**NMAP Scan Report on -testphp.vulnweb.com**

**Name: Enoghayin Osarobo**

**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 7.94

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 65534 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 target host is reachable, with port 80 open—typically used for serving web content over HTTP. This is consistent with the purpose of "testphp.vulnweb.com," a site intentionally designed for educational and security testing.

All other ports appeared filtered, meaning they did not respond to the scan. This behavior may suggest the use of a firewall or network-level filtering that blocks access to non-essential or sensitive services.

**RECOMMENDATIONS**

To enhance security, the following practices are advised:

* Limit exposure by allowing only essential ports to be accessible over the internet.
* Upgrade from HTTP to HTTPS to ensure secure transmission of data.
* Regularly update server software to patch known vulnerabilities.
* Implement firewalls to block unused or potentially harmful ports.
* Continuously monitor network activity to detect suspicious behavior.
* Use additional tools to assess the web application for vulnerabilities like SQL injection or cross-site scripting (XSS).

**CONCLUSION**

The scan revealed that only port 80 is open on "testphp.vulnweb.com," which serves HTTP content. This minimal exposure reflects a controlled setup ideal for training and cybersecurity exercises. No additional services were detected. Such scanning activities are valuable for beginners to learn how to identify open ports and evaluate basic security configurations.

