Nmap Scan Analysis Report

Scanned Domain: groww.in

Target Summary

Scan Tool: Nmap
Scan Type: Service/port scan (results show tcpwrapped)
Detected Open Ports:

Port	Protocol	State	Service
21	tcp	open	tcpwrapped
25	tcp	open	tcpwrapped
80	tcp	open	tcpwrapped
443	tcp	open	tcpwrapped
8080	tcp	open	tcpwrapped
8443	tcp	open	tcpwrapped

Key Findings

1. Common Service Ports Open

The following well-known service ports are open: 21 (FTP), 25 (SMTP), 80 (HTTP), and 443 (HTTPS). These ports indicate standard services such as file transfer, email, and web services.

2. High-Risk / Suspicious Ports

Ports 8080 and 8443 are open. These are often used for web admin panels, proxies, or application backends. They are commonly targeted due to weak authentication or outdated software.

3. Vulnerability Risks

- FTP (21): May allow anonymous login or transmit credentials in plaintext. - SMTP (25): Could be misconfigured as an open relay, exploitable by spammers. - HTTP (80): Unencrypted traffic vulnerable to interception. - HTTPS (443/8443): Potential SSL/TLS misconfigurations. - Alt Web Ports (8080/8443): May expose admin consoles or applications susceptible to known exploits.

4. Critical Observations

The scan results indicate multiple open ports associated with sensitive services. The use of 'tcpwrapped' suggests access restrictions, which is a good practice, but also prevents full service/version detection. If these services are exposed externally without proper hardening, they may lead to exploitation.

5. Recommendations

- Disable or secure FTP; replace with SFTP/FTPS. - Ensure SMTP is not an open relay. - Redirect HTTP (80) to HTTPS (443). - Perform SSL/TLS audits on 443 and 8443. - Restrict access to ports 8080 and 8443 (admin services). - Conduct deeper vulnerability scanning with Nmap NSE and service version detection.

6. Impact on Data Security and Privacy

Open service ports increase the attack surface. If misconfigured, attackers could: - Intercept unencrypted communications (HTTP, FTP). - Exploit weak authentication on admin consoles (8080/8443). - Compromise sensitive data through vulnerable services. This poses risks to both data security and user privacy, potentially enabling data breaches or unauthorized access.