Ethical Report

This report discusses the ethical aspects of a **Python-based port scanning script** and evaluates whether the implementation complies with accepted **ethical standards** in cybersecurity. The script in question performs a scan of **TCP ports** within a specific range on either the **local machine** or a **remote host**, and **logs** the results for review.

Port scanning is often used by system administrators to **assess network security**, but it can also be misused by malicious actors to identify vulnerabilities. Because of this dual-use nature, **ethical considerations** play a critical role in determining whether such a tool is being used appropriately. One of the most important ethical principles related to port scanning is that it must only be performed on **systems that the user owns** or has **explicit permission to test**. Unauthorized scanning of remote systems is generally considered a violation of cybersecurity law and professional ethical standards.

In terms of design, the script shows several signs of ethical responsibility. It includes **input validation** to ensure that the user provides a correctly formatted IP address. It also adds a **delay between scans** to prevent overwhelming the target system, which helps avoid potential denial-of-service effects. Furthermore, the **script logs all scan activity** to a file, which supports **transparency** and **accountability**.

However, the script does not prevent a user from **scanning remote systems without consent**. It allows the user to input any IP address, and it relies entirely on the **user to act ethically**. While this does not make the script unethical by itself, it does place the burden of **ethical compliance** on the person running the scan. When used only on local machines or systems with permission, the script aligns with ethical standards. When used without consent, however, it violates them.

In conclusion, the script itself incorporates several features that support ethical use, such as **logging**, **validation**, and **scan rate control**. It is ethically compliant when used responsibly on authorized systems. The responsibility to follow these ethical guidelines ultimately **falls on the user**, and proper usage must always involve **legal authorization** and respect for **system ownership**.