Vulnerability Scanning Report Using Nmap

Name: Ranjan Kumar\ **Tool Used:** Nmap (Network Mapper)\ **Target IP:** 192.168.236.132\ **Date of Scan:** July 30, 2025

1. Objective

This report aims to document the findings of a vulnerability assessment conducted on a local virtual machine using Nmap. The purpose was to identify open ports, running services, potential misconfigurations, and known vulnerabilities.

2. Tools & Methodology

Tools Used:

- Nmap 7.94SVN (Parrot OS)

Commands Executed:

```
nmap -sS -sV -T4 -Pn 192.168.236.132
nmap --script vuln 192.168.236.132
nmap -A --script vuln 192.168.236.132
```

Explanation of Flags:

- `-sS` : Stealth SYN scan
- `-sV` : Service and version detection
- `-T4` : Faster execution
- `-Pn` : No ping (treat host as up)
- `--script vuln` : Use default vulnerability scripts
- `-A` : Enable OS detection, version detection, script scanning, and traceroute

3. Scan Results Summary

Open Ports Identified:

Port	State	Service	Version
22/tcp	Closed	SSH	
80/tcp	Open	HTTP	Apache httpd
443/tcp	Open	SSL/HTTP	Apache httpd

MAC Address: 00:0C:29\:BB:1C:1B (VMware)

4. Vulnerability Findings

a) CSRF Vulnerabilities Detected

- **Path:** `/wp-login.php`
- Multiple suspicious JavaScript files and forms were discovered indicating potential CSRF vulnerabilities.
- Forms lacked CSRF tokens in various locations like:
- `/js/BASE_URL`
- `/js/rs;...`
- `/js/vendor/null...`

b) XSS (Cross-Site Scripting)

- **Stored XSS:** Not found
- **DOM-based XSS:** Not found

c) WordPress Enumeration

Several endpoints indicate an outdated WordPress installation:

Path	Description
`/feed/`	WordPress version: 4.3.1
`/wp-includes/...`	WP versions 2.2 to 2.7 detected
`/admin/`, `/wp-login.php`	Admin/login pages exposed
`/robots.txt`, `/readme.html`	Info disclosure possibilities
`/0/`, `/image/`	Suspicious folders, likely not intended for public access

Risk: Older WordPress versions are vulnerable to multiple CVEs including RCE, XSS, SQL Injection, etc.

---

5. Observations & Inference

- Multiple potentially dangerous scripts detected without CSRF protection.
- WordPress installation is outdated, significantly increasing the attack surface.
- No immediate XSS issues, but deeper manual testing recommended.
- SSH port (22) is closed — helpful for reducing attack surface.

---

6. Recommendations

1. **Update WordPress** to the latest stable version.
2. **Implement CSRF tokens** in all login and form-based submissions.
3. Restrict access to sensitive folders (`/admin`, `/0`, `/image`) using `.htaccess` or authentication.
4. Remove or restrict public access to `readme.html` and `robots.txt`.
5. Conduct manual XSS testing and secure client-side JS.

6. Consider using a Web Application Firewall (WAF).

---

7. Conclusion

This Nmap vulnerability scan revealed that the target system is running a vulnerable WordPress installation with missing CSRF protections and exposed administrative paths. Immediate remediation is advised to prevent exploitation by attackers.

---

8. References

- OWASP CSRF Guide
- NIST Vulnerability Management
- SANS Security Resources

Report Prepared By: Ranjan Kumar

End of Report