**Nessus scan report**

**1. Installation of Nessus Essentials**

**Tool Used:** Nessus Essentials  
**Platform:** Windows 11 / Linux (Ubuntu 22.04)  
**Installation Steps:**

* Downloaded the installer from the Tenable Nessus Essentials website.
* Installed Nessus and registered with a free activation key.
* Configured the Nessus web interface (usually accessible at https://localhost:8834).
* Allowed the application through the system firewall.

**2. Set up scan target as your local machine IP or localhost.**

**------------Ip address 192.168.0.182**

**3.Start a full vulnerability scan.**

**Wait for scan to complete (may take 30-60 mins).**

**Scan Type:** Full Vulnerability Scan  
**Scan Configuration:**

* Chose the “Advanced Scan” template.
* Defined the scan target as the local machine IP.
* Left most configurations as default for thoroughness.

The Nessus scan report you provided lists **12 vulnerabilities** detected on the host 192.168.0.186. Here's a breakdown of the findings and their severity:

### Vulnerability Review and Mitigation Recommendations for Report: **My Basic Network Scan**

**Target Host:** 192.168.0.186  
**Total Vulnerabilities Found:** 12  
**Severity Levels:**

* **Critical:** 0
* **High:** 0
* **Medium:** 0
* **Low:** 0
* **Informational (Info):** 12

All vulnerabilities listed are **informational**, meaning they do not pose immediate threats but may reveal useful data for attackers during reconnaissance. However, even these can be exploited under the right conditions. Here's a breakdown:

### **Vulnerability Review**

| **Plugin Name** | **Risk** | **Description** |
| --- | --- | --- |
| **Common Platform Enumeration (CPE)** | Info | Identifies software/hardware CPE names used for vulnerability mapping. |
| **DCE Services Enumeration** | Info | Lists Distributed Computing Environment (DCE) services, which may reveal RPC services. |
| **Device Type** | Info | Detects the general type of device (e.g., router, PC, printer). |
| **Ethernet Card Manufacturer Detection** | Info | Uses MAC address to detect NIC manufacturer. May help fingerprint hardware. |
| **Ethernet MAC Addresses** | Info | Lists MAC addresses for interfaces; can aid in tracking devices. |
| **LLMNR Detection** | Info | LLMNR can be abused for man-in-the-middle attacks (e.g., spoofing). |
| **Nessus SYN Scanner** | Info | Performs a TCP SYN scan to identify open ports. |
| **Nessus Scan Information** | Info | Details about the scan itself; useful for audit logs. |
| **OS Fingerprints Detected** | Info | Identifies OS using TCP/IP stack characteristics. |
| **OS Identification** | Info | Confirms the operating system of the host. |
| **TCP/IP Timestamps Supported** | Info | Timestamps can reveal system uptime and aid in OS fingerprinting. |
| **Traceroute Information** | Info | Reveals network path to target host; helps map network structure. |

### **Mitigation and Hardening Recommendations**

| **Vulnerability** | **Mitigation Strategy** |
| --- | --- |
| **LLMNR Detection** | Disable LLMNR if not required:  Windows: via Group Policy or registry (DisableMultiCast=1). |
| **MAC Address/Ethernet Detection** | Limit Layer 2 exposure; implement port security on switches and use VLANs. |
| **DCE Services Enumeration** | Restrict RPC exposure through firewall rules. Consider disabling unused DCE/RPC services. |
| **TCP/IP Timestamps** | Disable timestamps (Linux: net.ipv4.tcp\_timestamps = 0). Helps prevent uptime fingerprinting. |
| **OS Fingerprints/Identification** | Use host-based firewalls or security software to obfuscate stack behavior. Consider implementing passive OS fingerprinting prevention tools. |
| **Traceroute Information** | Use firewall rules to limit ICMP responses and hop-reveal data. |
| **General Recommendations** |  |

* Segment networks and use proper firewall rules.
* Harden host configurations using CIS Benchmarks.
* Minimize broadcast protocol usage like NetBIOS, LLMNR, and mDNS unless necessary.
* Keep systems updated and monitored.