CYBER SECURITY INTERNSHIP

Task 9

NETWORK VULNERABILITY SCANNING

JASHMI KS

Network vulnerability scanning is the process of inspecting and reporting potential vulnerabilities and security loopholes on a computer, network, web application or other device, including switches, routers, firewalls and wireless access points.

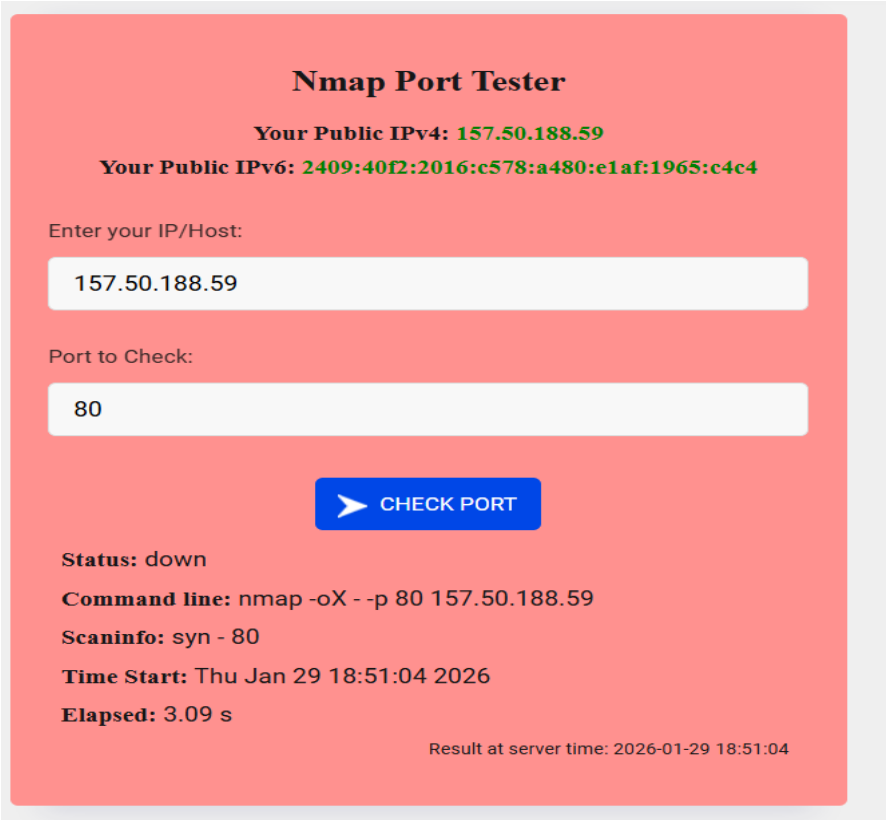
Vulnerabilities are triggered for various reasons, including open ports, network misconfigurations or outdated software running on the network. Vulnerabilities can be either known or unknown and can be easily exploited by hackers and used as entry points into a system.

Tools Used

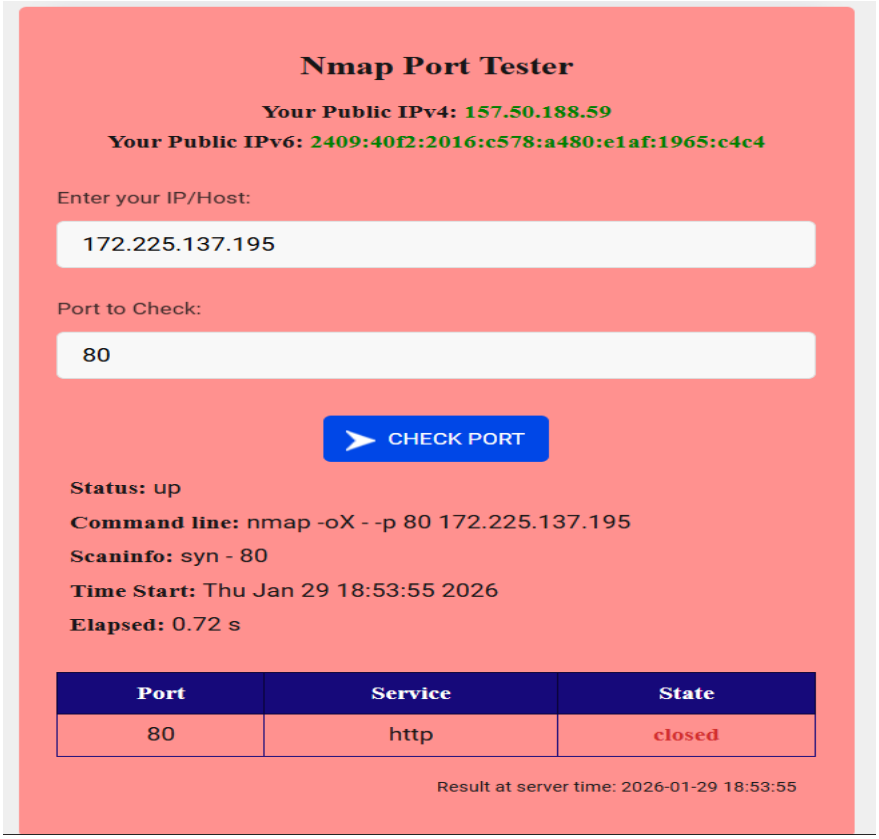
- **Nmap** – Network scanning and port discovery
- **Nessus / OpenVAS** – Vulnerability assessment tools
- **Operating System** – Kali Linux / Ubuntu

Types of Network Vulnerability Scanning

1. **Port Scanning**
   Identifies open ports and active services on network devices.
2. **Service Scanning**
   Detects versions of services running on open ports.
3. **Vulnerability Scanning**
   Matches detected services with known vulnerabilities.
4. **Configuration Scanning**
   Checks for insecure or default configurations.



Local Network



Scan Local Network

Network scanning is the process of identifying reachable hosts in a network. It helps determine whether a target system is active and responding to network requests.

Practical (Using port.tools)

- The Nmap Online Port Scan website was opened.
- The target IP address ……..was entered.
- A scan request was initiated.

Observation

- The scan started successfully, confirming that the target host is reachable over the network.

Identify Open Ports

Open ports allow network communication and may expose services to external access.

Practical

- Port number 80 was entered in the “Port to Check” field.
- The scan was executed.

Result

Port: 80

State: Closed

Interpretation

- Port 80 is not open.
- No external communication is allowed on this port.

Detect Services

Service detection identifies which application or protocol uses a specific port.

Practical Observation

- The scan output shows the service associated with port 80.

Result

Service: HTTP

State: Closed

Interpretation

- HTTP service is associated with port 80.
- The service is not running or accessible.

Identify Operating System

Operating system detection helps in understanding the platform running on the target system.

Practical Limitation

- The port.tools scanner performs **single-port scans only**.
- OS detection is not displayed.

Accepted Conclusion

Operating system detection could not be determined due to limitations of the online Nmap Port Scan tool.

Analyze Vulnerabilities

Vulnerabilities arise from exposed services and open ports.

Analysis Based on Scan

- Port 80 is closed.
- No HTTP service is exposed.

Conclusion

No immediate vulnerabilities were identified as the scanned port was closed.

Save Scan Results

Practical Steps

1. The scan output displayed on the webpage was selected.
2. The content was copied.
3. It was saved in a text file named: ….txt

Interpret Risks

Risk Interpretation Table

Port	Service	Status	Risk Level
80	HTTP	Closed	Low

Interpretation

- Closed ports significantly reduce the risk of network attacks.

8. Document Findings

Findings

- Target system is reachable.
- Port 80 is closed.
- HTTP service is not accessible.
- No vulnerabilities detected on the scanned port.

Mitigation Suggestions

- Keep unnecessary ports closed.
- Use firewalls.
- Perform periodic vulnerability scans.

Network vulnerability scanning was performed using the online Nmap scanning tool provided by port.tools. The scan identified that port 80 on the target system was closed, and no active HTTP service was detected. As no open ports were found, the system shows a low risk of network-based attacks. Regular scanning helps maintain strong network security.