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.

1. **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.
2. **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    - **Step 4:** The tool scans connected devices and identifies that his home printer, used for work documents, has outdated firmware.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.
3. **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

1. **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.
2. **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.
3. **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.