**Network Security Scan Report**

**Scan Tool:** Nmap 7.95  
**Scan Date:** 26 May 2025  
**Time Zone:** India Standard Time (IST)  
**Target Host:** xxx.xxx.xx.1 (IP address masked for security)  
**Latency:** 0.25s  
**Scan Duration:** 20.82 seconds

**🎯 Summary**

Nmap scanned 1000 TCP ports.

* **Host Status:** Up
* **Total Open Ports:** 5
* **Filtered Ports:** 995 (no response received)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port** | **Protocol** | **Service** | **Common Uses** | **Potential Risks** |
| 21 | TCP | FTP (File Transfer Protocol) | Transfers files between client and server in plaintext. Often used for legacy systems or unauthenticated file sharing. | - **Unencrypted communication**: Allows interception of credentials and data. - **Anonymous login**: Can expose sensitive files. - **Brute-force target**: Widely exploited. |
| 80 | TCP | HTTP (HyperText Transfer Protocol) | Default protocol for serving unencrypted web content. | - **No encryption**: User data and credentials are visible in transit. - Vulnerable to **injection**, **XSS**, and **man-in-the-middle** attacks. - Attracts scanning bots. |
| 443 | TCP | HTTPS (HTTP Secure) | Encrypted web communication using TLS. Common for secure websites. | - **TLS misconfigurations**: Use of weak ciphers or self-signed/expired certificates. - **Heartbleed-like attacks** if server is unpatched. - **Downgrade attacks** possible. |
| 8080 | TCP | HTTP-Proxy / Alt HTTP | Alternate HTTP port; used for testing, admin consoles, or proxy services. | - May expose **debugging interfaces** or **internal services**. - Often **unsecured or misconfigured**. - Target for **directory traversal or RCE** vulnerabilities. |
| 8443 | TCP | HTTPS-Alt (Alternate HTTPS) | Often used for secure access to admin panels (e.g., Tomcat, Plesk). | - Commonly hosts **sensitive management consoles**. - Subject to **brute-force login attempts**, especially on Java-based platforms. - May reveal **banner info**. |

**General Observations**

* **The host is reachable and responsive, indicating it's exposed to the public internet.**
* **All detected services are commonly scanned and attacked by automated bots and threat actors.**
* **Presence of both standard and alternate HTTP(S) ports suggests possible web applications or admin panels are exposed**