**CYB 333 Midterm**

Jonathan Ricafrente

National University, School of Engineering and Computing, BS Cybersecurity Program

CYB 333 Security Automation

Sean Ayersman

June 22, 2025

The following hyperlink will direct you to my GitHub repository, which contains the uploaded Python scripts required for the midterm. Explanations are provided in each script to identify the required components of the midterm (Ricafrente, 2025).

<https://github.com/R1CA4R3NT3/MIDTERM.git>

Written Reflection Using the criteria listed in the midterm instructions for the socket and port scanner implantation, I employed a systematic approach in drafting the python script for each. With the help of Visual Studio Code and GitHub Copilot suggestions, I drafted the basic client-server communication script using the suggested Python sockets demonstrated in ITPROTV. , The server code listens for connections on a specified port and echoes back any messages received from the client (Ricafrente, 2025). The client code connects to the server, sends a message, and prints the server's response. After laying out the primary objective of the scripts, I began to implement script to satisfy the proper shutdown handling and error reporting. With the help of copilot, I assembled the strings to achieve and report those requirements.

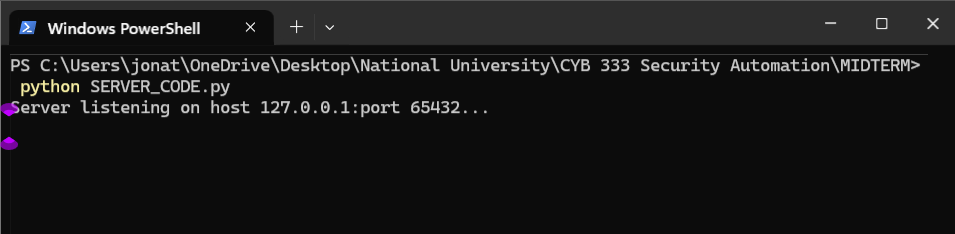
In drafting the local port scanner script, I utilized a similar approach but created the strings for the error reporting, failed port reporting, and error handling individually and incorporated them into my script. Again, with the help of VS Code debug and copilot functions, I could consolidate all the strings in a logical format for execution. The only challenges I encountered was integrating the script drafted in VS code and publishing to GitHub. The process was not difficult thanks to the user friendly interface of VS code. The challenge was acquainting myself with the configuration requirements for GIT and settings within GitHib.

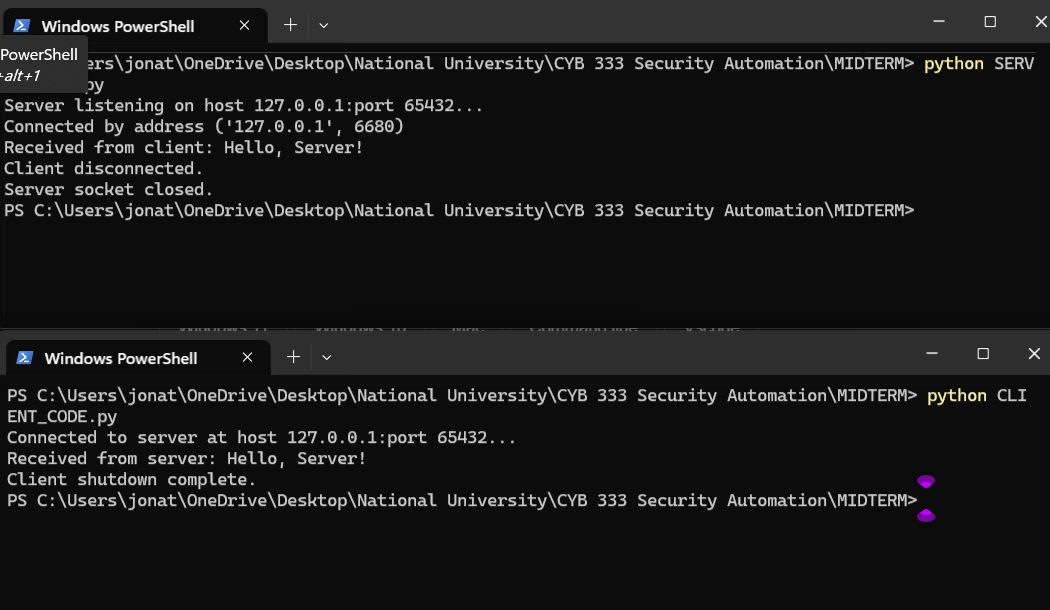
I activated multi-layer authentication with the third-party app Authy and set all my repositories to public to avoid any issues for users viewing my code.

Using any port scanner is essential for checking network issues, learning cybersecurity, or testing network services. Legally, scanning systems not under your or your organization purview without permission is unauthorized access. Ethically, users’ intentions are relevant but do not offer a strong defense. Even if no damage occurs, unauthorized scanning is intrusive as it can reveal sensitive or privileged information. In summary, port scanning is acceptable when accomplished in a controlled way and with authorization.

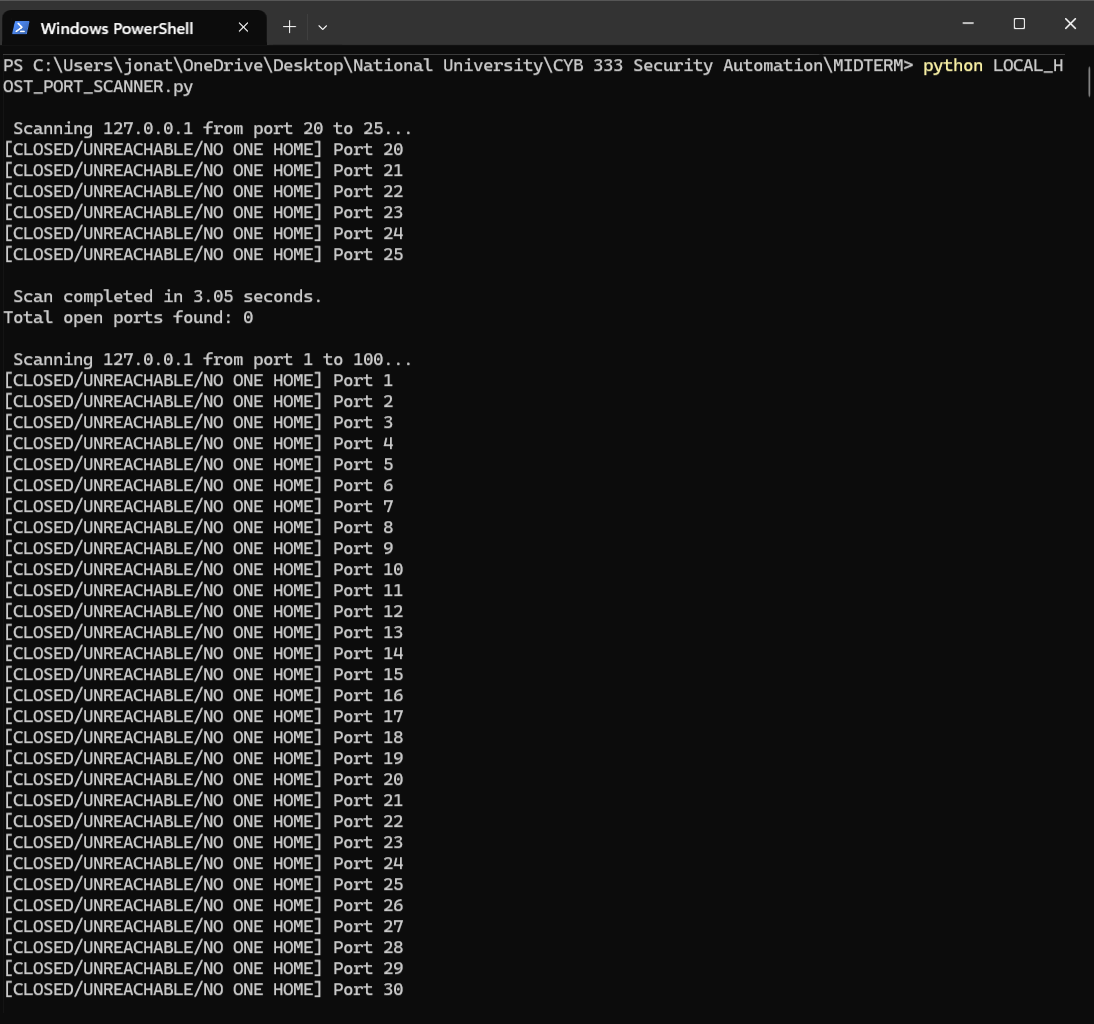
I learned that GitHub is a powerful open-source tool to help troubleshoot or create network solutions.

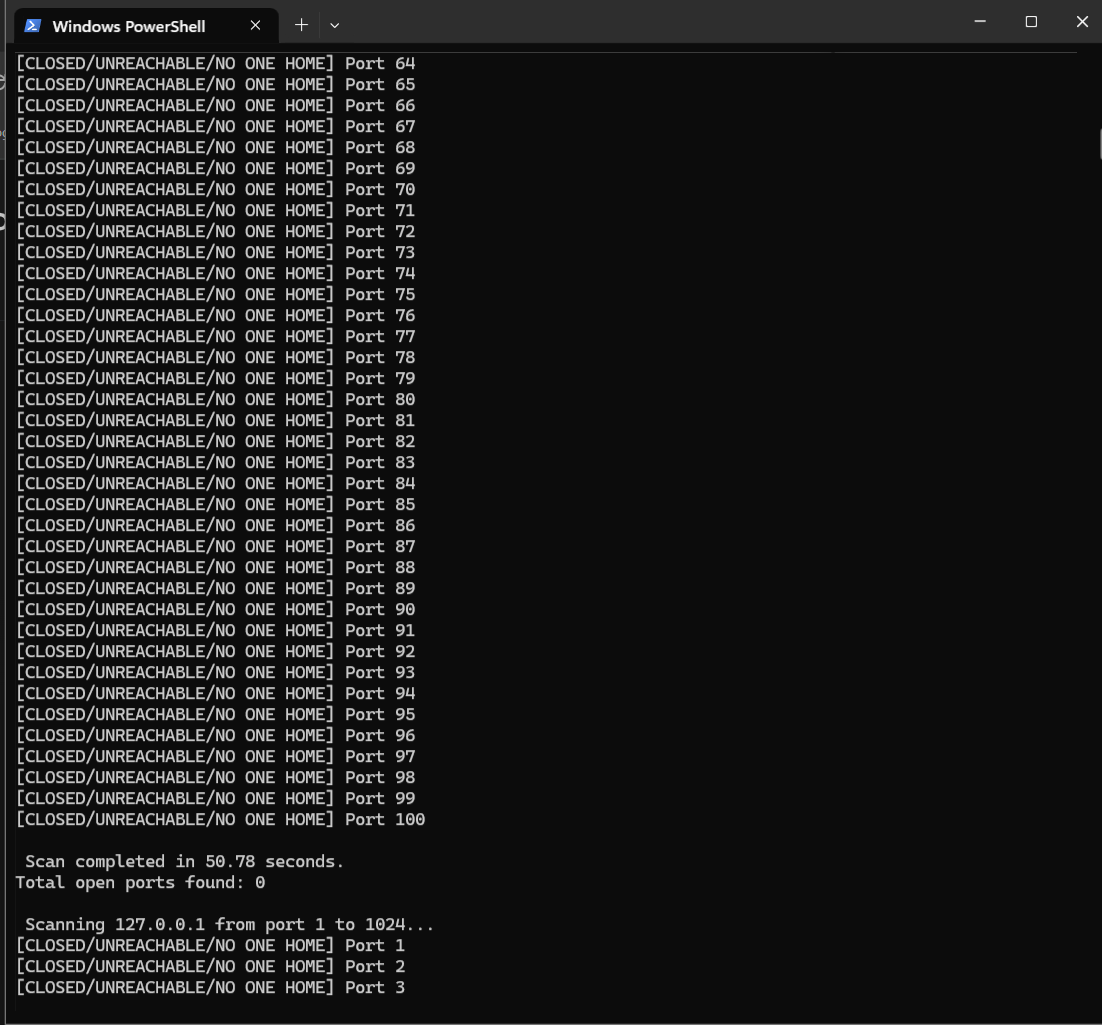
Program Execution Screenshots

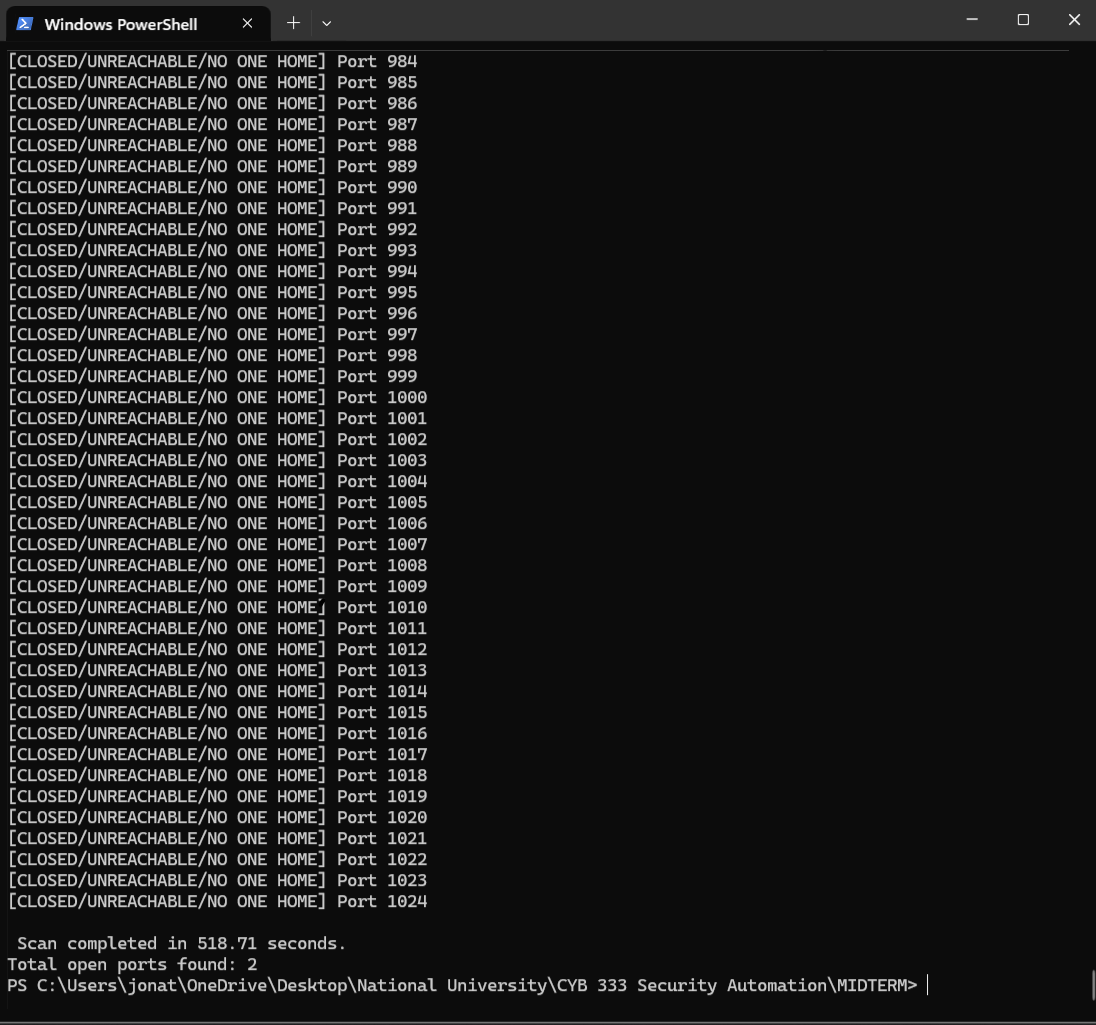
Server Script

Client to Server Script Interaction

LOCAL PORT 20-25 SCANNER RESULTS AND PERFORMANCE



LOCAL PORT 1-100 SCANNER RESULTS AND PERFORMANCE

LOCAL PORT 1-1024 SCANNER RESULTS AND PERFORMANCE

References

Ricafrente, J. (2025, June 22). *R1CA4R3NT3/midterm: Midterm for cyb333*. GitHub. <https://github.com/R1CA4R3NT3/MIDTERM>