PYTHON PROJECT

1. Write the code to create a port scanner in Python.
2. Implement error handling and input validation to ensure the program handles unexpected scenarios gracefully.

```python
from socket import *

1 usage
def conScan(target_Host, target_Port):
    try:
        connskt = socket(AF_INET, SOCK_STREAM)
        connskt.connect((target_Host, target_Port))
        print('[+] %d/tcp open' % target_Port)
        connskt.close()
    except:
        print('[-] %d/tcp closed' % target_Port)

1 usage
def portScan(targetHost, targetPorts):
    try:
        targetIP = gethostbyname(targetHost)
    except:
        print('[-] Cannot resolve %s' % targetHost)
        return
    try:
        targetName = gethostbyaddr(targetIP)
        print('\n[+] Scan result of: %s' % targetName[0])
    except:
        print('\n[+] Scan result of: %s' % targetIP)
    setdefaulttimeout(1)
    for targetPort in targetPorts:
        print('Scanning Port: %d' % targetPort)
        conScan(targetHost, int(targetPort))

if __name__ == "__main__":
    targetHost = input("Enter the hostname or IP address to scan: ")
    targetPorts = [int(targetPort) for targetPort in input("Enter the ports to scan (comma-separated): ").split(",")]
    portScan(targetHost, targetPorts)
```

- After writing the program with python,
- I copied the script and saved it in a file **(port_scanner.py)** in windows Terminal by using **nano editor**
- I gave the script execution privilege with sudo chmod +x port_scanner.py

3. Test the port scanner on localhost and a remote host to verify its functionality.(Note: Remote host must be within a subnet created with VMs)
    - Testing on localhost

```
┌──(kali㉿kali)-[~]
└─$ python port_scanner.py
Enter the hostname or IP address to scan: 192.168.56.10
Enter the ports to scan (comma-separated): 80,22

[+] Scan result of: 192.168.56.10
Scanning Port: 80
[-] 80/tcp closed
Scanning Port: 22
[+] 22/tcp open
```

- Testing on first remote host

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ ssh kali@192.168.38.7
The authenticity of host '192.168.38.7 (192.168.38.7)' can't be established.
ED25519 key fingerprint is SHA256:oSEde6CGEmlH8heqa6xbI+ORk3tLPEE0FZ3uPHqmXmY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.38.7' (ED25519) to the list of known hosts.
kali@192.168.38.7's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 11 04:54:38 2024 from 192.168.56.103
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  port_scanner.py  Public  sshkey  sshkey.pub  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ python port_scanner.py
Enter the hostname or IP address to scan: 192.168.38.7
Enter the ports to scan (comma-separated): 53,22

[+] Scan result of: 192.168.38.7
Scanning Port: 53
[+] 53/tcp open
Scanning Port: 22
[+] 22/tcp open
```

- Testing on second remote host (windows)

```
C:\Users\betta>ssh kali@192.168.38.7
The authenticity of host '192.168.38.7 (192.168.38.7)' can't be established.
ED25519 key fingerprint is SHA256:oSEde6CGEmlH8heqa6xbI+ORk3tLPEE0FZ3uPHqmXmY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.38.7' (ED25519) to the list of known hosts.
kali@192.168.38.7's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 17 11:15:37 2024 from 192.168.38.6
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  port_scanner.py  Public  sshkey  sshkey.pub
 Templates  Videos

┌──(kali㉿kali)-[~]
└─$ python port_scanner.py
Enter the hostname or IP address to scan: 192.168.38.7
Enter the ports to scan (comma-separated): 53,22

[+] Scan result of: 192.168.38.7
Scanning Port: 53
[+] 53/tcp open
Scanning Port: 22
[+] 22/tcp open
```