

Home Network Vulnerability Assessment Tool

Nicholas Scafidi

Mercer University

INFM480: Capstone Project for Information Technology and Informatics

Feng Liu Ph.D.

December 15, 2024

Executive Summary

The Home Network Vulnerability Assessment Tool is a comprehensive application designed to bridge the gap between technical complexity and user accessibility in home network security. This project addresses a critical need in modern society, where remote work, smart home devices, and the increasing risks of cyber threats make secure home networks essential.

The tool empowers non-technical users to identify and mitigate vulnerabilities within their home networks through features such as port scanning and closure guidance, password strength assessment, and step-by-step instructions for setting up secure guest networks for IoT devices. A user-centered design methodology was employed throughout the development process to ensure ease of use and effectiveness.

The report outlines the following key aspects:

- **Development Process:** The project followed a structured timeline, balancing research, design, development, and iterative testing phases. Agile practices allowed for flexibility and rapid response to usability testing feedback.
- **System Design:** Core components include a user-friendly interface, a robust vulnerability detection system, and educational resources to build user awareness of cybersecurity best practices.
- **Usability Testing:** Testing revealed critical areas for improvement, such as interface navigation and instructions clarity. Observations were used to refine the tool, resulting in a more intuitive and efficient user experience.
- **Technical Outcomes:** A functional prototype (Version 1.0) was developed and enhanced based on user feedback, with plans for further refinements in Version 2.0. The tool successfully identified and provided solutions for common security vulnerabilities in home networks.

By equipping users with actionable insights and practical tools, the Home Network Vulnerability Assessment Tool enhances digital safety and productivity. It addresses not only individual security needs but also contributes to a broader culture of cybersecurity awareness and resilience within the community. This project demonstrates the transformative potential of accessible technology in addressing pressing cybersecurity challenges.

Acknowledgments

I would like to extend my sincere gratitude to all those who contributed to the successful completion of this capstone project, "Home Network Vulnerability Assessment Tool."

First and foremost, I am deeply grateful to my professor, Dr. Feng Liu, for their guidance, feedback, and support throughout this project. Your expertise and mentorship have been instrumental in shaping this work, and I truly appreciate the time and effort you dedicated to helping me achieve my goals.

Special thanks to the participants who generously shared their time and insights during the needs assessment and usability testing phases. Your feedback provided the foundation for creating a tool that truly addresses real-world challenges in home network security.

Finally, I am profoundly thankful to my family and friends for their constant encouragement and support. Your patience and belief in me have been a source of strength and motivation throughout this journey.

To everyone who contributed directly or indirectly to this project, your contributions have made a lasting impact, and I am sincerely grateful.

Thank you.

Background

In today's increasingly connected world, home networks have become a cornerstone of daily life, supporting work, education, entertainment, and communication. The proliferation of Internet of Things (IoT) devices, such as smart home systems, security cameras, and voice assistants, has created unprecedented opportunities for convenience and automation. However, these advancements come with significant cybersecurity risks, especially for individuals who lack the technical expertise to secure their networks.

Why This Project?

Cybersecurity has traditionally been a domain reserved for large enterprises, leaving individual users to fend for themselves with minimal guidance or resources. Reports indicate that home networks are becoming prime targets for cyberattacks, with threats such as unauthorized access,

data theft, and malware propagation becoming more common. Despite the availability of commercial tools, many home users struggle to understand or implement basic security measures.

This project, the Home Network Vulnerability Assessment Tool, was conceived to address this gap. By providing an easy-to-use application tailored for non-technical users, the tool empowers individuals to evaluate and enhance the security of their home networks. It aims to bridge the gap between technical complexity and user accessibility.

Problem It Is Solving

The primary problem this project addresses is the lack of accessible tools and guidance for home network security. Traditional security tools often cater to IT professionals, leaving everyday users overwhelmed and their networks vulnerable. Key issues include:

Lack of knowledge about basic security measures like changing default passwords, updating firmware, or segregating IoT devices.

Difficulty in identifying open ports or weak network configurations.

Absence of step-by-step instructions to mitigate vulnerabilities.

The project solves these problems by offering:

A user-friendly interface that walks users through a vulnerability assessment process.

Actionable recommendations for securing their network.

Educational resources to build cybersecurity awareness.

Social Impact

The potential social impact of this project is significant:

Improved Cybersecurity Awareness: By educating users, the tool fosters a culture of cybersecurity consciousness at the grassroots level.

Reduction in Cybercrime: Secure home networks act as a barrier against unauthorized access, protecting sensitive personal data.

Enhanced Productivity: With a secure and reliable network, remote workers and students can focus on their tasks without worrying about disruptions caused by cyberattacks.

Community Resilience: As more individuals adopt secure practices, collective digital resilience improves, making entire communities less susceptible to cyberthreats.

In conclusion, the Home Network Vulnerability Assessment Tool addresses a pressing need in modern society. By enabling users to take charge of their home network security, the project has the potential to safeguard personal data, improve productivity, and contribute to a more secure digital ecosystem.

Project Planning and Management

Project Timeline:

Week 1: Research and Planning

- Day 1-2 (2 hours/day): Conduct a focused literature review on home network vulnerabilities (4 hours total).
- Day 3 (2 hours): Develop the user survey.
- Day 4-5 (2 hours/day): Get feedback on survey questions and prepare to revise surveys as needed.

Week 2: Survey Revisions and Initial Scenario Development

- Day 1-2 (2 hours/day): Finalize the revised survey questions based on recent insights and prepare for distribution (4 hours total).
- Day 3 (2 hours): Revise timeline to reflect current tasks and outcomes (2 hours total).
- Day 3-4 (3 hours/day): Draft initial scenarios for tool usage (6 hours total).

Week 3: Tool and Checklist Development

- Day 1 (2 hours): Begin Survey distribution and analyze results as they come in. Revise timeline to reflect current tasks (2 hours total).
- Day 2-3 (4 hours/day): Begin developing the vulnerability assessment tool (8 hours total).
- Day 4-5 (3 hours/day): Design and draft the checklist for manual assessments (6 hours total).

Week 4: Tool Refinement and Finalization

- Day 1-3 (4 hours/day): Continue developing the tool, incorporating any refinements based on the checklist (12 hours total).
- Day 4-5 (3 hours/day): Conduct internal tests on the tool and checklist, preparing them for validation (6 hours total).

Week 5: Testing and Validation

- Day 1-2 (3 hours/day): Begin vulnerability assessments on sample home networks using the tool (6 hours total).
- Day 3-5 (4 hours/day): Collect feedback and refine the tool and checklist based on testing results (12 hours total).

Week 6: Feedback Analysis and Tool Refinement

- Day 1-3 (3 hours/day): Continue feedback analysis, finalizing tool functionality and user interface (9 hours total).

- Day 4-5 (2 hours/day): Final refinement of the checklist (4 hours total).

Week 7: Finalization and Documentation

- Day 1-2 (3 hours/day): Finalize the tool, ensuring functionality across different network setups (6 hours total).
- Day 3-5 (4 hours/day): Write the project report, including methodology, tool development, and testing results (12 hours total).

Week 8: Submission and Presentation

- Day 1-3 (2 hours/day): Prepare the final user guide for the tool and checklist (6 hours total).
- Day 4-5 (3 hours/day): Review and submit the final report (6 hours total).

Total Estimated Time:

- Research and planning: 22 hours
- Tool and checklist development: 36 hours
- Testing and validation: 18 hours
- Finalization and documentation: 24 hours
- Submission and presentation: 12 hours

Explanation:

Some delays occurred in usability testing due to participant availability. To mitigate this, additional sessions were conducted during Week 7, and the timeline was adjusted to ensure at least some feedback was gathered for the beginning development of Version 2.0. The overall project timeline was monitored, with some backup plans implemented to address unexpected challenges. The main hurdle to overcome was the learning curve of using python and constructing the GUI using tkinter. Due to powers beyond control not all assets for the tool were implemented in the seven week time frame since another course did take up a significant amount of time. Only one participant feedback was acquired for usability testing see usability section for details.

Project Scope :

The Home Network Vulnerability Assessment Tool includes the following features:

- Port Scanning and Closure Guidance: Scans for open ports and provides step-by-step instructions for securing them.
- Password Strength Assessment and Recommendations: Evaluates existing passwords and offers tips for creating stronger alternatives.
- Guest Network Setup for IoT Devices: Guides users in setting up separate networks for IoT devices to enhance overall security.

The scope also includes creating a user-friendly interface and integrating educational content to raise awareness about common cybersecurity threats.

Project Deliverables Definition:

- Functional Prototype Version 1.0: A basic working model with core features for usability testing.
- Functional Prototype Version 2.0: An enhanced version incorporating user feedback and additional features.
- Final Report: A comprehensive document outlining the project's development, design, testing, and outcomes.
- User Help Document: A guide for users to navigate and utilize the tool effectively.
- Presentation: A detailed PowerPoint summarizing the project and its results.

Success Measurements:

Success was defined through the following metrics:

1. Task Completion: 90% of usability test participants successfully complete predefined tasks without assistance.
2. User Feedback: Positive feedback on clarity, functionality, and ease of use.
3. Effectiveness: The tool identifies at least three critical vulnerabilities in test networks, providing clear instructions for resolution.

Project Management:

Project management was executed using the following strategies:

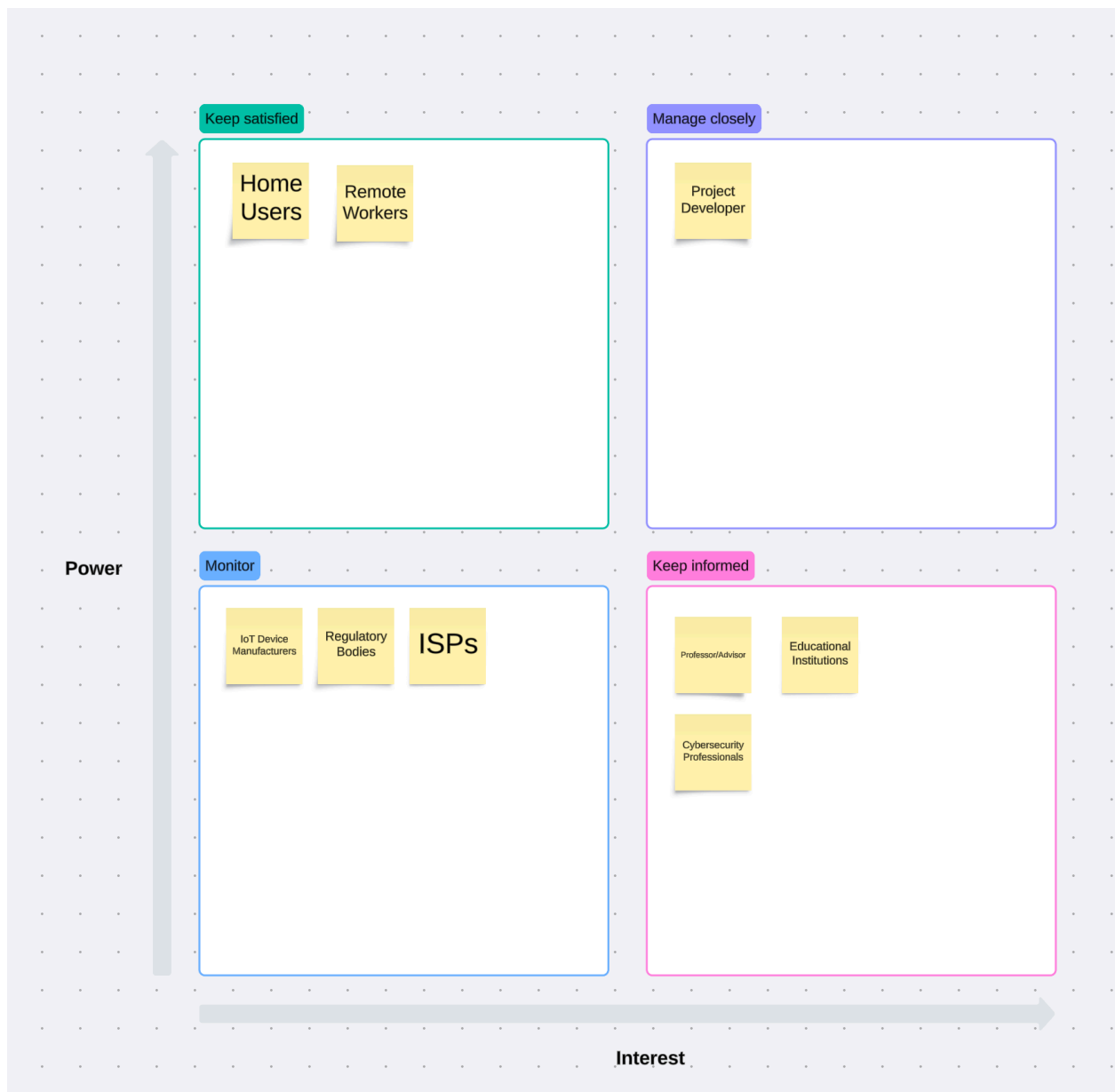
- Task Breakdown: Clear milestones and weekly goals were defined at the outset.
- Communication: Regular updates and meetings ensured alignment with the professor, participants and stakeholders.
- Agile Development: Iterative feedback cycles were used to refine the tool based on usability testing outcomes.
- Risk Mitigation: Potential risks, such as participant unavailability and technical issues, were identified, and backup plans were put in place.

Not all deadlines were met, but professional communication was maintained throughout the project. Weekly progress reports and prompt responses to instructor feedback contributed to the successful execution of the project.

System Design

Stakeholders Map:

Stakeholder Map outline



1. Primary Stakeholders

Home Users:

Description: Non-technical individuals who own and manage home networks, including families, students, and IoT enthusiasts.

Influence: Their needs and preferences directly shape the tool's features and user interface. The success of the project depends on its ability to address their pain points and provide a seamless user experience.

Remote Workers:

Description: Professionals who rely on home networks for their work, especially those in industries requiring secure access to sensitive corporate data.

Influence: As frequent users of home networks for work-related tasks, their feedback ensures that the tool addresses vulnerabilities that could compromise professional activities or sensitive data. Their adoption of the tool is vital to preventing breaches that could impact both personal and corporate security.

2. Secondary Stakeholders

Cybersecurity Professionals:

Description: Experts in network security who may use the tool to provide services or training for home users.

Influence: Their feedback and best practices inform the technical design, ensuring the tool adheres to cybersecurity standards.

Internet Service Providers (ISPs):

Description: Companies that provide internet connectivity to home users.

Influence: ISPs could endorse or promote the tool to enhance customer satisfaction by addressing network security issues.

3. Tertiary Stakeholders

Educational Institutions:

Description: Schools, universities, or organizations providing cybersecurity education and awareness programs.

Influence: They may integrate the tool into training curricula, helping to raise awareness about home network vulnerabilities.

IoT Device Manufacturers:

Description: Companies producing smart devices commonly found in home networks.

Influence: Their cooperation could help ensure compatibility with the tool and encourage users to adopt secure practices for IoT device setup.

Regulatory Bodies:

Description: Government agencies or organizations focused on data privacy and cybersecurity regulations.

Influence: They set guidelines for cybersecurity best practices that inform the tool's recommendations and ensure legal compliance.

4. Development Team

Project Developer:

Description: The designer and developer of the tool.

Influence: Responsible for translating user needs into technical features, maintaining project scope, and ensuring timely delivery.

Professor/Advisor:

Description: Academic guide providing oversight and feedback on the project.

Influence: Offers critical insights and ensures the project aligns with educational and professional standards.

5. Indirect Stakeholders

Families of Users:

Description: Individuals who share home networks with primary users.

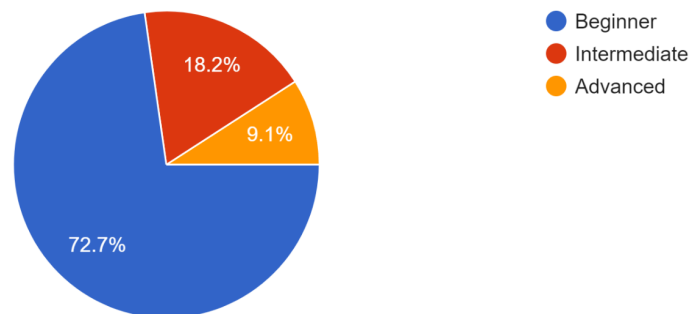
Influence: They benefit from enhanced network security, reducing the risk of breaches and protecting shared resources.

Needs Finding:

A survey was conducted to determine the user's knowledge of the cybersecurity climate and what home users do for their own home network security. The survey was also conducted to see if there is a need for simplified tools to address network vulnerabilities. The questions are included in the graph images.

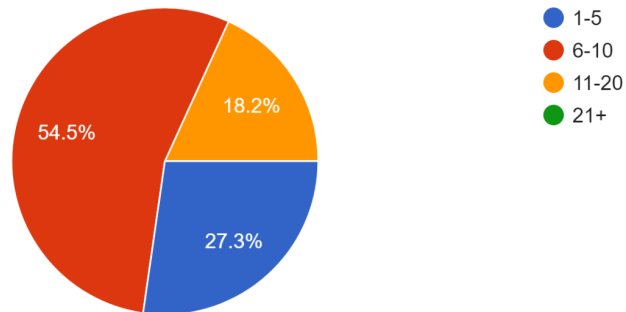
How would you rate your knowledge of home network security?

11 responses



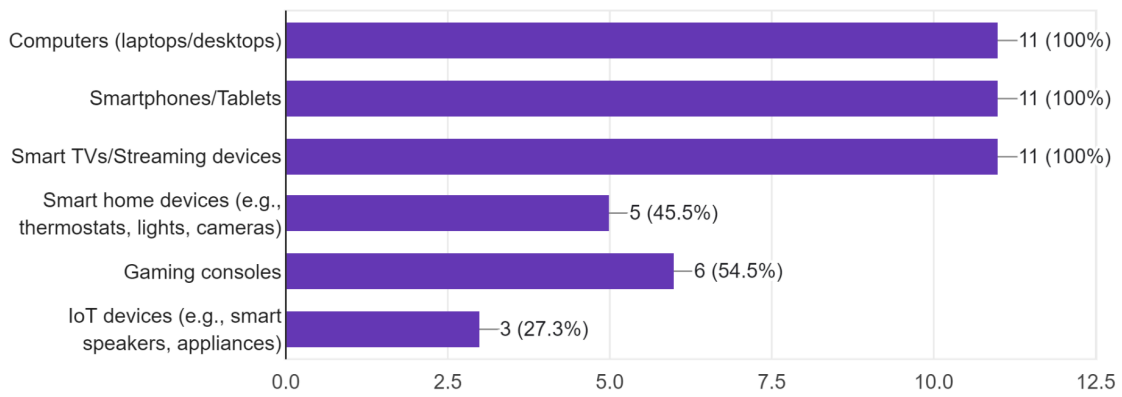
How many connected devices do you typically have on your home network?

11 responses



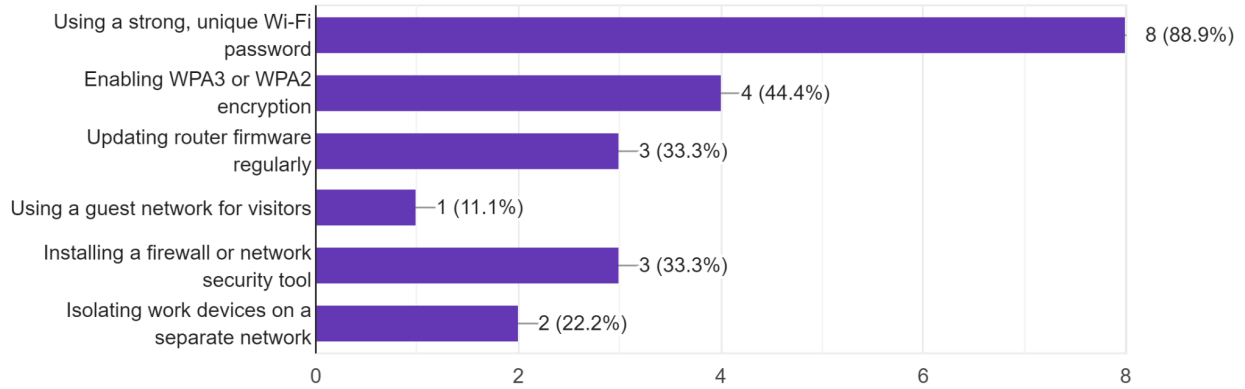
What types of devices do you have on your network? (Select all that apply)

11 responses



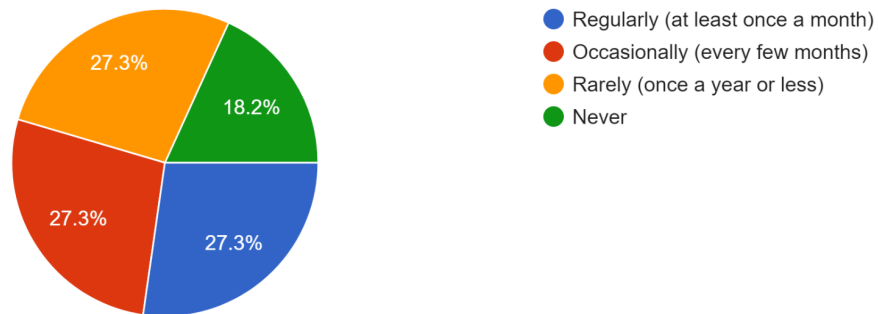
What steps do you currently take to secure your home network? (Select all that apply)

9 responses



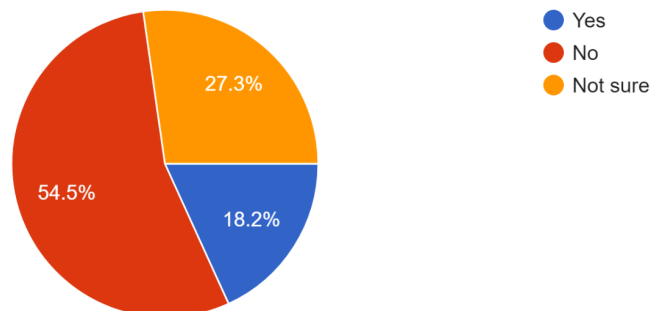
How often do you update the firmware or software of your devices?

11 responses



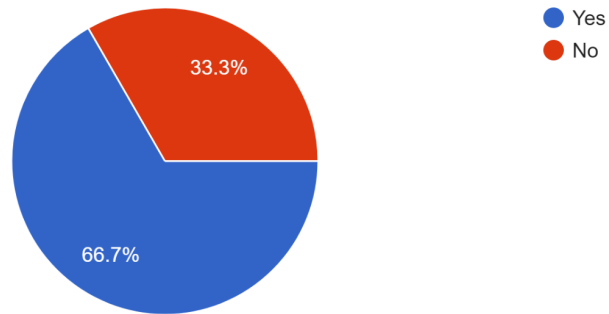
Do you have a dedicated firewall or security appliance in your home network?

11 responses



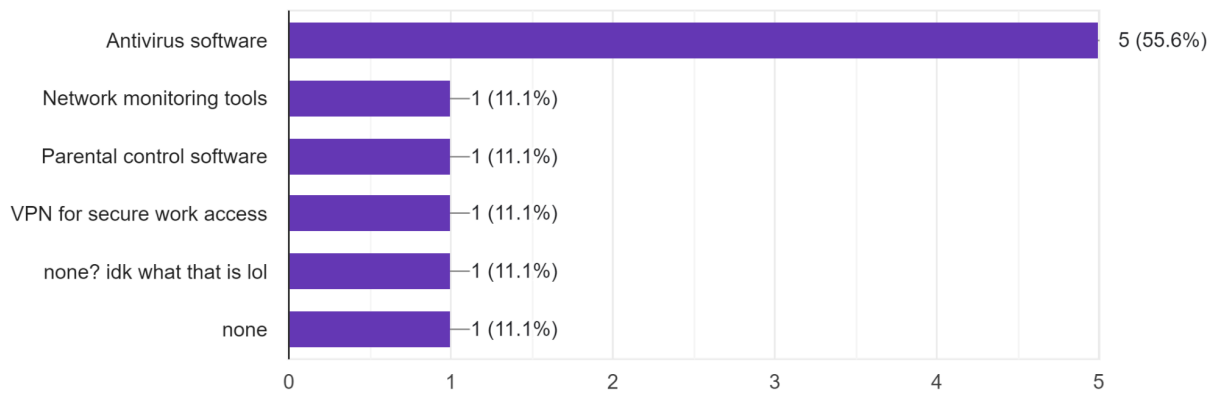
Do you use any security tools or software specifically for your home network?

9 responses



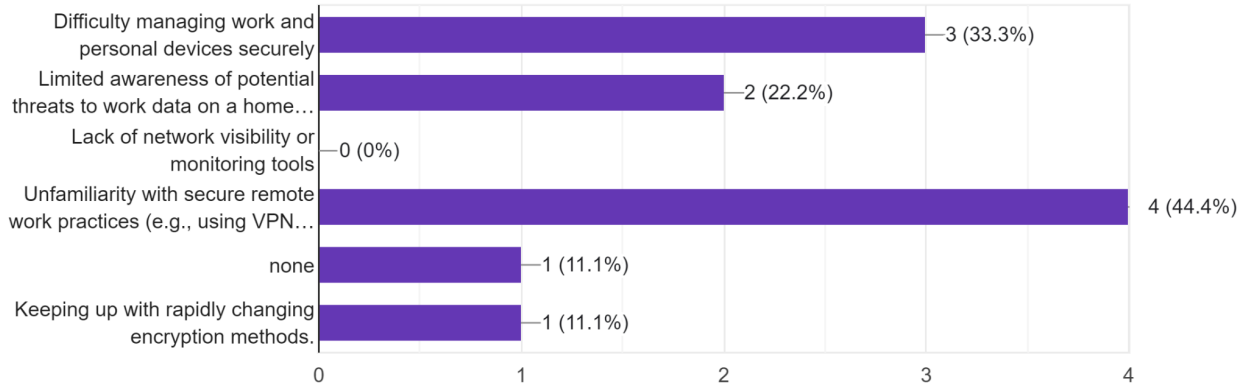
If yes, which security tools do you use? (Select all that apply)

9 responses



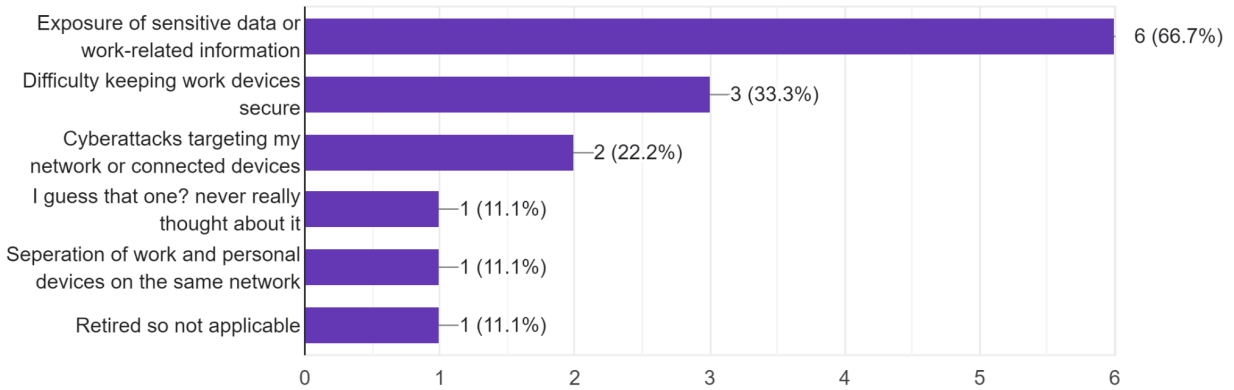
What challenges do you experience with remote work security on your home network? (Select all that apply)

9 responses



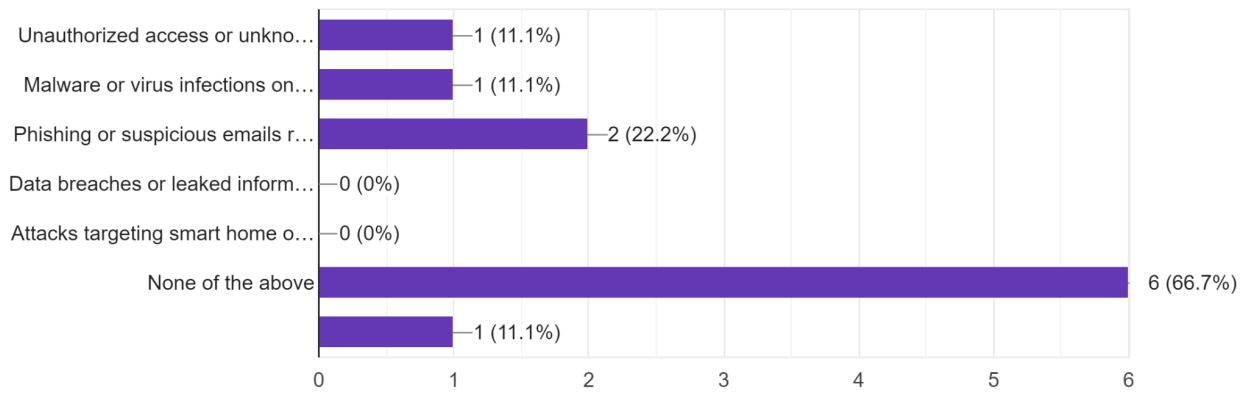
What concerns you most about using your home network for work-related activities?

9 responses



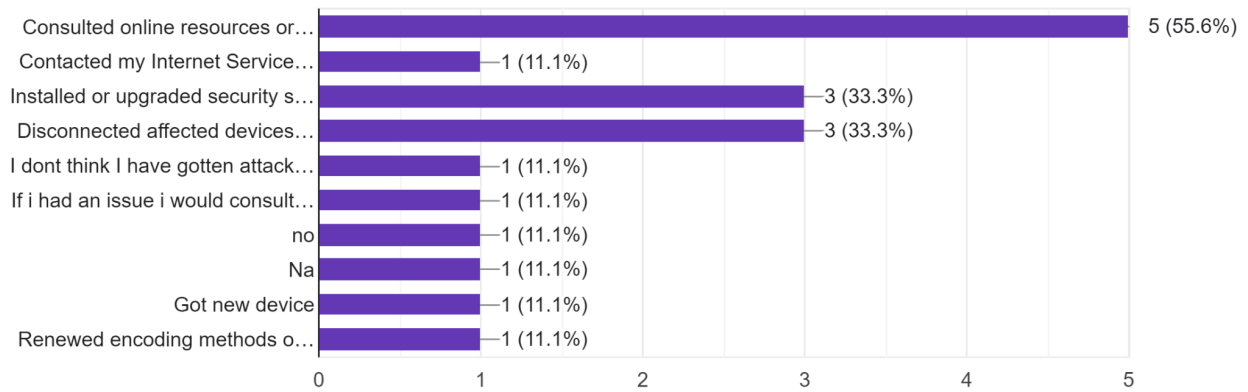
Have you experienced any security incidents on your home network? (Select all that apply)

9 responses



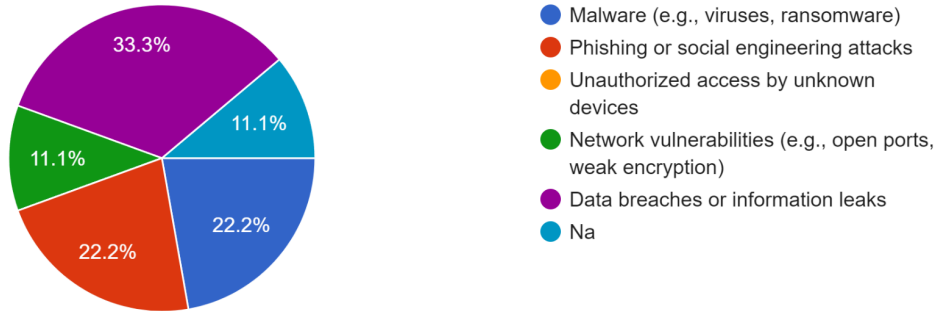
If you experienced a security incident, what actions did you take to address it?

9 responses



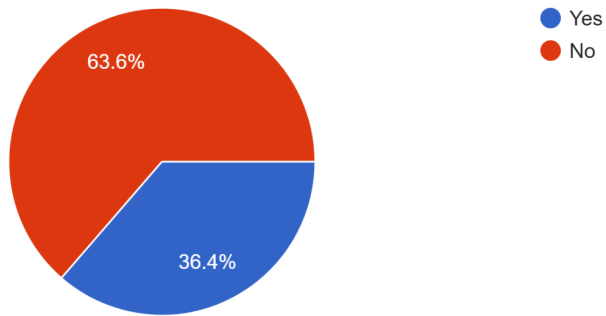
What types of threats do you believe pose the most risk to your home network?

9 responses



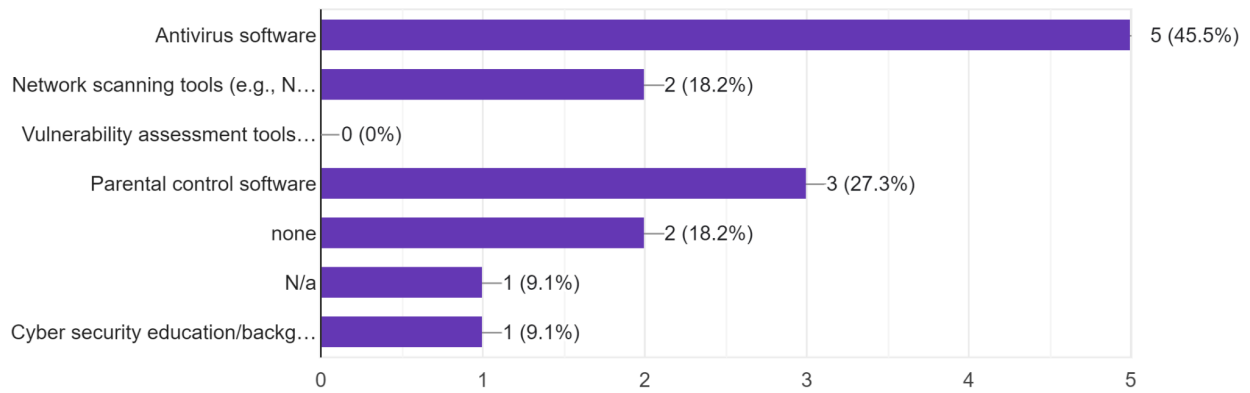
Have you ever used a network security tool to assess your home network?

11 responses



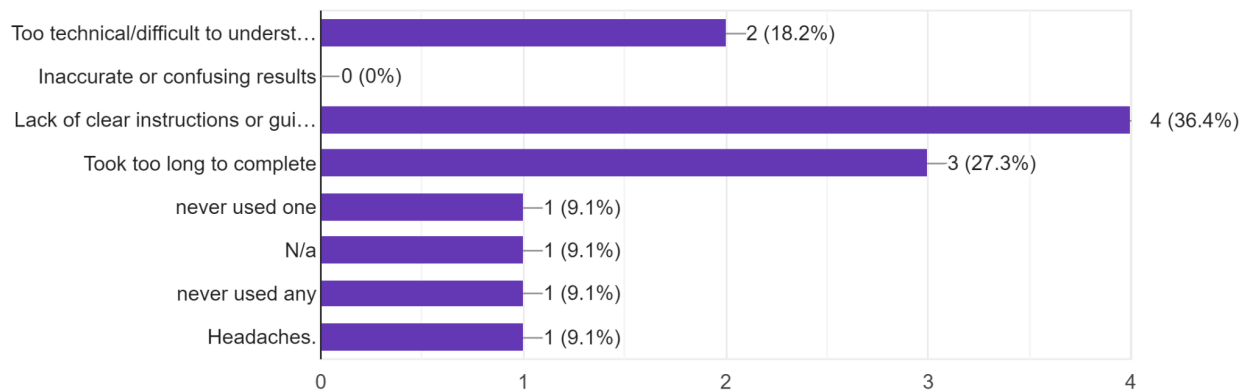
If yes, what tools have you used? (Select all that apply)

11 responses

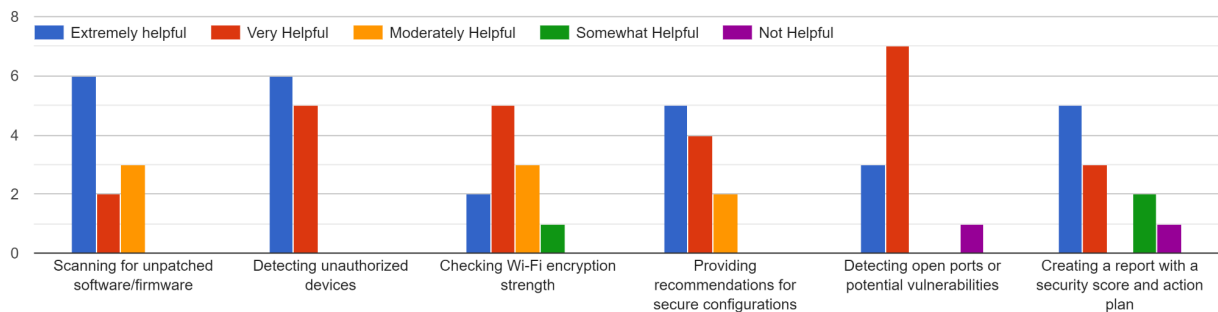


What challenges did you face when using these tools?

11 responses

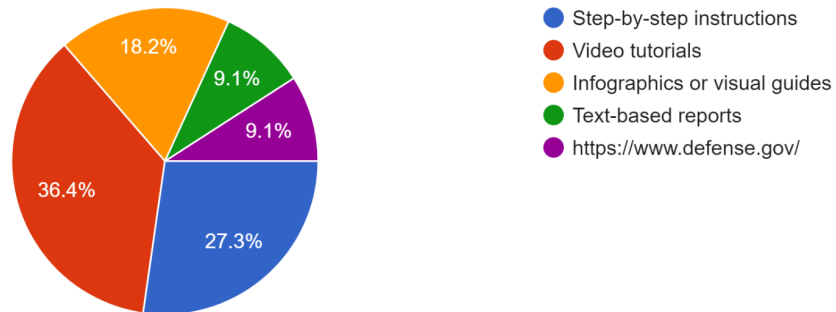


What features would you find most helpful in a home network security assessment tool? Please rate each feature according to the scale.



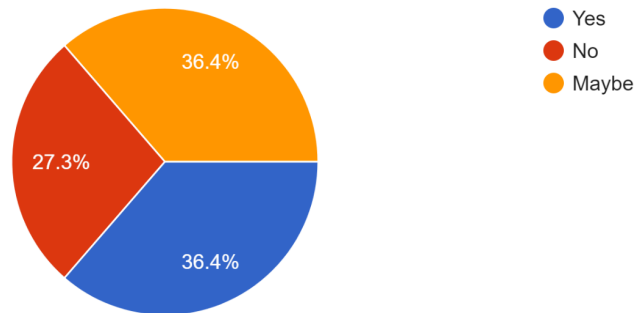
How would you prefer to receive recommendations for improving your network security?

11 responses



Would you be interested in ongoing monitoring or alerts for your home network security?

11 responses



Section 5: General Feedback

What other features or functionalities would you like to see in a home network security tool?

6 responses

honestly not too sure

something that explains things clearly to a person that doesn't know a lot about these kind of things (ie. me)

After problems are identified there should be a plan along with it to help customers mitigate those hazards.

Nothing

Plug and play installation

Better signal encryption methods.

Are there any specific concerns you have about the security of your home network?

8 responses

im always worried about social engineering attacks but thats something no ammout of security can fix

nah

Not especially

Not at this time

Unauthorized. Access of information on the device. Download of inappropriate content.

Network vulnerabilities from weak or incompatible hardware

General educating material for the security issue at a public spot without secured network

Someone who decides to get bored and figures out how to bypass an encrypted VPN.

Any additional comments or suggestions?

4 responses

thank you

Hi

Good UI

Good luck on your project!

Scenarios:

Scenario 1: A Remote Worker Securing His Home Office Setup

Background: Mike, an IT professional, has transitioned to a fully remote position. His job involves handling sensitive client data and accessing his company's internal systems, making network security a priority.

Mike's Motivation:

Mike's company recently enforced strict cybersecurity policies for remote employees due to a recent uptick in phishing attacks and data breaches.

He needs to make sure his home network is secure to prevent unauthorized access and ensure compliance with his company's data protection requirements.

With limited time between work projects, Mike needs a straightforward, reliable tool to perform an assessment without needing deep technical knowledge.

Steps Mike Took Using the Tool:

Step 1: Mike downloads and opens the Home Network Vulnerability Assessment tool. The tool prompts him with an introductory tutorial on the assessment process, so he knows what to expect.

Step 2: The tool starts by checking the router's firmware version and configuration. It flags that his router still uses the default login credentials and recommends a change.

Step 3: Mike follows the prompt to create a strong, unique password and enable WPA3 encryption. The tool also suggests disabling WPS (Wi-Fi Protected Setup), which can be a vulnerability.

Step 4: The tool scans connected devices and identifies that his home printer, used for work documents, has outdated firmware. It recommends updating the firmware and setting a strong password on the printer.

Step 5: Finally, the tool checks for a firewall and prompts Mike to enable one on his router. It also suggests adding a software firewall on his primary work device to add an extra layer of security.

Predicted Outcome:

With the tool's guidance, Mike successfully secures his network, updating credentials and configurations without much hassle.

He submits a compliance report generated by the tool to his employer, demonstrating his adherence to the company's cybersecurity standards.

With these security measures in place, Mike feels more confident handling sensitive client data from home, knowing that his network is now more resilient against cyber threats.

Scenario2: A Tech Enthusiast Wanting to Optimize and Secure a Smart Home

Background: Alex, a tech enthusiast and early adopter of smart home technology, has set up her home with smart lighting, security cameras, voice assistants, and various IoT devices. Although she is savvy with tech, she is aware of the risks posed by poorly secured IoT devices.

Detailed Storyboard

Alex's Motivation:

Alex has read about IoT vulnerabilities, such as data breaches and malware targeting smart home devices. She wants to be proactive in protecting her privacy and avoiding network slowdowns caused by numerous devices sharing bandwidth.

She's also interested in optimizing her network to handle the demand from multiple smart devices without impacting performance.

Steps Alex Took Using the Tool:

Step 1: Alex launches the Home Network Vulnerability Assessment tool and starts a full scan of her network.

Step 2: The tool scans her router settings and identifies that her Wi-Fi network is unsegmented, meaning both personal and IoT devices are connected to the same network. It recommends setting up a guest network for IoT devices to keep them isolated from her personal devices.

Step 3: Alex follows the tool's advice to create a separate network exclusively for IoT devices, securing it with WPA3 encryption and a unique password.

Step 4: Next, the tool checks bandwidth utilization and suggests enabling Quality of Service (QoS) settings on her router. It recommends prioritizing certain devices, like her home computer and smart speakers, over less critical devices to prevent performance bottlenecks.

Step 5: The tool provides an IoT security checklist, prompting Alex to change default passwords on her devices, disable unnecessary services, and enable automatic updates on her smart devices.

Step 6: The tool also includes guidance on configuring her smart home hubs (such as voice assistants and smart lights) to limit data collection and set up local-only access where possible.

Predicted Outcome:

By following the tool's recommendations, Alex achieves both better security and performance on his network. Her IoT devices are now segmented, reducing the likelihood of lateral attacks on personal devices.

With QoS enabled, her primary devices receive prioritized bandwidth, leading to smoother streaming and faster internet speeds, even with heavy IoT usage.

She now feels confident that her smart home setup is more secure and optimized, and she continues to use the assessment tool regularly to stay updated on emerging vulnerabilities and best practices for IoT security.

Database Design or Key Tech Component:

- Vulnerabilities: Tracks identified issues and solutions.
- Python
- Nmap Python package
- Tkinter

Function/Feature Design and desired functions:

The tool enables:

- Real-time network scanning
- Step-by-step instructions for addressing vulnerabilities
- Interactive checklist for the user to follow along with instructions on how to address said problems
- Desired tool functions
 - Functions of the tool itself and deliverables alongside the tool
 - Tool: Scan network and show ssid and passwords
 - Tool: Scan for open ports
 - Tool: Give recommendations and steps on how remediate problems

- Steps on how to properly close ports
- Steps on how to change wifi passwords
- Steps on how to make a guest network
- Steps on how to manage passwords
- Steps on how to hide your ssid
- Provide a detailed checklist for the assessment i.e. what to look for, and why to do it, how to do it, when to do it, where to do it

User Task List:

User Task List for the Home Network Vulnerability Assessment Tool

(Not all features are available within the tool as of right now. These are the desired user tasks based on the survey results)

Getting Started

Install the Tool:

Download the software from a secure link.

Install the tool on a device (Windows).

Accept the terms of use and disclaimers.

Set Up the Tool:

Launch the tool.

Enter basic information about the home network (e.g., number of devices, type of router).

Navigating the Interface

Access Main Menu:

Understand the layout and tabs (e.g., "Scan Network," "Security Checklist," "Reports," "Help").

Learn how to navigate between sections using intuitive tabs/buttons.

Review Disclaimer:

Acknowledge the tool's purpose, limitations, and cautions against misuse.

Network Scanning and Analysis

Run a Network Scan:

Initiate a scan to detect connected devices and open ports.

View results with details on device names, IP addresses, and vulnerabilities.

Identify Vulnerabilities:

Highlight weak or default passwords.

Detecting unnecessary open ports.

Flag outdated firmware or software.

Using the Security Checklist

Complete the Checklist(separate from tool for right now):

Step through a predefined security checklist (e.g., changing default credentials, enabling firewalls).

Mark tasks as completed, skipped, or pending.

Access detailed guides for:

Closing unnecessary ports.

Changing router/admin passwords.

Setting up a guest network for IoT devices.

Custom Actions

Generate Reports:

Export reports for reference or share with technical support.

Access Help Resources:

View FAQs, troubleshooting steps, and video tutorials.

Contact support for advanced guidance.

Site Structure/Information Architecture:

Includes a site map detailing navigation between Home, Scan Results, Tutorials, and Settings pages.

Usability Study Methodology

Methodology:

The usability study was conducted with one participant who was asked to perform specific tasks using the Home Network Vulnerability Assessment Tool. The tasks included scanning their network, identifying vulnerabilities, and implementing one recommended fix. Feedback was collected through observation. Participants were selected based on varying levels of technical expertise to ensure the tool's accessibility to diverse users.

Observation:

One participant, a 51-year-old non-technical user, ran a wifi profile password strength check. Once the scan began, they saw all of their wifi profile passwords and the recommendations of either removing them from the computer or changing the password in the router settings. They found the instructions for addressing vulnerabilities very unclear and confusing. Their feedback

led to giving clear instructions on how to access the router and change the password, and how to find the wifi profiles in the Windows settings to remove them from their system.

Tasks Observed:

Running Wifi-profile password strengths.

Reviewing reports.

Showing recommended password changes

Following step-by-step instructions to change passwords on the router.

Following step-by-step instructions on how to remove wifi profiles from the computer.(observer involvement was included in this)

Adjustments Based on Observations:

Improved instructions for accessing unique router settings to change.

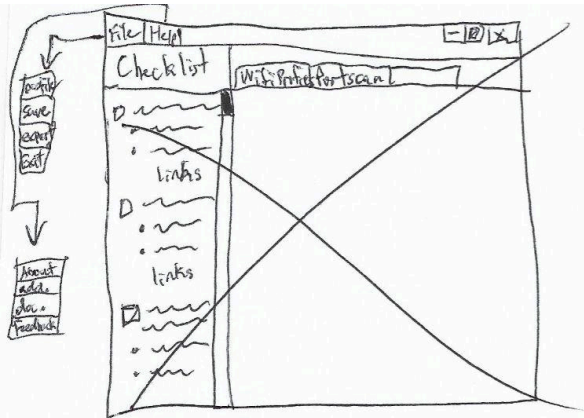
Added tooltips for first-time users to guide them through the process.

Technical Solution: Prototype Version 1.0

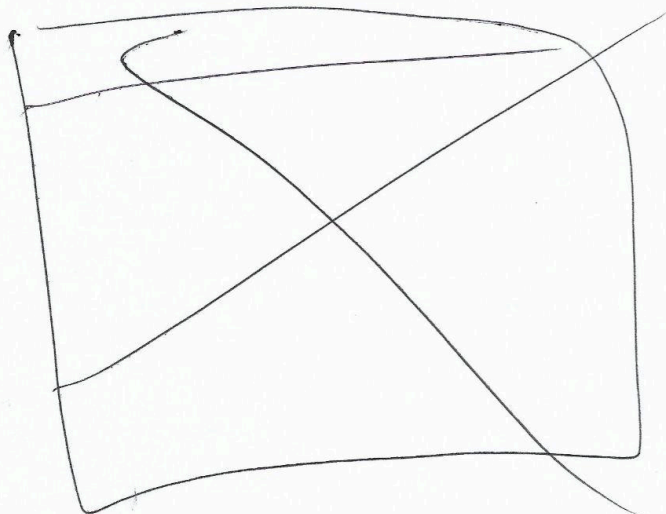
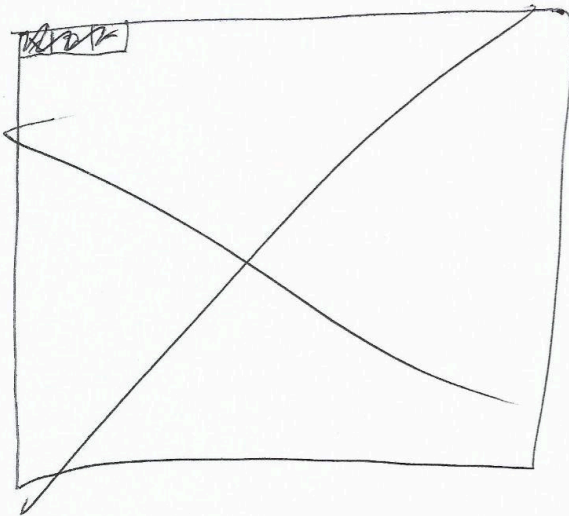
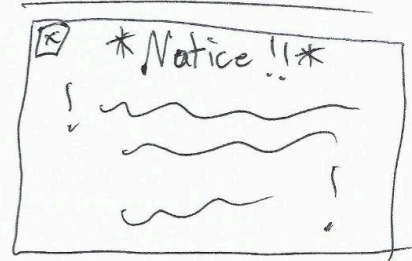
Initial Design: Paper sketches included basic navigation and core features.

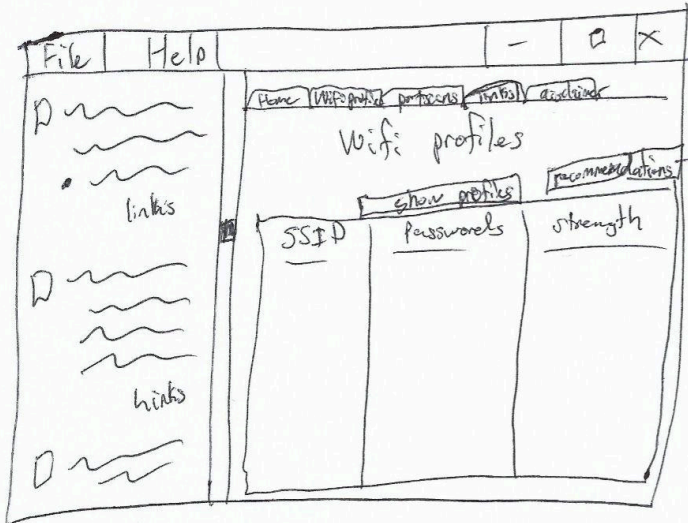
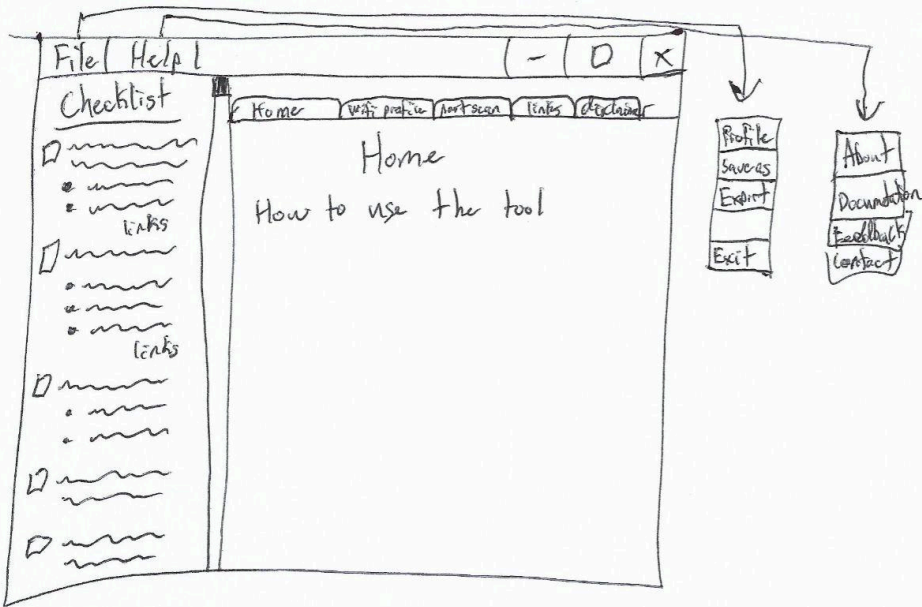
Digital Prototype: Developed using Python. Coding details are included on the Landing page through the github link for all testing pages and versions.

<https://github.com/Scafidi01/infm480capstone> – use checklistv1.py in an IDE, like pycharm, to access the latest version.

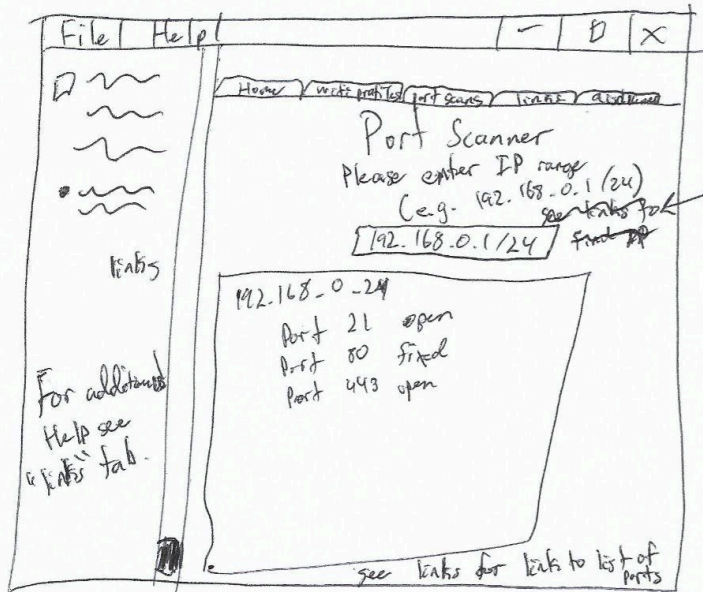


Initial disclaimer
pop-up on
Application start

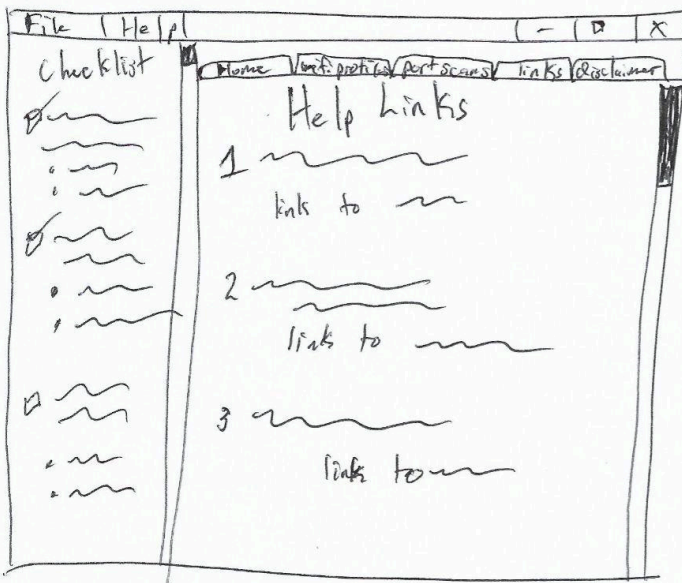


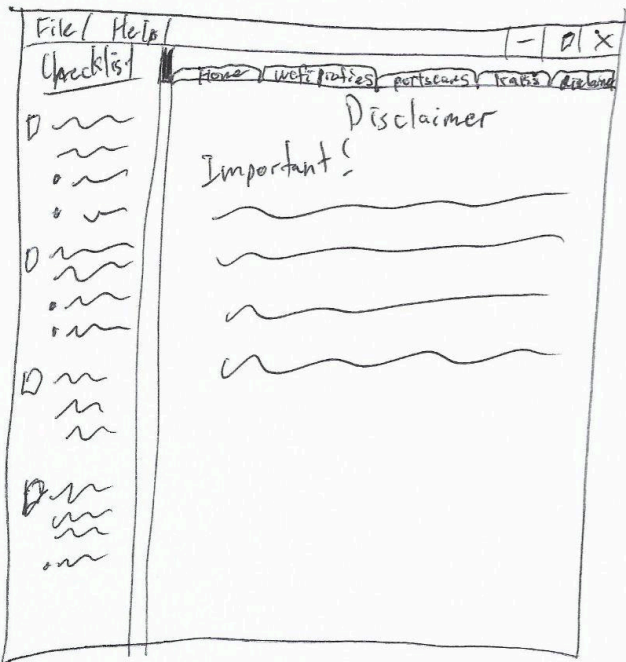


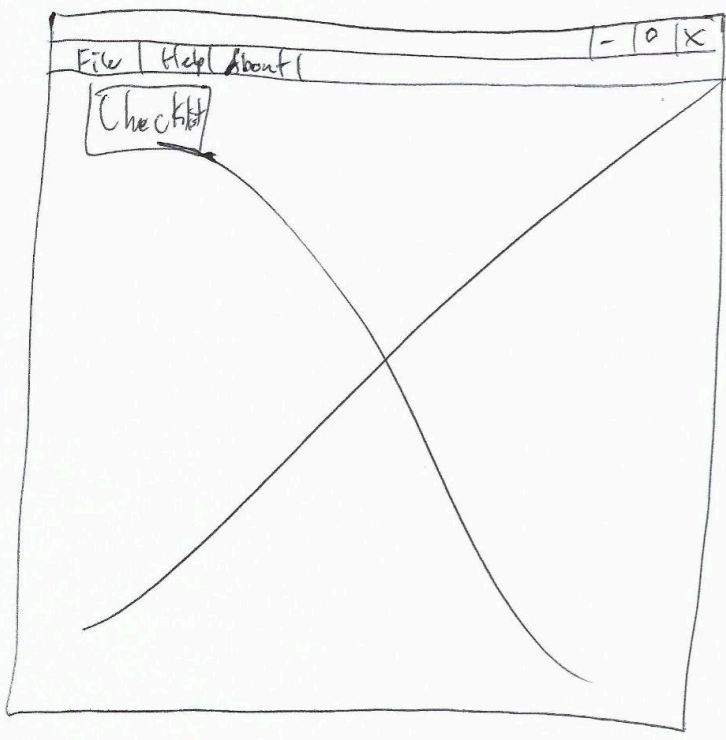
Recommendations*
 pop-up that advises
 on using on increasing
 the strength on
 password
 * the profile needs to
 be selected when
 trying to use this
 feature.



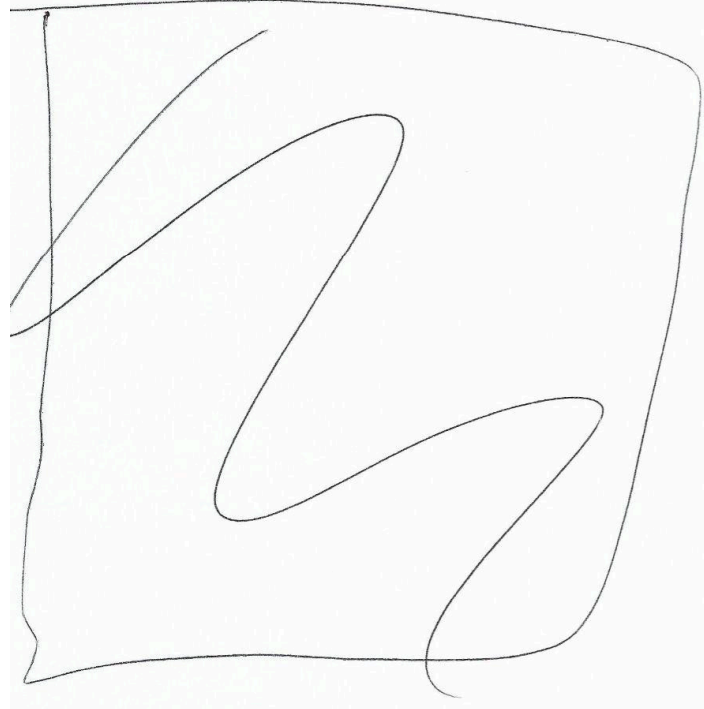
see links to documentation on how to find your IP address and what to enter.

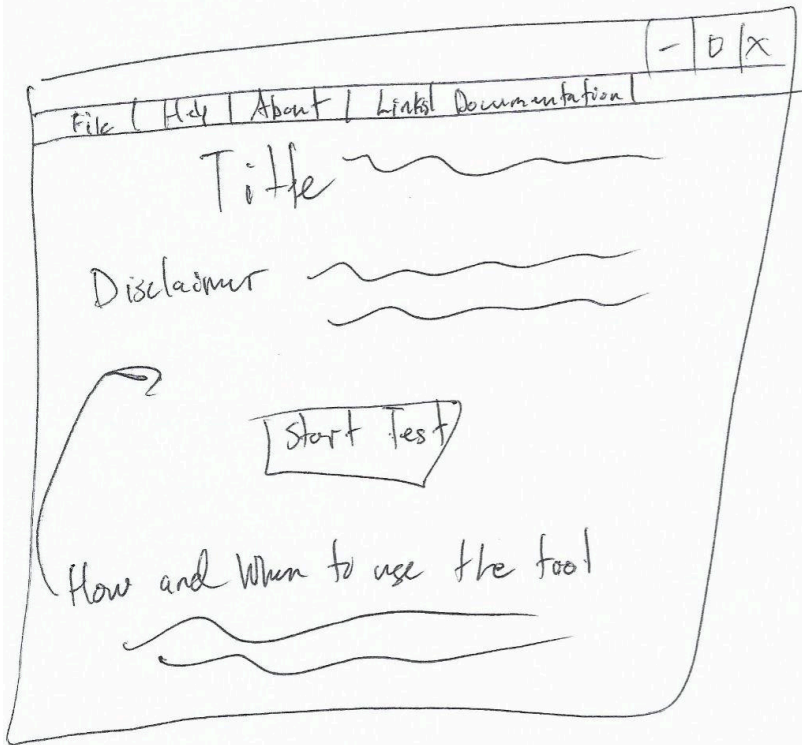
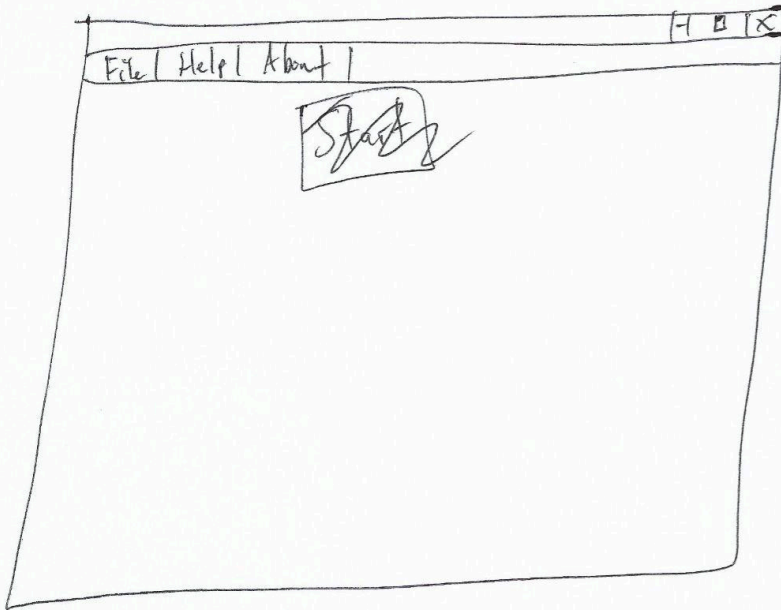




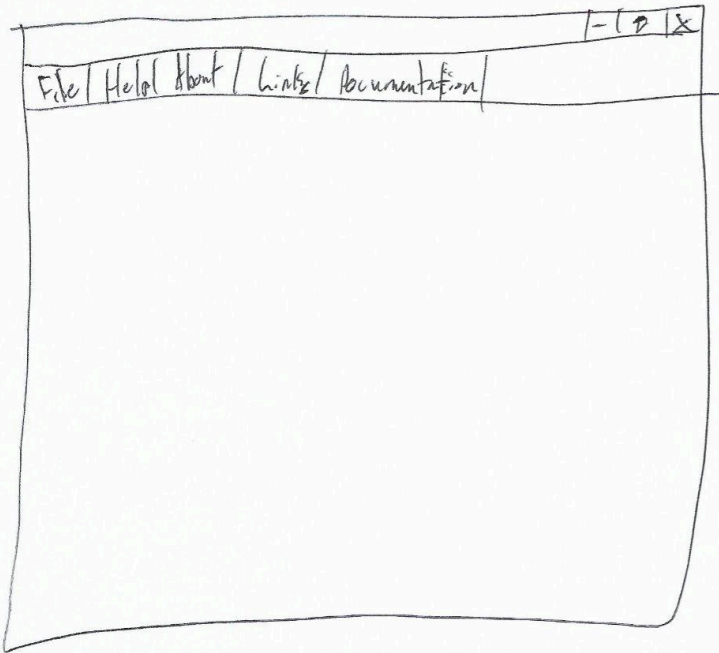


Version 2 ?



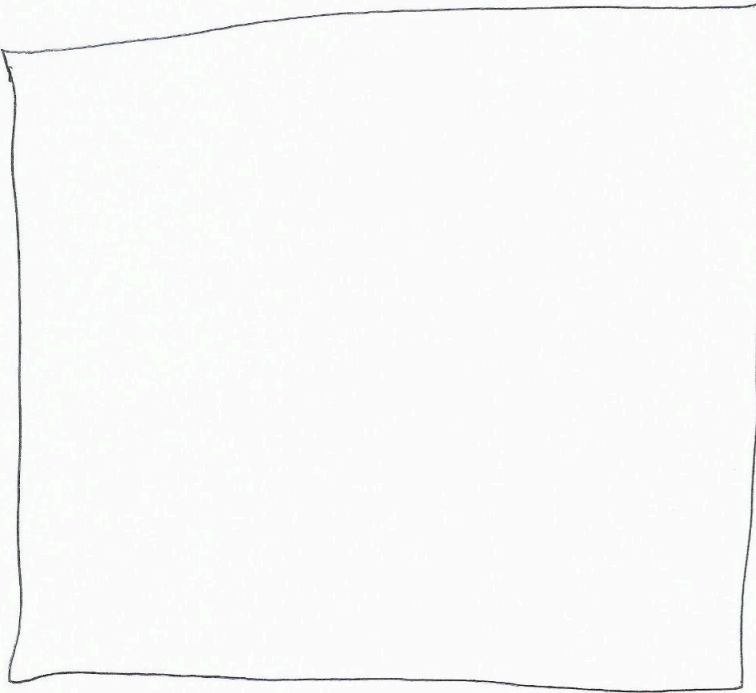


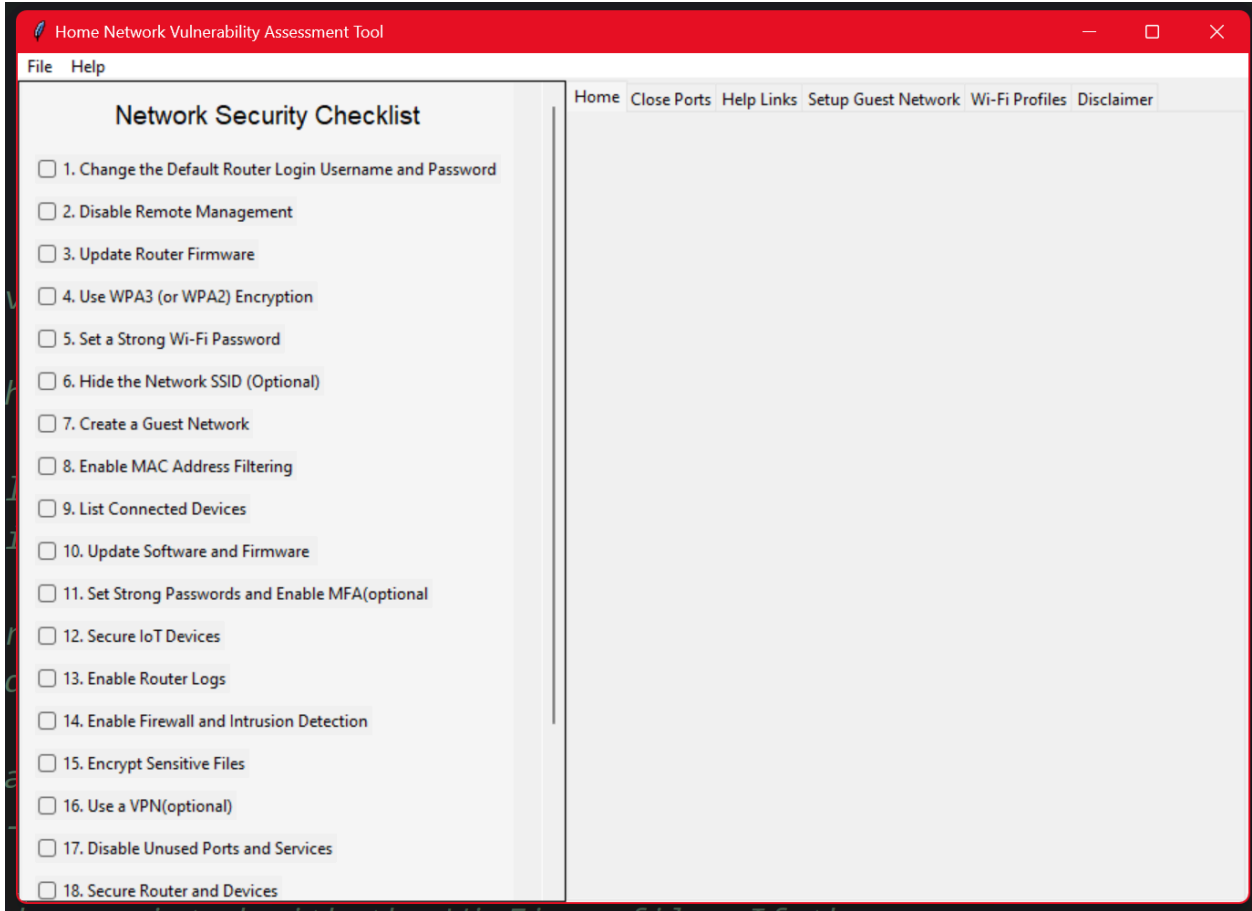
Other version
combining checklist
and application
making it
more interactive
and allowing the
user to do
the whole
checklist
and test
and save
their tests
and cross
reference
them with
past tests
on the
same network.

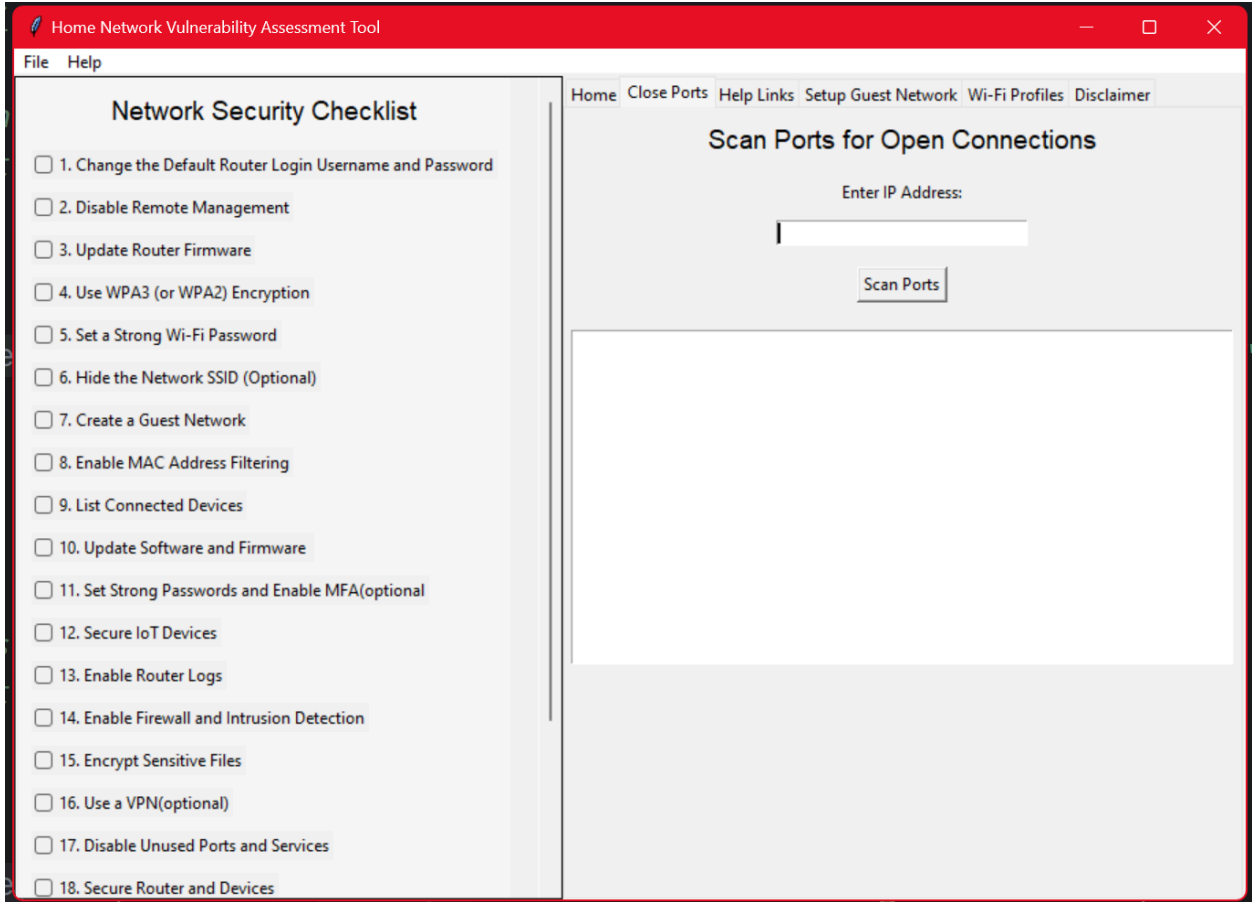


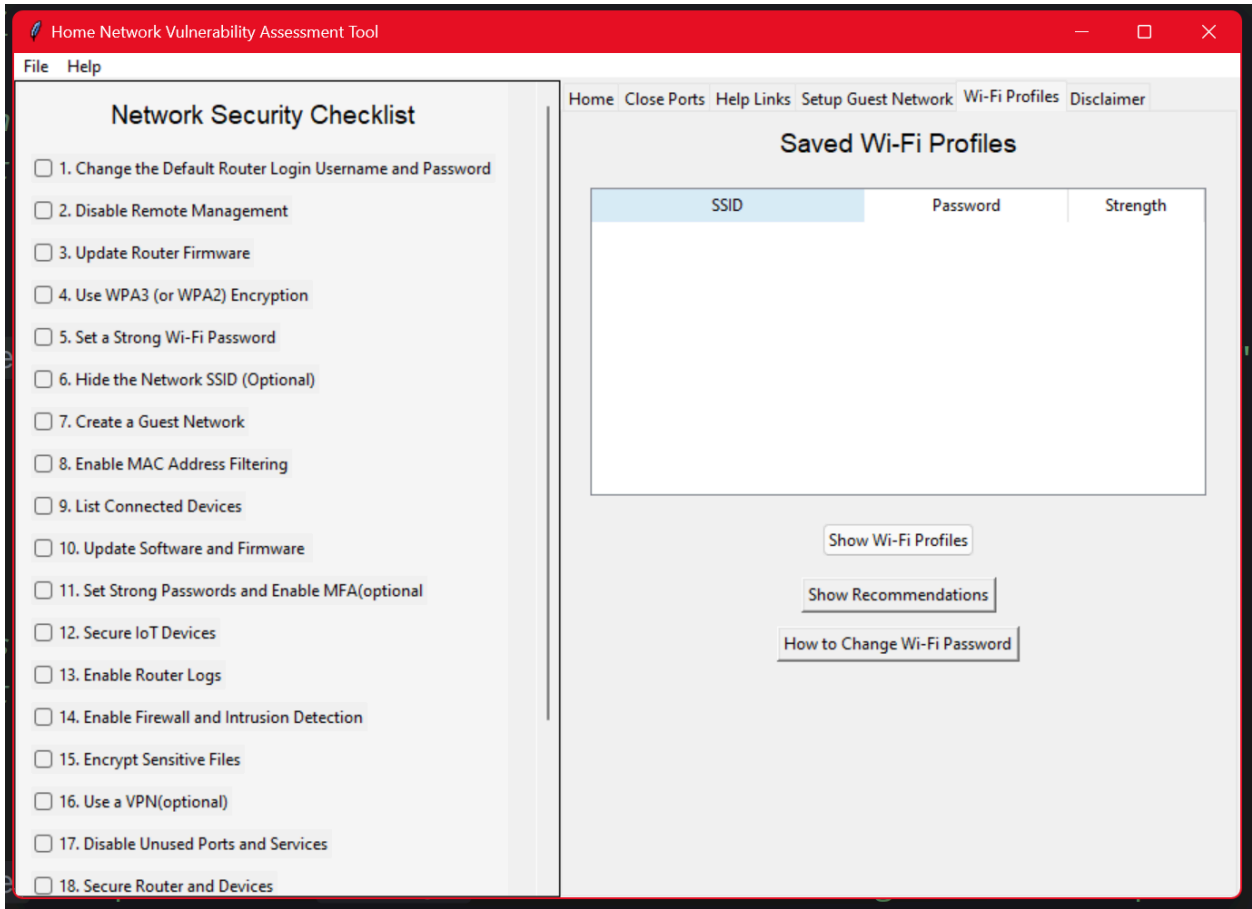
add password generator?

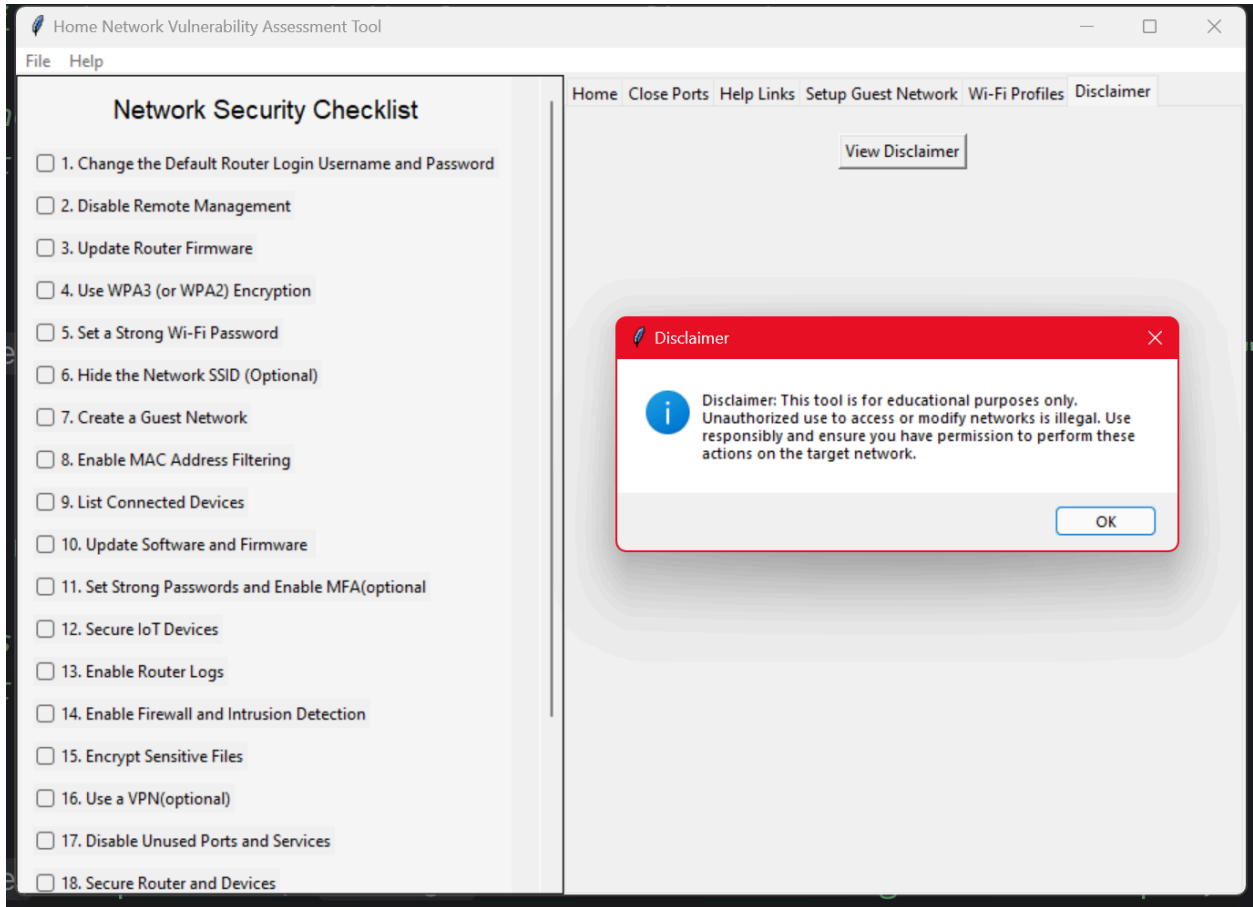
Make password images?

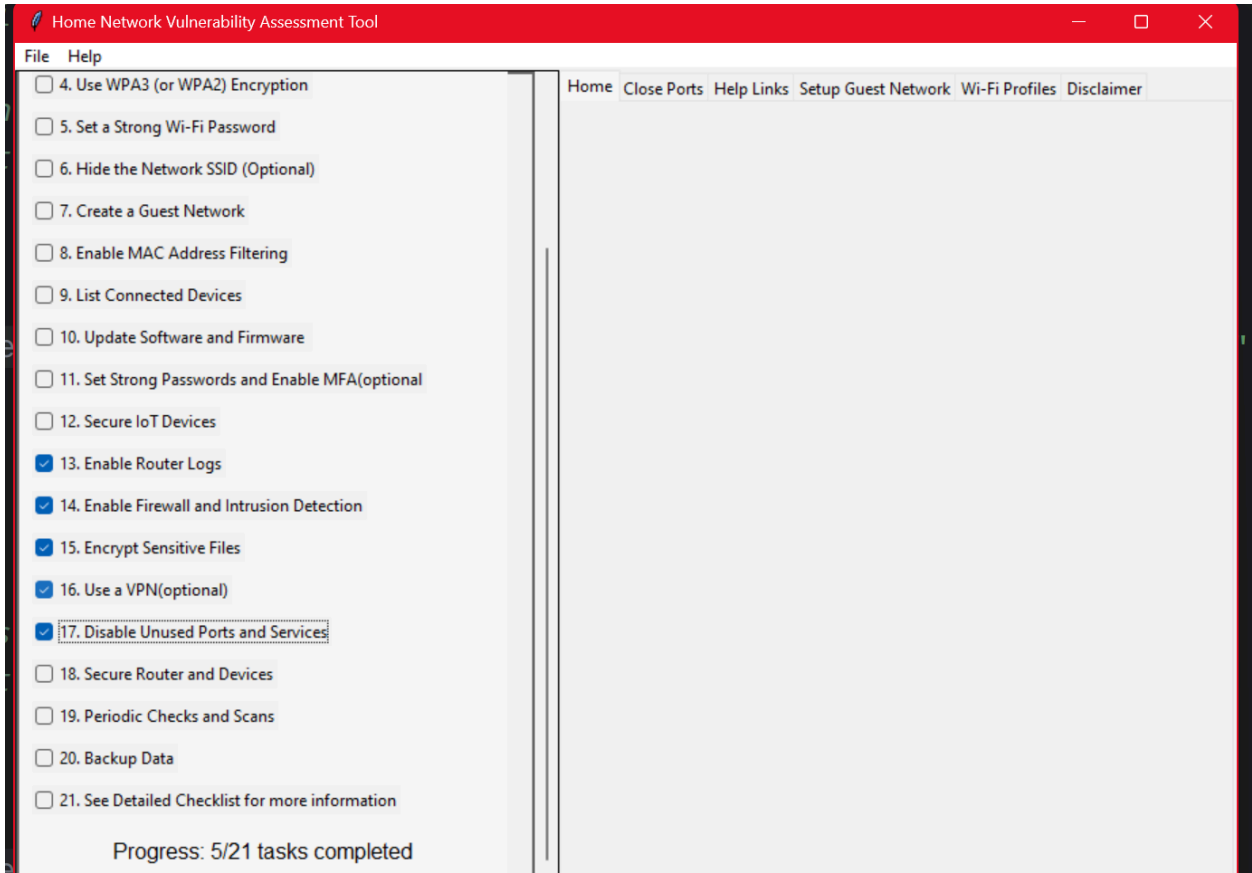












Home Network Vulnerability Assessment Tool

File Help

Network Security Checklist

- 1. Change the Default Router Login Username and Password
- 2. Disable Remote Management
- 3. Update Router Firmware
- 4. Use WPA3 (or WPA2) Encryption
- 5. Set a Strong Wi-Fi Password
- 6. Hide the Network SSID (Optional)
- 7. Create a Guest Network
- 8. Enable MAC Address Filtering
- 9. List Connected Devices
- 10. Update Software and Firmware
- 11. Set Strong Passwords and Enable MFA(optional)
- 12. Secure IoT Devices
- 13. Enable Router Logs
- 14. Enable Firewall and Intrusion Detection
- 15. Encrypt Sensitive Files
- 16. Use a VPN(optional)
- 17. Disable Unused Ports and Services
- 18. Secure Router and Devices

Home Close Ports Help Links Setup Guest Network Wi-Fi Profiles Disclaimer

Saved Wi-Fi Profiles

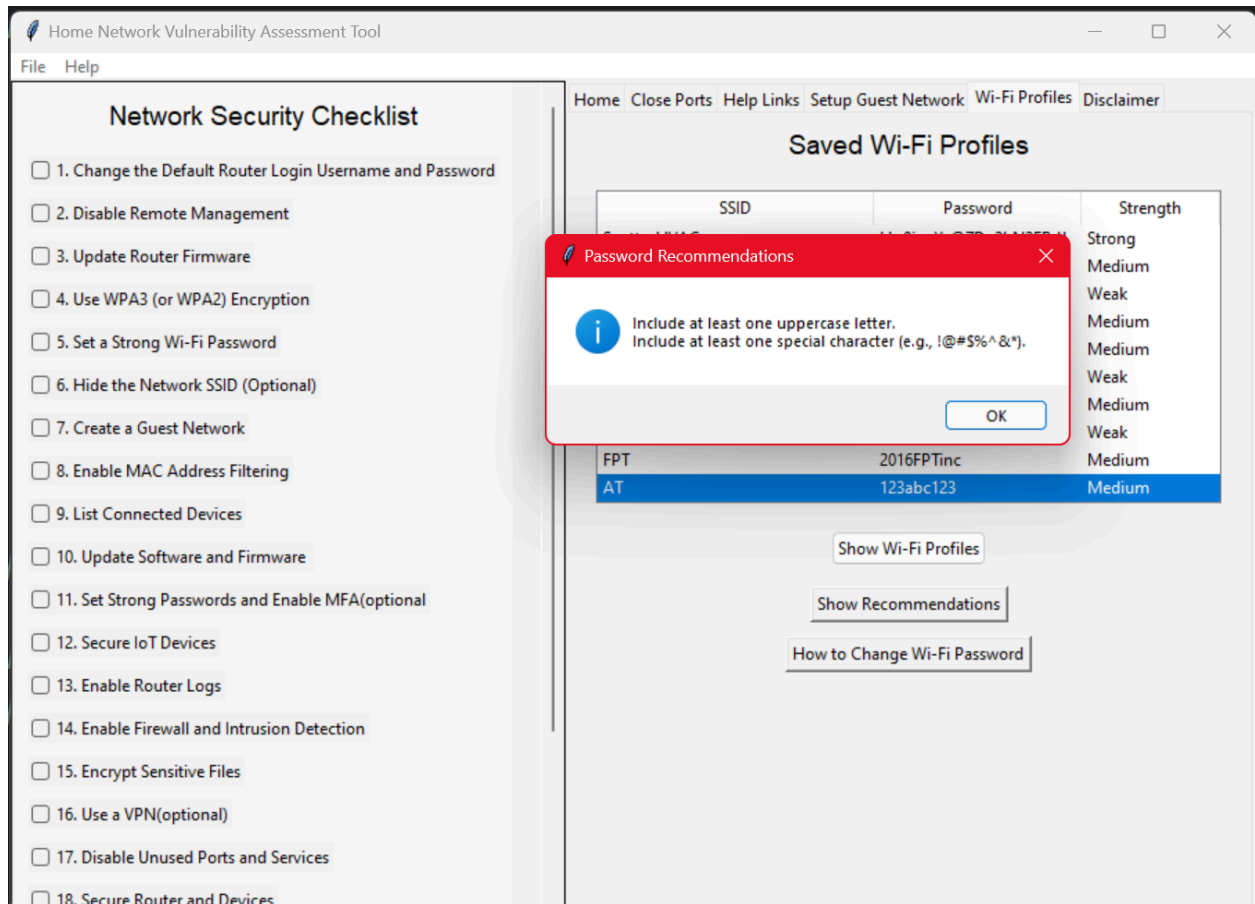
SSID	Password	Strength
------	----------	----------

Change Wi-Fi Password

i To change your WiFi password:

1. Open your router's web interface (usually accessed via a browser at 192.168.1.1).
2. Log in with your router's credentials.
3. Go to the Wi-Fi or wireless settings section.
4. Change the Wi-Fi password to a stronger one.
5. Save the settings and reconnect devices with the new password.

OK



Usability Study Analysis

Methodology: Participants used the tool for pre-defined tasks.

Results highlighted issues with navigation, lack of instructions, unsure how to enter the correct IP address for the port scanner, lack of help links for completing tasks on the checklist.

Technical Solution: Prototype Version 2.0

(Unavailable due to time constraints)

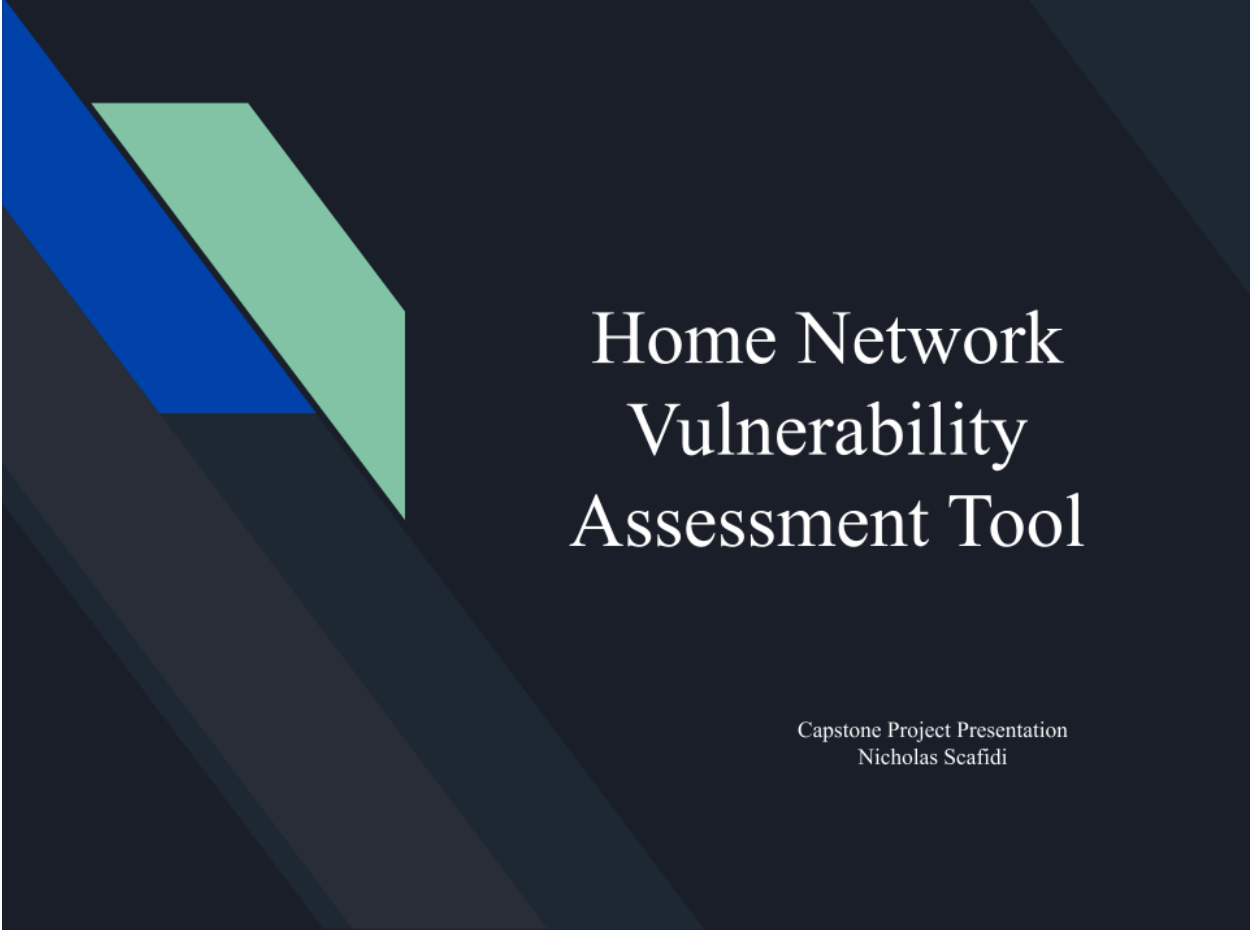
Possible Improvements: Enhanced navigation, added tooltips, and simplified instructions.

User Help Document:

(Unavailable due to time constraints)

Would be included in the appendix.

Presentation



Home Network Vulnerability Assessment Tool

Capstone Project Presentation
Nicholas Scafidi

Executive Summary

- The Home Network Vulnerability Assessment Tool addresses the critical need for accessible cybersecurity solutions for non-technical home users.
- Key Features:
 - Port scanning and closure guidance
 - Password strength assessment
 - Secure guest network setup for IoT devices
- User-friendly tool enhances digital safety and contributes to a culture of cybersecurity awareness.

Background

- Increased reliance on home networks has heightened cybersecurity risks:
- Proliferation of IoT devices
- Risks like data breaches and unauthorized access
- The project aims to bridge the gap between technical complexity and user accessibility.

Project Goals

- Develop a tool that simplifies network vulnerability assessment
- Provide actionable recommendations for home users
- Promote cybersecurity awareness and education

Project Planning and Management

- Timeline:
 - Week 1: Research and proposal
 - Week 4: Prototype 1.0 development
 - Week 7: Usability testing
 - Week 8: Report and presentation
- Success Metrics:
 - 90% task completion in usability tests
 - Positive user feedback
 - Identification of critical vulnerabilities

System Design

- Core Features:
 - Real-time network scanning
 - Comprehensive vulnerability reports
 - User-friendly interface with educational resources
- Stakeholders:
 - Home users
 - Cybersecurity professionals
 - IoT manufacturers
 - Instructors

Usability Study

- Methodology:
 - Tasks: Scan network, identify vulnerabilities, implement fixes
 - Participants: Varied technical expertise
- Findings:
 - Improved navigation and instructions clarity
 - Enhanced tooltips for first-time users

Prototype Development

- Version 1.0:
 - Basic navigation and core features
- Version 2.0:
 - Enhanced navigation
 - Additional and Simplified instructions
 - Additional tooltips
- Future Improvements:
 - Advanced help documentation
 - Expanded feature set

Conclusion

The Home Network Vulnerability Assessment Tool empowers home users to take control of their network security. By simplifying complex tasks, it contributes to safer digital environments and promotes cybersecurity awareness.