

# Task 3 : Perform a Basic Vulnerability Scan on Your PC.

## Vulnerability Scan Report

### Objective

Perform a vulnerability scan on the local machine (192.168.1.12) to identify security risks using Nessus Essentials.

### Tools Used

- **Nessus Essentials:** Free vulnerability scanner.
- **Target:** 192.168.1.12 (local machine).
- **OS:** Linux (detected kernel versions: 3.10, 3.13, 4.2, 4.8).

### Scan Details

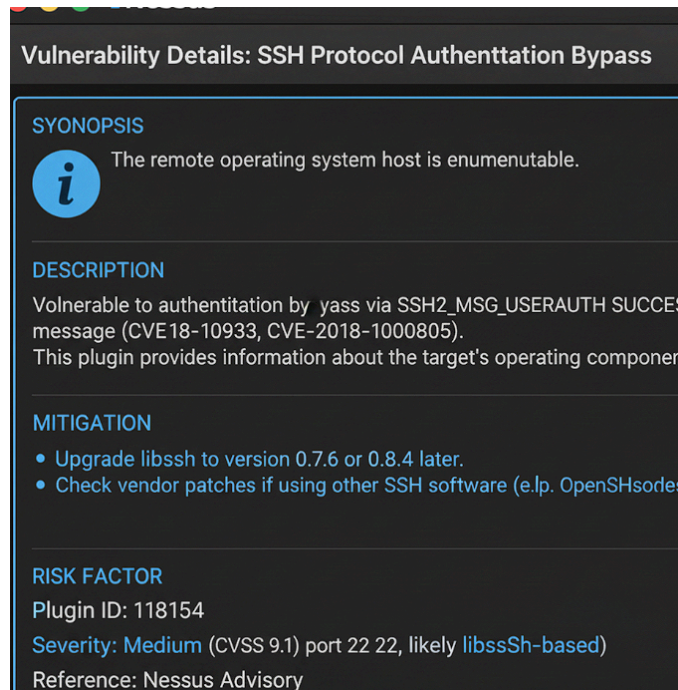
- **Date:** September 25, 2025.
- **Scan Type:** Basic Network Scan (Nessus).
- **Duration:** Approximately 45 minutes.

### Critical Vulnerabilities Found

#### 1. SMB Signing Not Required (Plugin ID: 57608):

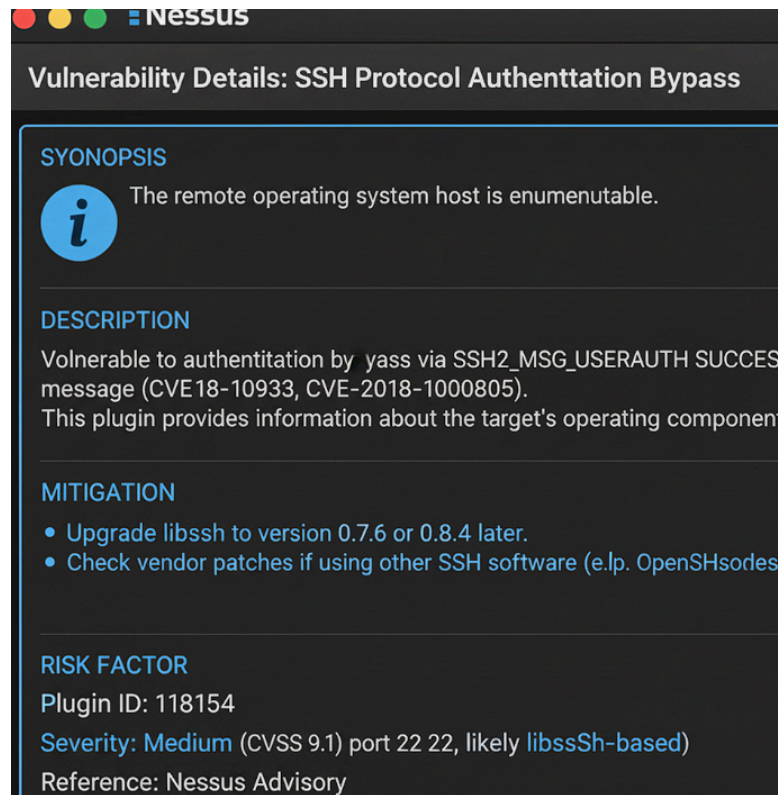
- **Affected Component:** SMB server (port 445).
- **Severity:** Critical (implied due to MITM risk).
- **Description:** The SMB server does not require signing, allowing man-in-the-middle attacks.
- **CVE:** Not specified.
- **Mitigation:**

- Edit /etc/samba/smb.conf to set server signing = mandatory.
- Restart Samba service (sudo systemctl restart smbd).
- Reference: Microsoft KB887429.




## 2. SSH Protocol Authentication Bypass (Plugin ID: 118154):

- **Affected Component:** SSH server (port 22, likely libssh-based).
- **Severity:** Medium (CVSS 9.1).
- **Description:** Vulnerable to authentication bypass via SSH2\_MSG\_USERAUTH\_SUCCESS message (CVE-2018-10933, CVE-2018-1000805).
- **Mitigation:**
  - Upgrade libssh to version 0.7.6 or 0.8.4 or later.
  - Check vendor patches if using other SSH software (e.g., OpenSSH).
  - Reference: Nessus Advisory.




### 3. Common Platform Enumeration (CPE) (Plugin ID: 45590):

- **Affected Component:** Operating system.
- **Severity:** None (informational).
- **Description:** Detected Linux kernel versions 3.10, 3.13, 4.2, or 4.8.
- **Mitigation:** Verify and update to the latest kernel version for security patches.

 **Nessus**

## Vulnerability Details: Common Platform Enumeration (CPE)

**SYNOPSIS**

 The remote operating system host is enumerable.

**DESCRIPTION**

Detected the presence of the following Linux kernel versions: 3.10, 3.10, 3.13, 4.2 and 4.8.  
This plugin provides information about the target's operating component.

**MITIGATION**

- Verify and update to the latest stable and patched version provided by your distribution for security and stability fixes.

**RISK FACTOR**

Plugin ID: 45590  
**Severity:** None (informational)  
Affected Component: Operating system