**🛡️ Cyber Security Internship – Vulnerability Scan Summary Report**  
**Scan Tool:** Nessus Essentials  
**Scan Type:** Full Vulnerability Scan  
**Scan Date:** June 28, 2025  
**Prepared by:** Piyush Manghnani  
**Target:** Local Network (192.168.29.112)

### ****1. Objective****

The purpose of this report is to document the results of a full vulnerability assessment conducted using Nessus Essentials. The assessment was performed as part of a cybersecurity internship project to identify potential security risks on local network devices.

### ****2. Tools Used****

* **Nessus Essentials** by Tenable
* Version: 10.8.4
* OS: Kali Linux
* Scan Duration: ~1 hour
* Scan Target: Local Network (192.168.29.0/24)

### ****3. Summary of Findings****

| IP Address | Critical | High | Medium | Low | Info | Total |
| --- | --- | --- | --- | --- | --- | --- |
| 192.168.29.1 | 0 | 0 | 4 | 2 | 27 | 33 |
| 192.168.29.13 | 0 | 0 | 0 | 1 | 3 | 4 |
| 192.168.29.17 | 0 | 0 | 0 | 1 | 3 | 4 |
| 192.168.29.64 | 0 | 0 | 0 | 1 | 3 | 4 |
| 192.168.29.112 | 0 | 0 | 1 | 0 | 64 | 65 |
| 192.168.29.118 | 0 | 0 | 0 | 1 | 5 | 6 |
| 192.168.29.214 | 0 | 0 | 0 | 1 | 3 | 4 |

### ****4. Key Vulnerabilities (Sample from Top Hosts)****

#### ****192.168.29.1****

* **SSL Certificate Cannot Be Trusted** – Medium severity
* **IP Forwarding Enabled** – Medium severity
* **Self-Signed Certificate Detected** – Medium severity
* **DNS Cache Snooping** – Medium severity

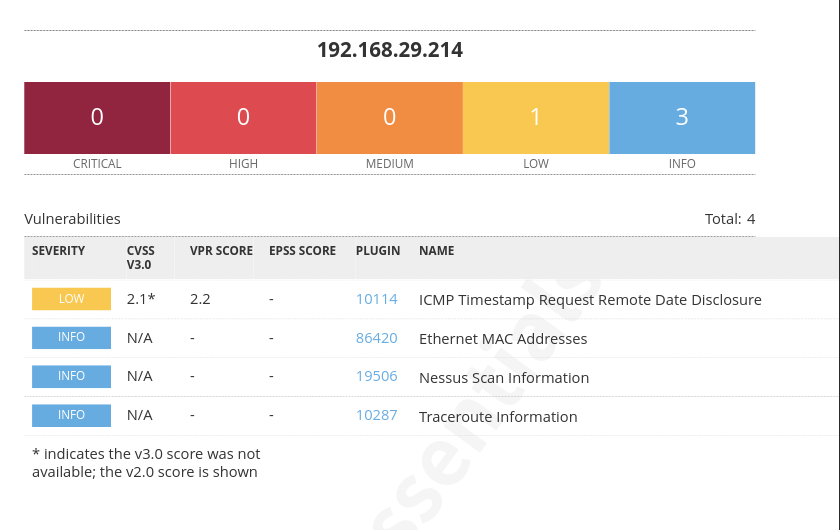
#### ****192.168.29.112****

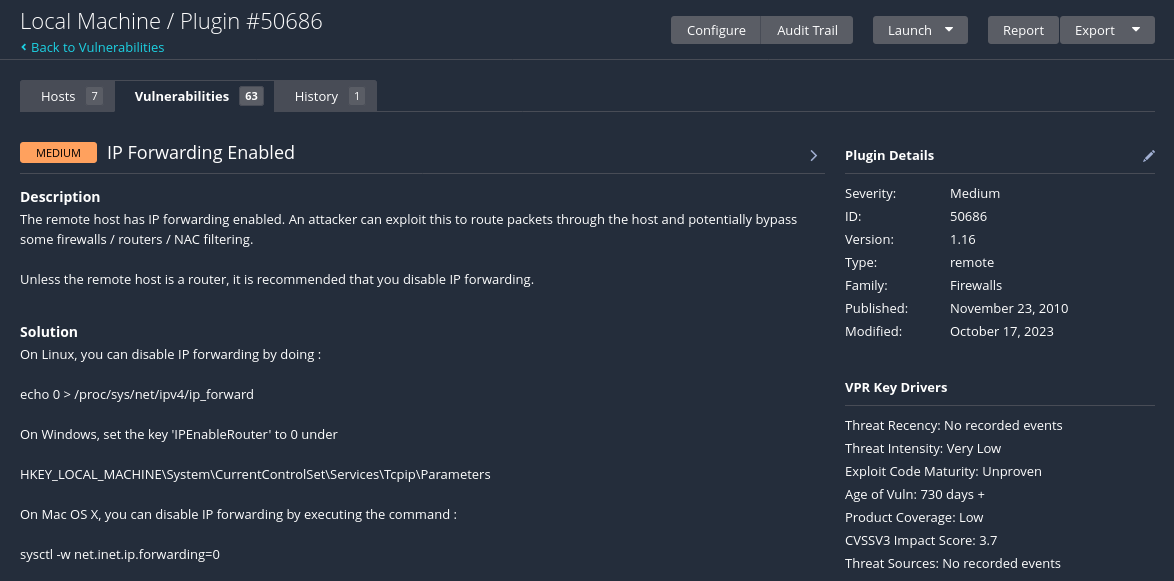
* **SSL Certificate Cannot Be Trusted** – Medium severity
* **Multiple software and service versions detected (Apache, PHP, OpenVPN, Node.js, etc.)**
* **Possible outdated cryptographic protocols (TLS 1.2, 1.3)**

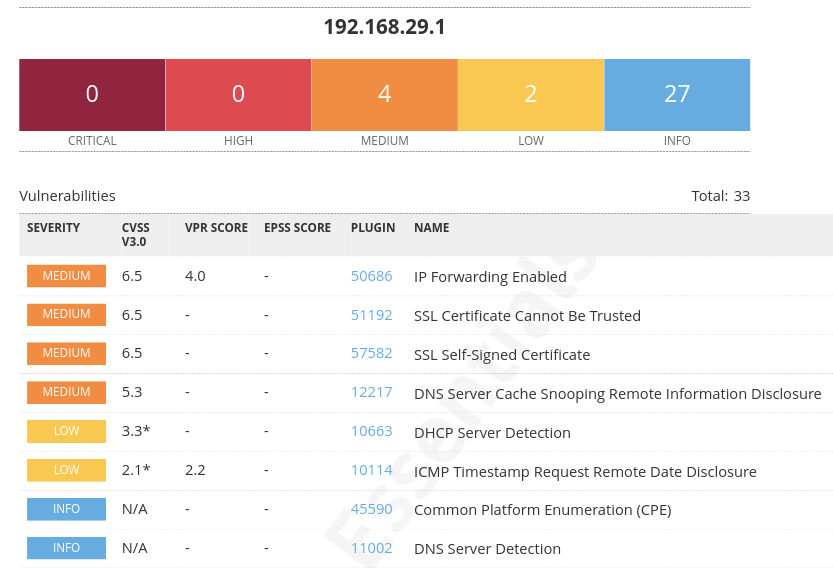
### ****5. Recommendations & Fixes****

* **Replace or reissue SSL certificates** from a trusted CA.
* **Disable IP forwarding** if not required.
* **Configure DNS securely** to avoid cache snooping.
* **Review and update software packages** like Apache, OpenVPN, Node.js.
* **Harden server configurations** by enforcing updated cipher suites and enabling HSTS.

### ****6. Screenshots****









### ****7. Mitigation****

**1. IP Forwarding Enabled**

* 🔧 **Fix**: Disable IP forwarding if not required by editing /etc/sysctl.conf and setting net.ipv4.ip\_forward = 0.
* 💡 **Why**: Prevents packet forwarding, reducing the risk of unauthorized routing or MITM attacks.

**2. SSL Certificate Cannot Be Trusted / Self-Signed Certificate**

* 🔧 **Fix**: Replace with a valid SSL certificate from a trusted Certificate Authority (CA).
* 💡 **Why**: Ensures secure communication and user trust.

**3. ICMP Timestamp Request Remote Date Disclosure**

* 🔧 **Fix**: Block ICMP timestamp requests using firewall rules (e.g., iptables or ufw).
* 💡 **Why**: Prevents remote attackers from gathering system time and fingerprinting the OS.

**4. DNS Server Cache Snooping**

* 🔧 **Fix**: Restrict DNS responses to known clients and disable recursion if not required.
* 💡 **Why**: Protects against attackers discovering previously queried domains.

**5. TLS/SSL Weak Cipher Suites**

* 🔧 **Fix**: Reconfigure services (e.g., Apache/Nginx/SSH) to support only strong cipher suites and disable deprecated protocols like TLS 1.0/1.1.
* 💡 **Why**: Ensures modern, secure encryption methods are used.

### ****8. Conclusion****

**This vulnerability scan revealed multiple informational and medium-level issues across several hosts. While no critical or high-risk vulnerabilities were detected, remediation of these issues is recommended to strengthen network security.**