Nmap Scan Report — WordPress Lightsail PCI Practice

Date: November 19, 2025
Target: `wp.98-89-111-197.sslip.io`
IP Address: `98.89.111.197`
Environment: Bitnami WordPress on AWS Lightsail

---

1. Overview

A network and service enumeration scan was conducted using Nmap to identify open ports, running services, SSL certificate configuration, and server fingerprints.
This scan supports **PCI DSS Requirement 1** (network monitoring) and **Requirement 4** (encryption).

Command executed:

```
nmap -sV -sC -p 22,80,443 wp.98-89-111-197.sslip.io
```

---

2. Summary of Findings

Port	Status	Service	Version	Notes
22/tcp	open	SSH	OpenSSH 9.2p1	Secure and updated SSH version
80/tcp	open	HTTP	Apache	Redirects to HTTPS
443/tcp	open	HTTPS	Apache + Let's Encrypt	Valid SSL certificate, modern configuration

No high-risk vulnerabilities detected.
The server is running correctly with HTTPS enforced.

---

3. Detailed Findings

Port 22 – SSH

```
22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u6
```

- Running a **modern & secure SSH version**.
- Key fingerprints match expected fresh installation behavior.
- No weak ciphers disclosed in Nmap's default scan.

PCI Impact:
✔ Meets secure remote access expectations (Requirement 8).

Port 80 – HTTP

```
80/tcp open http Apache httpd
Did not follow redirect to https://wp.98-89-111-197.sslip.io/
```

- Port 80 is open only to **force HTTP → HTTPS redirection**.
- This is normal and expected.

PCI Impact:
✔ Supports encrypted transmission requirements (Requirement 4).
✔ No sensitive content served over HTTP.

Port 443 – HTTPS

```
443/tcp open ssl/http Apache httpd
SSL Cert CN: wp.98-89-111-197.sslip.io
Valid: 2025-11-19 → 2026-02-17
WordPress 6.8.1 detected
```

- Let’s Encrypt certificate is valid.
- HTTPS is correctly configured.
- Server reveals WordPress version (normal for WordPress).

PCI Impact:
✔ Strong encryption in place (Req. 4)
⚠ WordPress version disclosure will be reviewed in later scans.

Robots.txt

```
1 disallowed entry: /wp-admin/
```

- This is standard for WordPress.
- No sensitive directories exposed.

---

4. Risk Rating

Risk Area	Rating	Notes
Network Exposure	**Low**	Only required ports open
Encryption	**Low**	HTTPS enforced, valid certificate

Service Versions	**Low**	All modern software
Fingerprinting	**Medium (normal)**	WordPress version exposed (to be hardened later)

---

5. PCI DSS Mapping

PCI Requirement	Status	Notes
Req 1 – Network Security	✔ PASS	Minimal ports exposed
Req 2 – Secure Configurations	✔ PASS	No insecure defaults detected
Req 4 – Encryption	✔ PASS	HTTPS enforced
Req 5 – Malware	N/A	Will scan with ClamAV later
Req 6 – System Hardening	⚠ In Progress	WordPress hardening to come

---

6. Next Steps (Planned Tools)

1. **Nikto** – Web server misconfigurations
2. **WPScan** – WordPress vulnerabilities
3. **ZAP** – Application security
4. **SSL Labs** – HTTPS grade
5. **SecurityHeaders** – Header hardening
6. **ClamAV** – Malware detection

7. **Final PCI report** combining all tools

---

7. Conclusion

The Nmap scan shows a **well-configured, secure Lightsail WordPress environment**. No critical issues were detected. The system is ready for deeper PCI scanning with Nikto, WPScan, and ZAP.