Penetration Testing Report

# 1. Target Information

- Target Domain: http://testphp.vulnweb.com  
- IP Address: 44.228.249.3  
- rDNS: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
- Scan Date: April 13, 2025  
- Scanner Used: Nmap 7.95

# 2. Objective

The objective of this assessment was to identify all open TCP ports and gather information about the services running on the host testphp.vulnweb.com, which is a vulnerable web application used for ethical hacking and testing.

# 3. Scan Summary

|  |  |  |
| --- | --- | --- |
| Scan Type | Command | Purpose |
| Basic Scan | nmap testphp.vulnweb.com | Identify common open ports |
| Aggressive Scan | nmap -A testphp.vulnweb.com | Detect services, versions, OS, and traceroute |
| Full Port Scan | nmap -p- testphp.vulnweb.com | Scan all 65,535 TCP ports |
| Service Detection | nmap -p- -sV testphp.vulnweb.com | Detect services on all ports |
| Script Scan | nmap -sC testphp.vulnweb.com | Use default Nmap scripts to gather additional info |
| Output to File | nmap -p- -sV -oN scan\_results.txt testphp.vulnweb.com | Store scan results locally |

# 4. Host Information

- Host Status: Online  
- Latency: Varies (0.00031s to 0.069s)  
- Traceroute Hops:  
 - Hop 1: 192.168.92.2  
 - Hop 2: ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)  
- OS Detection: Inconclusive due to limited open/closed port range

# 5. Open Ports Detected

|  |  |  |  |
| --- | --- | --- | --- |
| Port | State | Service | Version |
| 80/tcp | open | HTTP | nginx 1.19.0 / tcpwrapped |

# 6. Service and OS Details

- Web Server: nginx 1.19.0  
- Operating System Guesses:  
 - Actiontec MI424WR-GEN3I WAP (96%)  
 - DD-WRT v24-sp2 (Linux 2.4.37) (96%)  
 - Linux (various versions, 90–94%)  
 - Windows XP SP3 / 7 / Server 2012 (90–92%)  
- Note: OS detection was unreliable due to limited port visibility.

# 7. NSE Script Results

Default Nmap scripts (`-sC`) were executed. No additional open ports or critical vulnerabilities were detected beyond port 80.

# 8. Output File Summary

Command: nmap -p- -sV -oN scan\_results.txt testphp.vulnweb.com  
File: scan\_results.txt  
Summary: Port 80 was the only open port, service detected as `tcpwrapped`.

# 9. Key Findings

- Only one TCP port (80) is open across all scans.  
- The HTTP service is likely protected by TCP wrapper.  
- No other services or ports appear exposed.  
- Host is hosted on AWS EC2 in us-west-2 region.

# 10. Recommendations

1. Restrict Port Access (Firewall Rules): Ensure that only necessary ports are open.  
2. Upgrade Web Server (nginx): Consider updating from version 1.19.0 which is end-of-life.  
3. Use HTTPS (Port 443): Implement HTTPS to secure web traffic.  
4. Harden TCP Wrappers: Confirm that TCP wrapper configurations restrict unauthorized access.

# 11. Conclusion

The host is configured with a minimal attack surface (only port 80 open). OS fingerprinting and service enumeration were limited by firewall rules or TCP wrappers. No high-risk vulnerabilities were detected in this preliminary assessment.