
            - Date / Time
            - OS Name
            - OS Version
            - Computer Name
            - IP Address of computer

        - Data to send to server (AI portion):
            - List of security updates available

    - Run data through AI model (analyzing update information, prioritize patches), use this data for the report
        - Rank available updates based on security severity

    - Compile report with all information given to server

    - Web Interface
        - Generate NIST-compliant report based on AI output of information
        - Ability to download report as PDF or DOCX

Current Issues:

- Agent script that sends computer info to the server is only built to handle one computer
- Passwords are required when running the script
- Passwords are required when running SCP commands (last 2 lines of script)