Cybersecurity Final Year Project Functional Requirements

**Student Name:** Charlotte Strobl

**Degree and Major:** Bachelors in Cybersecurity

**Project Advisor**: Professor Henderson

**Expected Graduation Date**: August 2025

# Functionality

## 1.1 - Display Host Disk Information

**Priority**: High

**Description**: The system should display host disk information including total size, space remaining, and disk health.

**Rationale**: This provides essential system health information for users, enabling them to monitor disk usage and health to prevent failures.

**Fit Criterion**: The system must display the total disk size, remaining space, and health status (healthy, warning, critical).

## 1.2 - Display Operating System and Version

**Priority**: High

**Description**: The system should display the operating system and version.

**Rationale**: To provide users with information about the system’s environment and compatibility.

**Fit** **Criterion**: The operating system name and version must be accurately displayed on the dashboard.

## 1.3 - Display System Name and IP Address

**Priority**: High

**Description**: The system should display the system name and IP address.

**Rationale**: This allows users to easily identify the device in the network and ensures accurate network monitoring.

**Fit** **Criterion**: The system name and IP address must be visible in the system information section of the dashboard.

## 1.4 - Display Last Boot Time

**Priority**: Medium

**Description**: The system should display the last boot time.

**Rationale**: The last boot time provides an indication of the system's uptime and performance.

**Fit** **Criterion**: The system must show the accurate time of the last boot in the dashboard.

## 2.1 - Port Scanning Identification

**Priority**: High

**Description**: The port scanning feature should accurately identify open and closed ports on the target device.

**Rationale**: This is essential for diagnosing network vulnerabilities and ensuring security.

**Fit Criterion**: The tool must list open and closed ports for the target device and display the status next to each port.

## 2.2 - Port Scanning Visual Representation

**Priority**: High

**Dependency**: 2.1 – Port Scanning Identification

**Description**: The port scanning feature should display a visual representation of the open and closed ports in a grid format.

**Rationale**: A visual representation aids in easier comprehension of the scan results.

**Fit** **Criterion**: The port scan result should be displayed in a grid format with visual indicators for open and closed ports.

## 2.3 - Port Information on Click

**Priority**: Medium

**Dependency**: 2.2 - Port Scanning Visual Representation

**Description**: The user should be able to click on a port to see more information about where it is routed.

**Rationale**: This allows users to understand the specific network paths for each open port.

**Fit** **Criterion**: When a user clicks on a port, detailed information about the port's routing should be displayed in a side panel.

## 3.1 - Network Discovery Identification

**Priority**: High

**Description**: The Network Discovery feature should identify active IP addresses of devices within the network.

**Rationale**: Network Discovery helps users identify all active devices in the network for troubleshooting or security audits.

**Fit Criterion**: The tool should display a list of active IP addresses in the network.

## 3.2 - Host Name Display in Network Discovery

**Priority**: Medium

**Dependency**: 3.1 - Network Discovery Identification

**Description**: The system should display the host name of each identified device in the network, if available.

**Rationale**: Displaying the host name of devices helps users to identify them more easily.

**Fit Criterion**: The host name should be displayed next to the IP address of each device in the Network Discovery section.

## 4.1 - Side Navigation Panel

**Priority**: High

**Description**: The system should include a side navigation panel for easy access to various tools and features.

**Rationale**: The side navigation improves usability and navigation between different sections of the tool.

**Fit** **Criterion**: The side navigation should be visible at all times and provide links to all the major sections of the tool (System Information, Port Scanning, Network Discovery, etc.).

## 4.2 - Display Sections for Each Feature

**Priority**: High

**Description**: Each tool or feature should have a section within the dashboard with relevant information clearly displayed.

**Rationale**: Organized sections help users find the information they need quickly.

**Fit** **Criterion**: The dashboard should display distinct sections for Disk Information, OS, System Information, Network Discovery, and Port Scanning.

# Look and Feel

## 5.1 - Minimalistic Dark Theme Design

**Priority**: High

**Description**: The dashboard should have a minimalistic design with a dark theme to ensure ease of use and a modern aesthetic.

**Rationale**: A minimalistic design makes it easier for users to focus on key information, while the dark theme reduces eye strain.

**Fit Criterion**: The dashboard should have a clean design with all essential features displayed without unnecessary clutter, and a dark theme should be applied.

# Usability

## 6.1 - Seamless Navigation

**Priority**: High

**Dependency**: 4.1 – Side Navigation Panel

**Description**: The system should have easy-to-use navigation, allowing users to seamlessly switch between features via the side navigation panel.

**Rationale**: Smooth navigation ensures a positive user experience and improves overall usability.

**Fit Criterion**: Users should be able to switch between features with one click from the side navigation menu without any delays or errors.

## 6.2 - Descriptive Explanations for Features

**Priority**: Medium

**Description**: The system should provide clear, descriptive explanations on each page to help users understand the purpose of each feature.

**Rationale**: Descriptive explanations help users with little knowledge of networking to understand what each feature does.

**Fit** **Criterion**: Each page should contain an explanation section that describes the purpose of the tool or feature being displayed.

## 6.3 - User-Friendly for Both Novice and Experienced Users

**Priority**: High

**Description**: The system should be user-friendly for both novice and experienced users.

**Rationale**: By catering to both novice and experienced users, the system can be widely used without being overly complex.

**Fit** **Criterion**: Novice users should be able to understand the basic functionalities without prior networking knowledge, while advanced users should still find valuable features.

# Performance

## 7.1 - Speed and Latency

**Priority**: High

**Description**: The system should perform tasks efficiently and provide results within a reasonable time frame.

**Rationale**: Slow performance can lead to frustration and inefficiencies, impacting the user experience.

**Fit** **Criterion**: The system must complete tasks within 6 minutes, even when pinging 246 IP addresses.

# Safety-Critical

## 8.1 - Non-Invasive Commands

**Priority**: High

**Description**: All commands executed by the tool should be non-invasive and not cause any harm to the system.

**Rationale**: The system must be safe to use, without risking damage to the target or causing security vulnerabilities.

**Fit** **Criterion**: The system must use harmless PowerShell commands (such as pings) to collect and display data.

# Reliability and Availability

## 9.1 - Available at Any Time

**Priority**: High

**Description**: The tool must be available for use at any time without requiring internet access.

**Rationale**: Users must be able to rely on the tool for continuous network monitoring, even without an active internet connection.

**Fit** **Criterion**: The tool should function completely offline and be accessible to users at all times.

## 9.2 - No Anticipated Downtime

**Priority**: High

**Description**: The system should not experience any downtime or require maintenance for normal functionality.

**Rationale**: Continuous availability is crucial for a tool that aids in real-time network monitoring.

**Fit** **Criterion**: The system should operate without interruption and not require any scheduled downtime or regular maintenance.

## 9.3 - No Regular Maintenance Required

**Priority**: Medium

**Description**: The system should be designed for low maintenance, requiring minimal updates or intervention from the user.

**Rationale**: This ensures the tool remains functional and easy to use over time without frequent updates.

**Fit** **Criterion**: The system should operate correctly without requiring regular patches, updates, or user intervention.

# Robustness or Fault-Tolerance

## 10.1 - Back-End Error Handling

**Priority**: High

**Description**: The system should implement robust back-end error handling to prevent system failures and ensure smooth operation.

**Rationale**: Effective error handling ensures the system continues to function even in the case of unexpected issues, improving reliability.

**Fit** **Criterion**: The system must gracefully handle backend errors, displaying appropriate error messages or fallback behaviors without crashing.

## 10.2 - Front-End Specific Error Prompts

**Priority**: High

**Description**: The front-end should provide specific error prompts, such as “No device found,” when issues are detected.

**Rationale**: Clear and specific error prompts help users understand what went wrong and how to fix it, improving user experience.

**Fit Criterion**: The system should display error messages on the front-end when no devices are found or any other similar issues occur.

# Scalability or Extensibility

## 12.1 - Single User Support

**Priority**: High

**Description**: The system should support only one user at a time for access and interaction with the features.

**Rationale**: As the tool is designed for individual use, supporting one user at a time simplifies development and reduces potential conflicts.

**Fit** **Criterion**: The system should only allow one active user session at a time.

## 12.2 - Expandable for Future Scripts

**Priority**: High

**Description**: The system should be highly expandable, allowing for new PowerShell scripts to be added in the future without significant changes to the architecture.

**Rationale**: As network needs evolve, new scripts and features must be easily added to improve the tool’s functionality.

**Fit Criterion**: The system should be able to integrate new scripts without requiring a major overhaul, with new features appearing seamlessly in the dashboard.

# Longevity

## 13.1 - Improvement of Visual Representations

**Priority**: Medium

**Description**: The system should allow for improvements in visual representations, such as graphs or charts, for better clarity and insight.

**Rationale**: Improved visual representations will help users better understand network data, making it more actionable.

**Fit Criterion**: The system should provide an option to update when available and enhance graphs and charts with more detailed or clearer visual elements.

# Maintainability and Support

## 14.1 - Low Maintenance Requirements

**Priority**: High

**Description**: The system should be designed to minimize the need for ongoing maintenance, requiring only occasional updates.

**Rationale**: A low-maintenance tool reduces long-term costs and ensures it remains operational for extended periods without needing frequent intervention.

**Fit Criterion**: The system should be functional for at least one year without requiring significant changes or maintenance efforts.

## 14.2 - User Support Documentation

**Priority**: Medium

**Description**: The system should provide support documentation that helps users understand how to use the tool and troubleshoot issues.

**Rationale**: Proper documentation improves usability and ensures users can resolve issues on their own without external help.

**Fit Criterion**: The system should include user guides, FAQs, and troubleshooting tips within the application or on an accessible online platform.

# Security

## 15.1 - Harmless PowerShell Scripts

**Priority**: High

**Description**: The system should use only harmless PowerShell scripts (e.g., simple pings) that do not compromise the system or network security.

**Rationale**: Using safe and harmless scripts ensures that the tool is non-invasive and does not introduce security risks.

**Fit Criterion**: All scripts used by the system should be verified as safe and non-invasive (such as pinging or system status checks).

# Audit

## 16.1 - Command History Tracking

**Priority**: Medium

**Description**: The system should maintain a log of all commands executed during the session.

**Rationale**: Command history helps track user actions, identify potential misuse, and allow for auditing purposes.

**Fit Criterion**: The system should record and display a list of all executed commands during the session in an accessible log.

# Privacy

## 17.1 - No Sensitive Data Collected

**Priority**: High

**Description**: The system should not collect or store any sensitive data, ensuring user privacy is maintained.

**Rationale**: To prevent any data leakage or misuse of personal or sensitive information.

**Fit** **Criterion**: The tool must not collect any personally identifiable information or sensitive data during its operation.