NAME ; Shrishti vishwakarma

CLASS : BVOC (First year) Sem 2

TITLE : Port Scanner using Python and Nmap

INSTRUCTOR : Shubham sir

TABLE OF CONTENT

INTRODUCTION

Port scanning is a technique used in network security to identify open ports and services available on a networked device. This project demonstrates how to build a simple port scanner using Python and the Nmap library. Nmap is a powerful network scanning tool commonly used by cybersecurity professionals to discover hosts, detect open ports, and gather information about network services.

OBJECTIVE

- To understand how port scanning works
- To implement a basic port scanner using Python and Nmap
- To analyze network ports and services
- To develop awareness of network security and vulnerabilities

TOOLS USED

1. Python
2. Nmap

PYTHON CODE

Below is a basic port scanner using the nmap module in Python:

```
import nmap

scanner = nmap.PortScanner()
ip = '127.0.0.1'
port_range = '20-1000'

print(f'Scanning {ip} for ports {port_range}...')
scanner.scan(ip, port_range)

for host in scanner.all_hosts():
    print(f'Host : {host}
({scanner[host].hostname()})')
    print(f'State : {scanner[host].state()}')
    for proto in scanner[host].all_protocols():
```

```
        print(f'Protocol : {proto}')
        ports = scanner[host][proto].keys()
        for port in sorted(ports):
            print(f'Port : {port}\tState :
{scanner[host][proto][port]['state']}')
```

OUTPUT

The scanner identifies open ports on the target IP. Below is an example output:

Scanning 127.0.0.1 for ports 20-1000...
Host : 127.0.0.1
State : up
Protocol : tcp
Port : 22 State : open
Port : 80 State : open

CONCLUSION

This project helped in understanding how network ports are scanned using Python and Nmap. It provided insight into how open ports can expose services to the outside world, and why it's important to secure them. Port scanning is a

fundamental skill in ethical hacking and network analysis.