**Ethical Hacking Project Report:** Port Scanning

**Author:** Daniel Muthama

**Date:** April 29, 2025

**Target:** testphp.vulnweb.com

**1. Executive Summary**

This report details the findings of a port scanning exercise conducted on the target testphp.vulnweb.com. The objective was to identify open ports on the target system using a custom Python port scanner and validate results with the industry-standard tool Nmap.

**2. Objectives**

Develop a Python-based port scanner to detect open ports.

Validate results using Nmap.

Identify potential attack surfaces for further security testing.

**3. Tools Used**

**Custom Python Port Scanner:**

Scans TCP ports sequentially within a specified range.

Timeout handling to skip unresponsive ports.

**Nmap:**

Used to verify open ports and service detection.

**4. Methodology**

**Step 1:** Port Scanning with Custom Python Script

**Command Executed:**

python3 port-scanner.py testphp.vulnweb.com -s 1 -e 100

**Parameters:**

**Target:** testphp.vulnweb.com

**Port Range:** 1-100

**Step 2:** Validation with Nmap

**Command Executed:**

nmap -p 80 testphp.vulnweb.com

**Purpose:** Confirm port 80 status and service details.

**5. Results**

**5.1 Python Port Scanner Output**

--------------------------------------------------

Scanning target: testphp.vulnweb.com

**Time started:** 2025-04-29 20:10:23.064218

--------------------------------------------------

[+] Port 80 is open

Scan complete!

**Open ports:** [80]

**5.2 Nmap Validation Output**

Nmap scan report for testphp.vulnweb.com (44.228.249.3)

PORT STATE SERVICE

80/tcp open http

**Key Findings:**

**Port 80 (HTTP):** Open and running a web server.

**Service:** HTTP (Web traffic).

**6. Analysis**

**6.1 Security Implications**

**Port 80:**

Indicates a web server is accessible.

**Common attack vectors include:**

Directory brute-forcing (e.g., /admin, /login).

SQL injection or XSS on web forms.

Outdated server software vulnerabilities (e.g., Apache, Nginx).

**6.2 Tool Comparison**

Metric Python Scanner Nmap

Port 80 Detection ✔️ ✔️

Service Detection ❌ ✔️ (HTTP)

Speed Slow (sequential) Fast

**7. Limitations**

**Scope:** Limited to ports 1–100 (Python scanner) and TCP only.

**Service Identification:** The Python script does not detect service banners.

**Speed:** No threading implemented for concurrent scans.

**8. Recommendations**

**Further Testing:**

Perform directory brute-forcing with tools like Gobuster or Dirbuster.

Test for web vulnerabilities (e.g., SQLi, XSS).

**Tool Improvements:**

Add threading to the Python scanner for faster results.

Implement banner grabbing to identify services.

**9. Ethical Considerations**

The target testphp.vulnweb.com is a publicly available test domain for security research.

No unauthorized systems were scanned.

**10. Conclusion**

The Python port scanner successfully identified port 80 as open on testphp.vulnweb.com, validated by Nmap. This port represents a critical entry point for web-based attacks, warranting further penetration testing.

**11. Appendices**

**Appendix A:** Python Port Scanner Code

[Code Attached in the Parent File]

**Appendix B:** Raw Terminal Outputs

**Python Scanner:**

[Python Scanner Output in the Parent folder]

**Nmap:**

[Nmap Output in the Parent folder]

**12. References**

**Nmap Documentation:** https://nmap.org/book/man.html

**Python socket Library:** https://docs.python.org/3/library/socket.html

**Submitted to:** Shivam Sir

**Verification Status:** Pending