كلية
AD8
تكنولوجيا المعلومات وعلوم الحاسوب

<< NetRiskScanner >>

Advanced Network Risk Assessment by AI and Scanning Tool

Authors:
Mohammad Majdalawy (2021904045)
Mustafa Banikhalaf (2021904052)

Supervised By
Dr. Malek Barhoush

Graduation Project | 2024 -2025

FINAL YEAR GRADUATION PROJECT

Information Technology Department
Faculty of Information Technology and Computer Science
Yarmouk University
Irbid - Jordan

Contact Information

This Project report is submitted to the Department of Information Technology/Cyber Security program at Yarmouk University in partial fulfilment of the requirements for the degree of Bachelor of Information Technology in Cyber security.

Authors:

1- Mohamad Majdalawy (2021904045)

Address: Irbid, Jordan

E-mail: 2021904045@ses.yu.edu.jo

2- Mustafa Banikhalaf (2021904052)

Address: Irbid, Jordan

E-mail: 2021904052@ses.yu.edu.jo

2025 – January

Supervisor:

Dr. Malek Barhoush

Business Information Technology

Department of Information Technology

Internet: http://yu.edu.jo

Faculty of Information Technology and Computer Sciences

Phone: +962 2 72711111 Ext. 2561

Yarmouk University, Jordan

Fax: +962 2 7211111

Graduation Project Report

Department of Information Technology

Faculty of Information Technology and Computer Sciences

Yarmouk University – Jordan

Intellectual Property Right Declaration

This is to declare that the work, under the supervision of Dr. Malek Barhoush, titled “NetRiskScanner: Advanced Network Risk Assessment and Scanning Tool” carried out in partial fulfillment of the requirements for the degree of Bachelor of Cybersecurity, is the sole property of Yarmouk University and the respective supervisor. It is protected under intellectual property laws and conventions. Any use of this work, including extension, enhancement, or commercial application, must have prior permission from the University and the respective supervisor.

Date: 9/1/2025
Author(s):
Name: Mohamad Majdalawy
Signature: ______________________
Name: Mustafa Banikhalaf
Signature: ______________________
Supervisor(s):
Name: Dr. Malek Barhoush
Signature: ______________________

Anti-Plagiarism Declaration:

This is to declare that the above publication produced under the supervision of Dr. Malek Barhoush having title "NetRiskScanner: Advanced Network Risk Assessment and Scanning Tool" is the sole contribution of the author(s) and no part hereof has been reproduced illegally (cut and paste) which can be considered as Plagiarism. All referenced parts have been used to argue the idea and have been cited properly. I/We will be responsible and liable for any consequence if violation of this declaration is proven.

Date: 9/1/2025

Author(s):

Name: Mohamad Majdalawy

Signature: _____________

Name: Mustafa Banikhalaf

Signature: _____________

ACKNOWLEDGMENTS

We express our deepest gratitude to our supervisor, Dr. Malek Barhoush, for their invaluable guidance and support throughout this project. Special thanks to our families and friends for their unwavering encouragement and belief in us.

Abstract:

NetRiskScanner simplifies network security auditing by integrating a graphical interface with Nmap's powerful command-line scanning capabilities. It allows users to perform various network scans, including port detection, OS identification, service enumeration, and network risk assessment, with user-friendly controls and real-time feedback. The tool incorporates threading for efficient execution, robust validation to minimize errors, and output exporting to enhance usability. This project demonstrates a practical application of cybersecurity principles and addresses the complexities of network scanning through an accessible and effective interface. The inclusion of advanced features like risk analysis makes it a comprehensive tool for network security evaluation.

Screen about tool interface

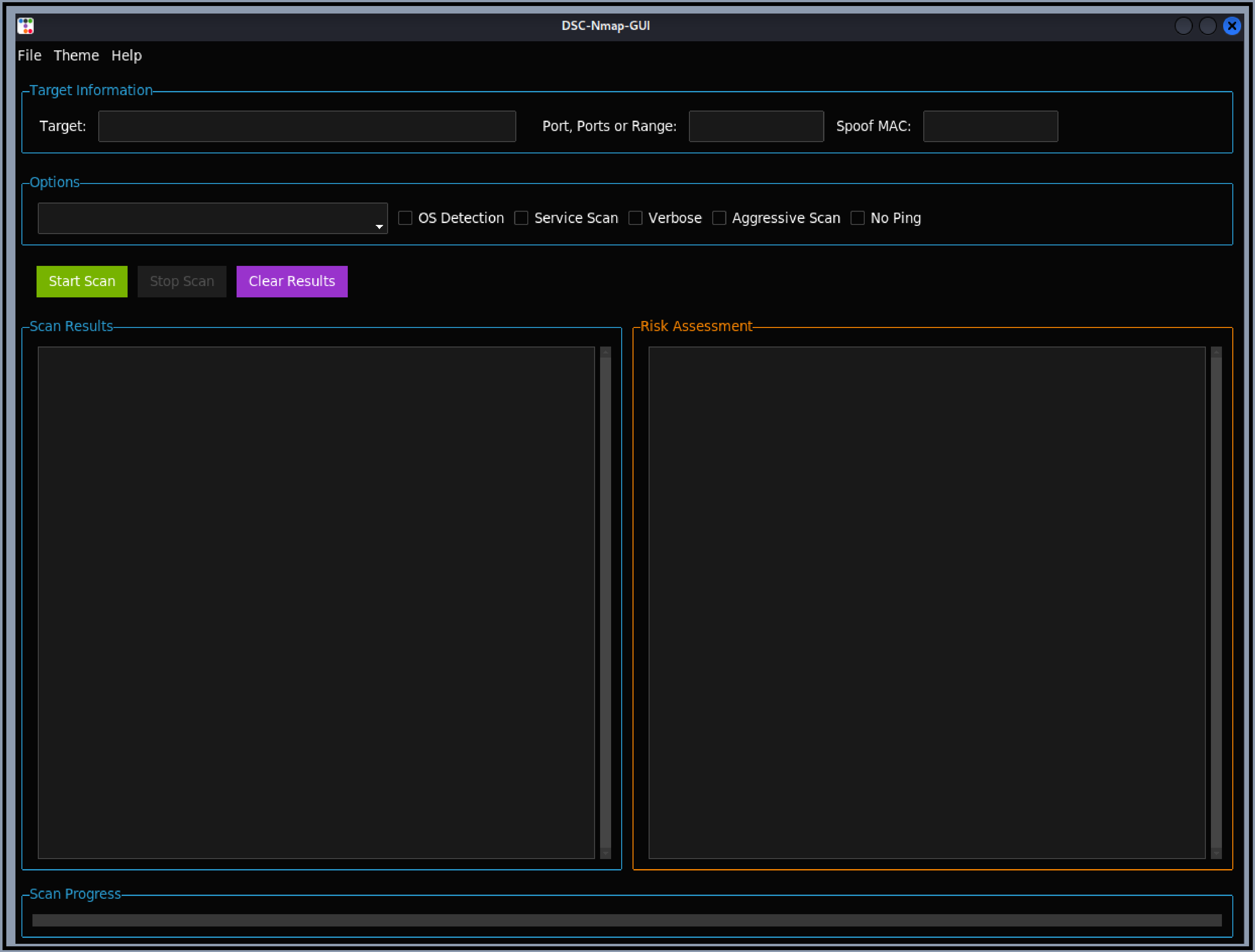

DSC-Nmap-GUI
File
Theme
Help
Target Information
Target:
Port, Ports or Range:
Spoof MAC:
Options
☐ OS Detection
☐ Service Scan
☐ Verbose
☐ Aggressive Scan
☐ No Ping
Start Scan
Stop Scan
Clear Results
Scan Results
Risk Assessment
Scan Progress

Table of Contents:

1.Introduction:

NetRiskScanner
Advanced Network Risk Assessment by AI and Scanning Tool

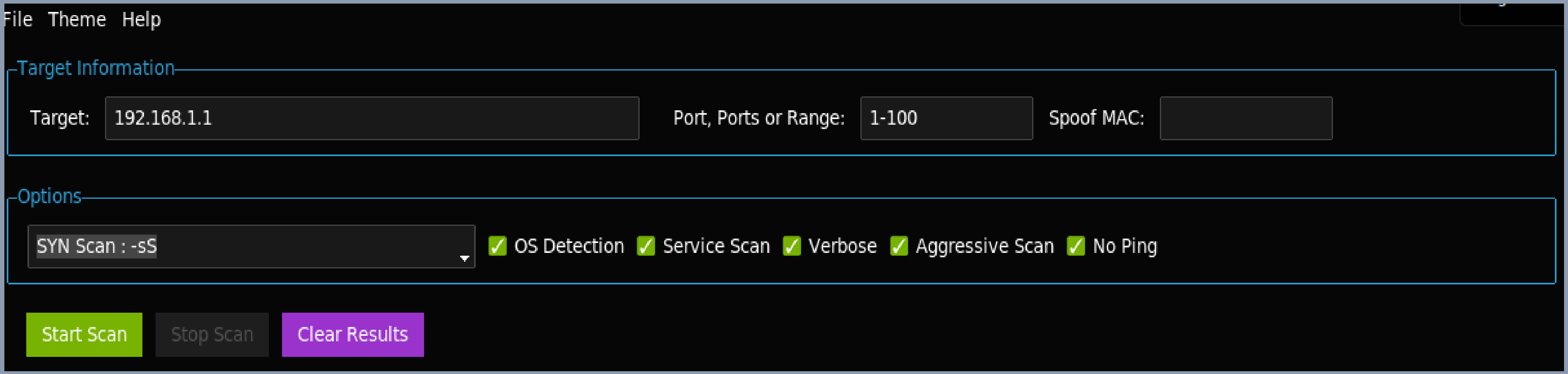
project is an initiative aimed at leveraging the capabilities of Nmap, a powerful open-source network scanning tool, to enhance network security and performance analysis. This project builds upon the foundational functionalities of Nmap to provide additional features, streamlined workflows, or customized functionalities tailored to specific use cases in network management and cybersecurity.

What is Nmap?

Nmap (Network Mapper) is a widely used tool in the field of cybersecurity and network administration. It allows users to perform tasks such as:

- Network Discovery: Identifying devices and hosts on a network.
- Port Scanning: Detecting open ports and associated services on networked devices.
- Vulnerability Assessment: Analyzing system vulnerabilities by identifying weak points in the network.
- Service Detection: Determining running services and their versions.

Screen about Tool Services



Target: 192.168.1.1

Port, Ports or Range: 1-100

Spoof MAC:

SYN Scan : -sS

☑ OS Detection ☑ Service Scan ☑ Verbose ☑ Aggressive Scan ☑ No Ping

2. Purpose of the Project:

The purpose of NetRiskScanner is to provide a user-friendly interface for conducting advanced network scans using Nmap. By abstracting the complexities of command-line operations, this tool allows cybersecurity professionals and students to easily analyze networks, identify vulnerabilities, assess risks by AI, and ensure system security.

3. Scope of the Project:

The project focuses on integrating essential Nmap functionalities, including target validation, various scan types, real-time progress updates, and risk assessment features into a graphical user interface (GUI). The tool targets individuals with limited command-line experience while maintaining robust scanning capabilities for advanced users.

4. Benefits of the Project:

- **Simplifies the process of network scanning and risk assessment through an intuitive GUI.**
- **Provides real-time feedback on scan progress and results.**
- **Ensures efficient and accurate scans with built-in validation mechanisms.**
- **Facilitates result export for reporting and documentation purposes.**
- **Introduces advanced features for identifying and evaluating network vulnerabilities and risks.**

5.System Analysis:

- **Existing Systems:**

Existing network scanning tools like Nmap rely heavily on command-line interfaces, which can be intimidating for inexperienced users. Moreover, these systems often lack interactive feedback and require extensive knowledge of command syntax. Risk assessment features are also typically separate from scanning tools, making comprehensive evaluation cumbersome.

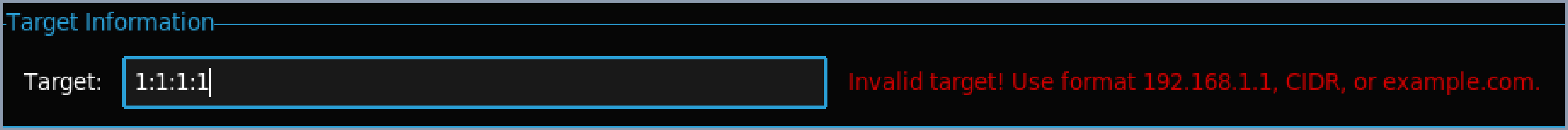
- **Problems in Existing Systems:**
    - **Steep learning curve for non-technical users.**
    - **Limited accessibility for those unfamiliar with command-line tools.**
    - **Difficulty in managing large-scale scans without progress tracking or export options.**
    - **Absence of integrated risk assessment features.**

6. Proposed Solutions :

- **NetRiskScanner addresses these issues by providing:**

- **An intuitive graphical interface.**

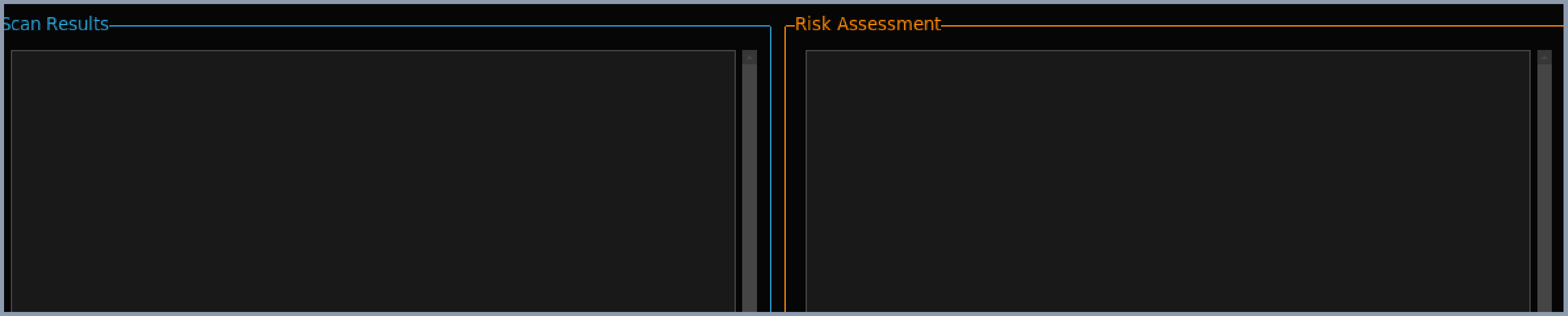
- **Robust input validation to minimize errors.**

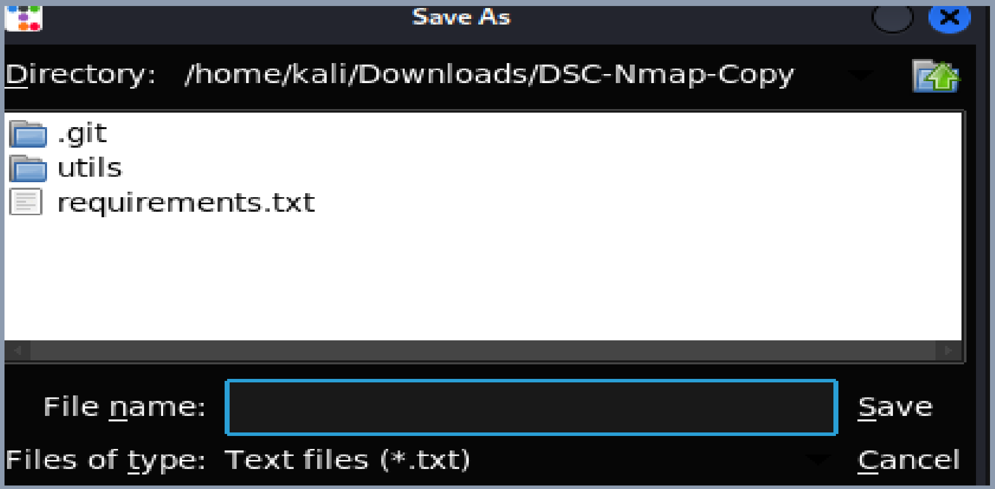


Target: 1:1:1:1

Invalid target! Use format 192.168.1.1, CIDR, or example.com.

- **Real-time progress updates and detailed results.**
- **Risk analysis integrated with scan results.**
- **Functionality to export scan outputs for further analysis.**





Directory: /home/kali/Downloads/DSC-Nmap-Copy

.git
utils
requirements.txt

File name:

Files of type: Text files (*.txt)

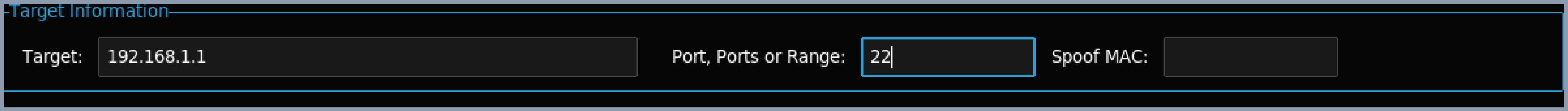
7.System Design :

1. System Architecture:

- The architecture integrates the following modules:
- GUI Module: Manages user input and displays outputs.
- Scan Execution Module: Manages threading and Nmap command execution.
- Validation Module: Ensures correct input formats for targets and ports.
- Result Parsing Module: Processes Nmap outputs and displays them in a structured format.
- Risk Assessment Module: Analyzes scan results to provide insights on potential vulnerabilities and threats.

8.Component Descriptions:

- **Input Fields: Collect target IP/domain and port range.**



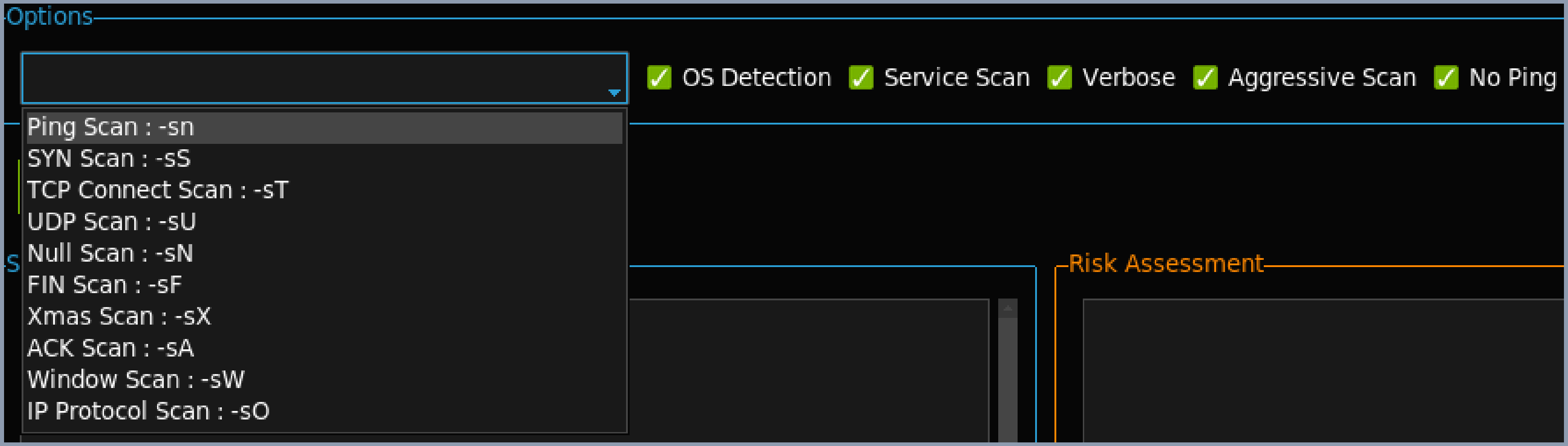
Target Information

Target: 192.168.1.1

Port, Ports or Range: 22

Spoof MAC:

- **Dropdowns and Checkboxes: Allow users to select scan types and additional options like OS detection.**

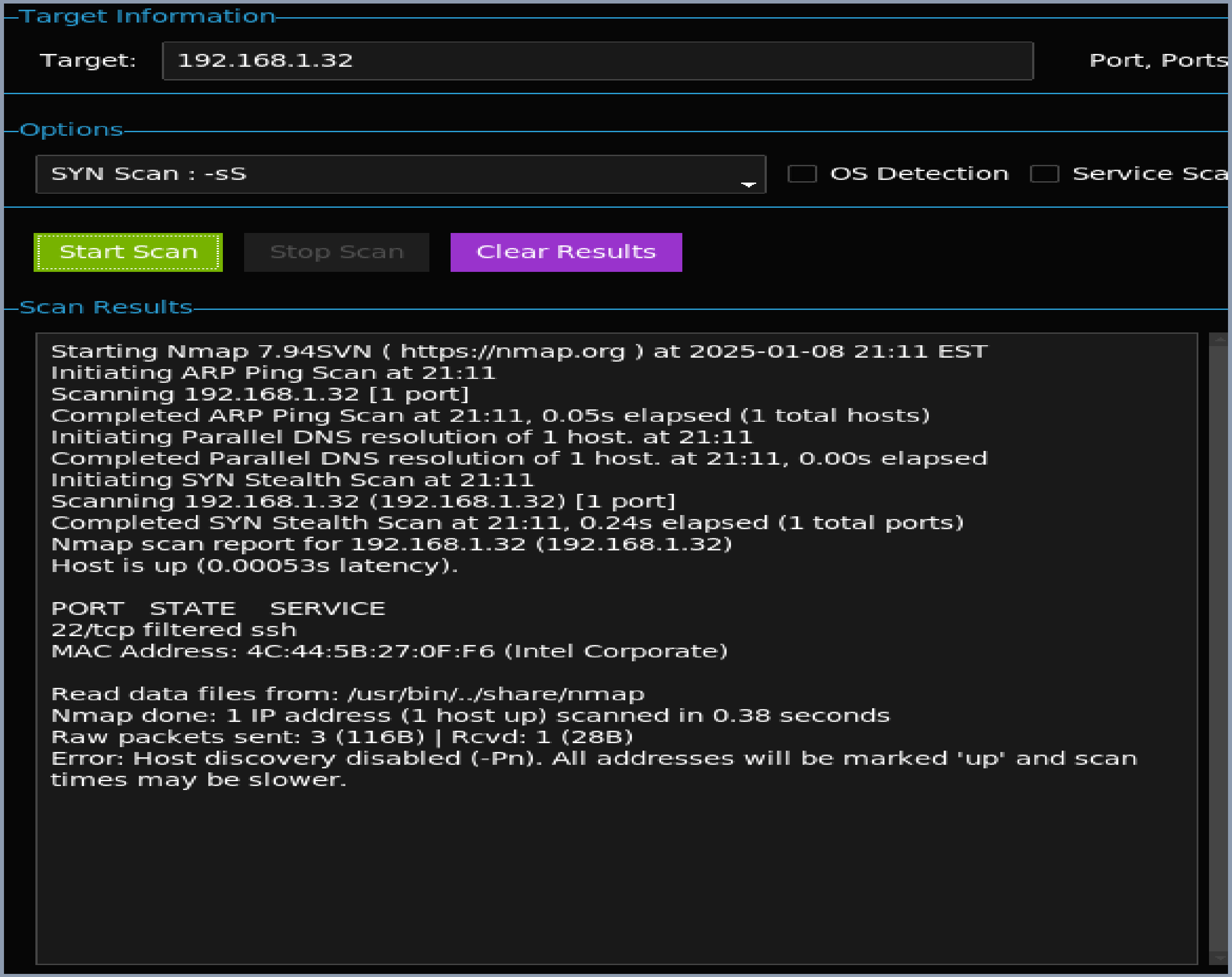


Options

☑ OS Detection ☑ Service Scan ☑ Verbose ☑ Aggressive Scan ☑ No Ping

Ping Scan : -sn
SYN Scan : -sS
TCP Connect Scan : -sT
UDP Scan : -sU
Null Scan : -sN
FIN Scan : -sF
Xmas Scan : -sX
ACK Scan : -sA
Window Scan : -sW
IP Protocol Scan : -sO

- **Risk Assessment: Provides detailed insights into potential vulnerabilities based on scan results.**
- **Export Functionality: Save results to text files for future reference.**
- **Result Display: Show real-time scan progress and outputs.**



Target: 192.168.1.32

Port, Ports

SYN Scan : -sS

□ OS Detection □ Service Sca

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 21:11 EST
Initiating ARP Ping Scan at 21:11
Scanning 192.168.1.32 [1 port]
Completed ARP Ping Scan at 21:11, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:11
Completed Parallel DNS resolution of 1 host. at 21:11, 0.00s elapsed
Initiating SYN Stealth Scan at 21:11
Scanning 192.168.1.32 (192.168.1.32) [1 port]
Completed SYN Stealth Scan at 21:11, 0.24s elapsed (1 total ports)
Nmap scan report for 192.168.1.32 (192.168.1.32)
Host is up (0.00053s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 4C:44:5B:27:0F:F6 (Intel Corporate)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
Raw packets sent: 3 (116B) | Rcvd: 1 (28B)
Error: Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
times may be slower.
```

9.Implementation and Validation:

- ## Key Functionalities:

  - **Target Validation: Ensures valid IPs, domains, and port ranges.**
  - **Scan Options: Supports multiple scan types, including TCP, UDP, OS detection, and risk analysis.**
  - **Real-Time Updates: Displays progress and results dynamically.**
  - **Threading: Ensures responsive GUI during scan execution.**
  - **Risk Assessment: Identifies potential vulnerabilities and prioritizes risks for mitigation.**
  - **Result Export: Allows users to save scan outputs for reporting.**

- **Validation and Testing:**
  - **Functional Testing: Verified all input fields, scan options, and result displays.**
  - **Stress Testing: Conducted scans on large networks to ensure stability.**
  - **Usability Testing: Gathered feedback from peers to refine the interface and features.**
  - **Risk Validation: Evaluated the accuracy of risk assessment by comparing outputs with known vulnerabilities.**

10.Conclusion and Future Enhancements:

Conclusion:

NetRiskScanner successfully bridges the gap between powerful network scanning capabilities and ease of use. By abstracting complex commands into a simple interface and incorporating risk analysis, the tool empowers users to conduct comprehensive network audits efficiently and identify vulnerabilities effectively.

Future Enhancements:

- **Add advanced visualization of scan results.**
- **Incorporate support for additional Nmap features like scripting and firewall evasion.**
- **Expand compatibility for cross-platform use.**
- **Integrate machine learning algorithms to enhance risk prediction and vulnerability analysis.**

11. References:

- **Nmap Documentation: https://nmap.org/docs.html**

- **Python Tkinter Library: https://docs.python.org/3/library/tkinter.html**

- **Threading in Python: https://docs.python.org/3/library/threading.html**

- **To install tool: https://github.com/MustafaFBK/DSC-Nmap-Copy.git**