**Technical Report: IoT Device Network Scanner Application**

**Overview**

Our application is tailored to scan networks for Internet of Things (IoT) devices that are presently not linked to it. It comes with a user-friendly executable file that acts as a helpful tool, making it easy for users to identify and establish connections with IoT devices on the network.

**Objectives**

**Network Scanning:** We go on a thorough network scan to identify devices, with a keen eye on IoT gadgets.

**Device Identification:** We use the scan results to spot IoT devices based on familiar patterns such as the watches, Tables and Phones etc. We then check if they're connected to the network.

**User Guidance:** We've put together some executable files to hold your hand through the scanning process and make sense of the results.

**Process**

The application follows a systematic process to ensure accurate and efficient scanning of the network:

**Network Detection**: The application/program first detects the network in which it is operating. This includes collecting information about the network’s IP address range, subnet mask, and default gateway.

**Device Discovery:** The application then scans the entire network, identifying all devices connected to it. This is achieved through a combination of techniques such as Nmap scanning and port scanning.

**IoT Device Recognition:** This application involves identifying devices present on a network and pinpointing which of these are specifically IoT devices. This entails analyzing device characteristics like MAC addresses, open ports, and responses to requests.

**Disconnected IoT Device Identification:** This application uses an Identification procedure that sifts through the list of IoT devices, singling out those that are presently offline or disconnected from the network. This disconnect can stem from reasons like device malfunction, network complications, or deliberate disconnection by the user.

**User Guidance:** The application gives guidance to the user on how to connect these severed IoT devices back to the network. This includes device-specific instructions, and recommendations for improving network security.

**Progress**

The development of this application has been a challenging yet rewarding process. We have successfully implemented all planned features and conducted extensive testing to ensure its accuracy and efficiency. The application is still in its developmental stage and will be deployed once its completed.

**Milestones Achieved:**

**Design and Development:** We've made strides in the design and development phases, from crafting network scanning scripts to figuring out how to recognize IoT devices.

**Executable File Creation**: We've written some executable files to walk the user through the scan process, making it super easy to use the app.

**Integration Testing:** We've run some serious integration tests, and we are encouraged by the results. This phase is too a working progress.

**Details/Results**

Our tests have shown that the application is capable of accurately identifying IoT devices within a network and determining their connection status. It has proven effective in various network environments and with a wide range of IoT devices. This phase is too a working progress.

**Cybersecurity Defense Mechanisms**

To keep things secure, we’ll be building safety mechanisms to make the application/program secure. Things that will be considered are;

**Secure Communication:** We've put in encryption to lock down communication between the app and your network, so no sneaky business can happen.

**Access Control:** Only the folks with the right keys can use the app and its scanning magic.

**Input Validation:** We've got a sharp eye for valid input, making sure nothing suspicious gets through and messes with the scan.

**Regular Updates:** We're committed to keeping things fresh and updated, to keep the application/program secure.

**Conclusion**

This application/program acts as a valuable tool for managing IoT devices within a network. It can identify disconnected devices and guide users through the process of reconnecting them not only improves network efficiency but also enhances security by ensuring all devices are properly managed and monitored.