**Name :** ABIDASS k

**Company:** CODTECH IT SOLUTIONS

**Intern ID :** CT08DS6417

**Domain :** CYBER SECURITY&ETHICAL HACKING

**Duration:** Augest to September 2024

**Mentor :** Muzammil Ahmed

**Vulnerability Scanning Tool**

This tool leverages Nmap to scan for open ports on a target system and includes a Python script to identify outdated software. The tool is essential for security professionals to assess and mitigate vulnerabilities.

**Nmap**: Verify that Nmap is installed on your system. If not, you can install it using the following commands:

sudo apt-get install nmap # For Debian/Ubuntu

brew install nmap # For macOS

**Python 3.x**: Confirm that Python 3.x is installed by checking the version with the command:

python3 --version

**Nmap Usage:** Scanning for Open Ports

To scan for open ports on a target IP or hostname, use the following command:

nmap -sS -p 1-65535 <target-ip>

\* **-sS**: Conducts a TCP SYN scan.

\* **-p 1-65535**: Scans all ports, from 1 to 65535.

Example:

Sudo nmap -sS 192.168.85.178

**Output image:**



**Python Script:** Checking for Outdated Software

This script compares your installed Python packages with the latest versions available on PyPI, helping you identify any outdated software.

**Installation**:

pip install pip-review

**Script:**

import subprocess

def find\_outdated\_packages():

result = subprocess.run(['pip-review', '--outdated'], capture\_output=True, text=True)

if result.returncode == 0 and result.stdout.strip():

print("Outdated Packages:")

print(result.stdout)

else:

print("All packages are up to date.")

if \_name\_ == "\_main\_":

find\_outdated\_packages()

**Usage:**

1. To run the script, use the following command

python3 outdated\_software.py

[Cite your source here.]

2.Sample Output image: 