**NMAP SCAN REPORT ON testphp.vulnweb.com** **Name:** Orji Ekeoma Miracle  
 **Date:** April 17, 2025

**Objective**  
 The aim of this project was to conduct a basic port scan on the domain "testphp.vulnweb.com" using Nmap. This was done to identify open ports and services on the host, as part of a cybersecurity learning exercise.

**Tool Used** Nmap (Network Mapper), version 7.95  
 Nmap is a free and open-source utility used for network discovery and security auditing.

**Command Used**  
 nmap -p- -sS testphp.vulnweb.com

**Explanation of the command:**  
 "nmap" is the command-line tool.  
 "-p-" tells Nmap to scan all 65535 TCP ports.  
 "-sS" initiates a SYN scan (also called a stealth scan) to detect open ports without completing the TCP handshake.

**Findings**  
 Target Domain: testphp.vulnweb.com  
 IP Address: 44.228.249.3  
 Reverse DNS: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
 Host Status: Host is up (online and responsive)  
 Open Port:  
 Port 80 (TCP) - HTTP service  
 Other Ports: 65534 ports were filtered (no response received)

**Analysis**  
 The host is accessible and has port 80 open, which is commonly used to serve web pages through HTTP. Since "testphp.vulnweb.com" is a known site for security testing and educational purposes, this result is expected.  
 All other ports were filtered, meaning no response was received. This could indicate the presence of a firewall or network filtering, which prevents access to unnecessary or sensitive services.

**Recommendations**  
 The following best practices are recommended:

* Only expose necessary ports to the internet.
* Replace HTTP with HTTPS (secure version) to protect transmitted data.
* Keep all server software updated to avoid known vulnerabilities.
* Use a firewall to filter unused or dangerous ports.
* Monitor network traffic to detect potential intrusions.
* Employ additional tools to test the web application for vulnerabilities, such as SQL injection or cross-site scripting.

**Conclusion**  
 The scan on "testphp.vulnweb.com" showed that only port 80 is open, which is hosting an HTTP web service. This suggests a minimal and controlled configuration, suitable for cybersecurity practice. No other services were exposed. This type of scan helps beginners understand how to identify active services on a system and assess basic security postures.

