Security Audit Report: Full Port Scan on testphp.vulnweb.com

Goal

The goal of this scan was simple:

Check all 65,535 TCP ports on testphp.vulnweb.com to ensure no services are hiding on non-standard ports.

This was part of a comprehensive security audit no shortcuts.

Tools Used

Nmap Industry-standard network scanner

Bash For automation scripting

Python (matplotlib) To generate visuals of scan results (optional)

What We Did (Methodology)

1. Full TCP Port Scan with Nmap

We used Nmaps full scan mode to sweep through all possible TCP ports.

nmap -p- -T4 -v testphp.vulnweb.com -oN full_port_scan_output.txt

-p-: Scans all 65,535 ports

-T4: Uses faster timing to reduce scan duration

-v: Enables verbose output

-oN: Saves output in a readable text file

2. Automation Script

To ensure repeatability and consistency, we wrote a Bash script:

```
#!/bin/bash
TARGET="testphp.vulnweb.com"
OUTPUT="full_port_scan_output.txt"
echo "[*] Starting full TCP port scan on $TARGET..."
nmap -p- -T4 -v $TARGET -oN "$OUTPUT"
echo "[*] Scan complete. Output saved to $OUTPUT"
```

Security Audit Report: Full Port Scan on testphp.vulnweb.com

To run:

chmod +x full_port_scan.sh

./full_port_scan.sh

What We Found

Port Service Notes

22 SSH Standard remote access

80 HTTP Web server expected

3306 MySQL Database exposed should be firewalled

8888 sun-answerbook Often used for dev tools like Jupyter investigate access

Script Submission

Bash Script: full_port_scan.sh

```
#!/bin/bash
TARGET="testphp.vulnweb.com"
OUTPUT="full_port_scan_output.txt"
echo "[*] Starting full TCP port scan on $TARGET..."
nmap -p- -T4 -v $TARGET -oN "$OUTPUT"
```

Final Conclusion

A full port scan of testphp.vulnweb.com revealed that while common services like SSH and HTTP were expected, critical services such as MySQL and a potential development interface on port 8888 were also exposed highlighting how important it is to scan every port, not just the usual suspects. This approach ensures hidden or misconfigured services don't go unnoticed, reinforcing the need for thoroughness in every security audit.