Name: Dean Joah Bell
Register No: 2462061

Assignment 16: Detect Service Versions with Nmap

🧪 Methodology

Performed Nmap service version scans on two publicly accessible legal targets:
1. testphp.vulnweb.com
2. scanme.nmap.org
Used the command `nmap -sV` to identify running services and their versions. Mapped detected versions to known vulnerabilities (CVEs) using trusted sources like the National Vulnerability Database (NVD).

🔍 Findings

Target: testphp.vulnweb.com

1. **Port 80: nginx 1.19.0**
   - CVE-2021-23009: On BIG-IP version 16.0.x before 16.0.1.1 and 15.1.x before 15.1.3, malformed HTTP/2 requests may cause an infinite loop which causes a Denial of Service for Data Plane traffic.

Target: scanme.nmap.org

2. **Port 22: OpenSSH 6.6.1p1**
   - CVE-2015-5600: The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks.
3. **Port 80: Apache httpd 2.4.7**
   - CVE-2014-0226: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information

📊 Conclusion

All identified services are outdated and have publicly known vulnerabilities.
- nginx 1.19.0 is vulnerable to remote code execution and DoS attacks.
- OpenSSH 6.6.1p1 allows brute-force login attempts.
- Apache 2.4.7 is susceptible to race conditions.