PROJECT SPEC

Network Scanner Tool Using Nmap

Aidan Moloney

Contents

Introduction

Most network scanning tools available today are extremely effective, but their steep learning curve can deter users from utilising them. The more advanced the tool, the more precise the commands and syntax the user must master to perform a scan.

The other issue with these scanning tools is the reproducibility of the command needed for a scan. It is unreasonable to expect someone to remember the specific command they need for one particular scan. When a user is running multiple scans with complex commands it becomes nigh impossible to remember each command in its entirety. The time spent checking documentation for the commands and syntax required for a specific scan can add up very quickly and slow down the user.

This project aims to address these issues by developing a tool that simplifies network scanning, making it more user-friendly through a GUI that allows users to initiate common scan types with a single click. Additionally, the tool will enable users to extend its functionality by creating custom scans and integrating them into the application for future use.

Deliverables

Core Deliverables

Network Scan

The core feature of this project is its functionality as a network scanner. To achieve this, I will utilize the Nmap API to perform a variety of scans in a test environment, ensuring the tool fulfils this requirement.

Default Scan Buttons

Once the scanning capabilities of the tool have been confirmed the next step is to create a list of the most commonly used scans and add them to the GUI as default buttons the user can select. Once selected these buttons will auto-fill in the command required for the scan. The user will be prompted for the IP range of the scan and the ports they wish to scan.

The goal of this feature is to reduce the initial learning curve of Nmap by allowing users to simply open the tool and begin scanning targets. This will obviously not be quite as effective as custom command created to suit the specific use case of each user however I believe that is a reasonable trade-off for the speed and ease of use.

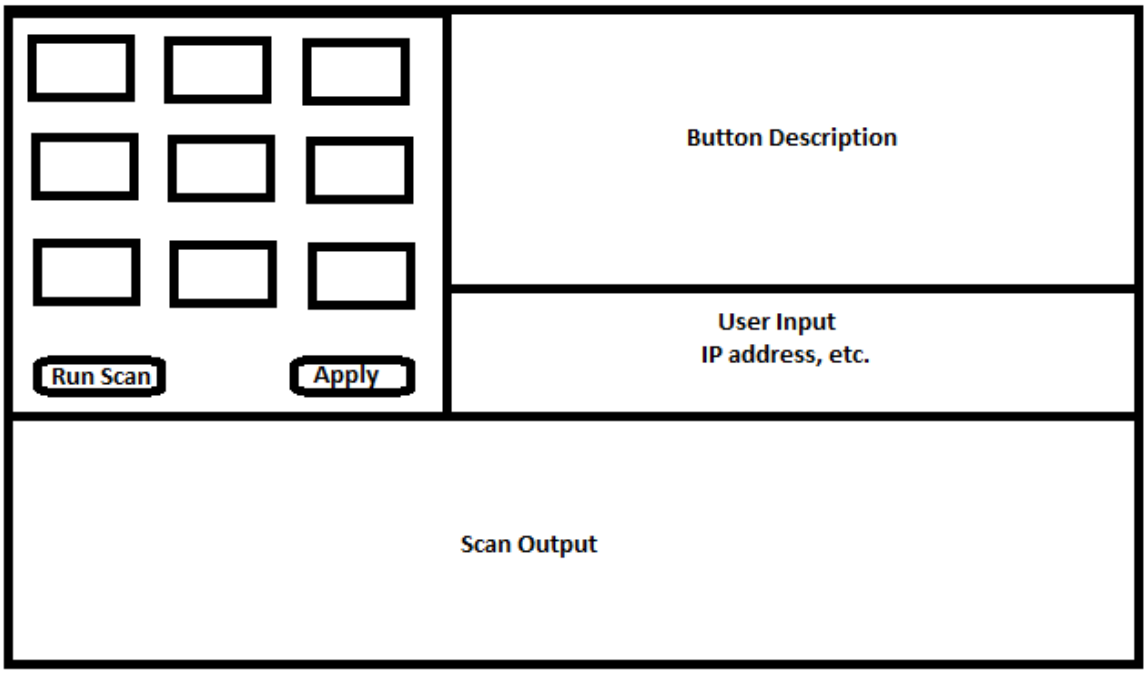
Custom Buttons

Furthermore, the plan is to enable users to create custom buttons for scans that are not included in the default set. To do this, the user will enter the desired command and create a button corresponding to the command. This allows the user to execute their custom scan with a simple click. I believe this feature will be particularly beneficial for network engineers who need to run complex scans across their network, as it eliminates the need to memorize or look up the full Nmap command each time they need to use it.

Non-Core Deliverables

Appealing design

The tool will be primarily designed for functionality and ease of use as a network scanner. If possible, I would like to make the tool more appealing to users by having a simple GUI that is aesthetically pleasing and user-friendly. Below is a preliminary design for the fully finished GUI, this design is liable to change as development continues.



Use Cases

Like many other cybersecurity focused tools there is no way for me to predict how exactly how this tool will be utilised. I am aware that once the tool is available users will find new uses, I had not considered or bend the tool for a purpose I may have thought

impossible. Nevertheless, I will give some examples of use cases for this tool that I considered while developing it.

Network Engineer

The primary use case for this tool will be fir network engineers who may be required to scan a network multiple times throughout the day to test for different things such as the number of machines active on the network.

Take for example a network engineer tasked with scanning a corporate network to identify and patch any possible vulnerabilities. The engineer opts to use Nmap for this task as it is extremely reputable and very well documented.

Pentesting

Similarly to a network engineer a pentester will conduct multiple complex scans, the difference is that unlike the network engineer the pentester will be scanning a variety of different networks. Having the commands for complex network scans ready at the click of a button will greatly increase the ease and speed at which a pentester can identify potential vulnerabilities on a target network.

Inspiration

The inspiration for this project came from my attempts to use Zenmap, a GUI for Nmap. Zenmap attempts to make Nmap more user friendly by creating a GUI to interface with Nmap and add other features that make it more user friendly than using Nmap through a command line. However, I discovered that when using Zenmap, the full Nmap commands were still required. This posed the biggest hurdle for a user to overcome when trying to use Nmap. I felt that Zenmap had not sufficiently addressed the aspect of Nmap most hostile to users. As a result of this experience, I began to wonder if there was any way I could address this issue myself. When presented with the opportunity to develop a project I decided it was the perfect opportunity to try and put this idea into practice. My idea for button to save command came from by my time learning cryptography and trying to decode cryptographic algorithms using python. Comparing the difficulties I had doing this to the simplicity of using a tool like CyberChef where decryption is as easy as clicking a button, inspired me to adopt a similar approach for my project.

Timeline

Name	Duration	Start	Finish
Phase 1: Project Documentation	**82**	**10/09/2024**	**02/12/2024**
Research Report	62	10/09/2024	11/11/2024
Project Spec	20	12/11/2024	02/12/2024
Phase 2: Development	**99**	**23/11/2024**	**02/03/2025**
Basic Network Scanner	7	23/11/2024	30/11/2024
GUI for network Scanner	22	01/12/2024	23/12/2024
Button for most common scans	26	27/12/2024	22/01/2025
Customizable buttons	39	23/01/2025	02/03/2025
Phase 3: Testing	**46**	**03/03/2025**	**28/04/2025**
Building a testbed	15	03/03/2025	18/03/2025
Testing completed tool	41	18/03/2025	28/04/2025
Phase 4: Final Documentation	**22**	**06/04/2025**	**28/04/2025**