Henry Cort

2/23/25

Prof. Long

CYB530

This paper outlines migrating a Python 2 port scanner script to Python 3. The assignment included comparing the two versions using the Linux diff command, updating the Python 3 script to scan all TCP ports (1–65,535) in descending order, and displaying the service name for each open port.

To compare the Python 2 and Python 3 versions, the following diff command was used: diff portscannerv2.py portscannerv3.py

The key differences identified were:

**Input Handling:** Python 2 used raw\_input() for user input, which was replaced by input() in Python 3, as raw\_input() no longer exists in Python 3.

**Print Function:** The print statement in Python 2 (print "text") was updated to the print() function in Python 3 (print("text")), aligning with Python 3 syntax.

**Port Range and Order:** The original script scanned ports 1–1024 in ascending order. The Python 3 version was modified to scan all ports from 65,535 to 1.

**Service Name Retrieval:** The Python 3 version includes the socket.getservbyport() function to display the well-known service name for each open port.

**Timeout Addition:** A socket timeout (sock.settimeout(1)) was added to prevent the scanner from stalling on unresponsive ports.

The Python 3 script was modified to:

* **Scan All TCP Ports:** Expanded the scanning range from 1–1024 to 1–65,535.
* **Descending Order Scan:** Implemented a descending loop (65,535 to 1) for security reasons.
* **Display Service Names:** Used socket.getservbyport() to retrieve and display the service associated with each open port.
* **Improved Efficiency:** Added a timeout for faster scanning by skipping unresponsive ports quickly.

### **Final Source Code**

### 

### 

### 

### 

### 

### 

### 

### **Program Output**

