

SUMMARY REPORT ON **VULNERABILITY ASSESSMENT**

Assessor Name:Esha Khadeeja C

Table of Contents

SI.NO	TOPIC	PAGE.NO
1	Executive Summary	3
2	Introduction	3
3	Scope	3
4	Methodolody	3
5	Setup and Installation	4
6	Conducting the scan	6
7	Analysis of FIndings	7
8	Risk Assessment	8
9	Remediation Recommendations	10
10	Conclusion	11

Executive Summary

The primary objective of this project was to conduct a vulnerability assessment on a Windows 7 virtual machine. This assessment aimed to identify security vulnerabilities and provide actionable recommendations for remediation.

Introduction

This assessment was conducted on a Windows 7 virtual machine, designated as WIN7, with the IP address 192.168.47.129. The primary goals of this vulnerability assessment are to :-

- Identify existing vulnerabilities in the Windows 7 virtual machine.
- Assess the severity of each identified vulnerability.
- Provide detailed recommendations for mitigating the identified vulnerabilities.

Scope

The assessment focused exclusively on a Windows 7 virtual machine with the following details:

- **Hostname:** WIN7
- **IP Address:** 192.168.147.129
- **Operating System:** Windows 7 Professional

Methodology

The assessment was conducted using Nessus Pro, a widely recognized vulnerability scanner. The approach included:

- Performing an internal, credentialed scan from within the same network to ensure comprehensive coverage.
- Scanning for a range of vulnerabilities, including missing patches, misconfigurations, and potential security weaknesses.

Setup and Installation

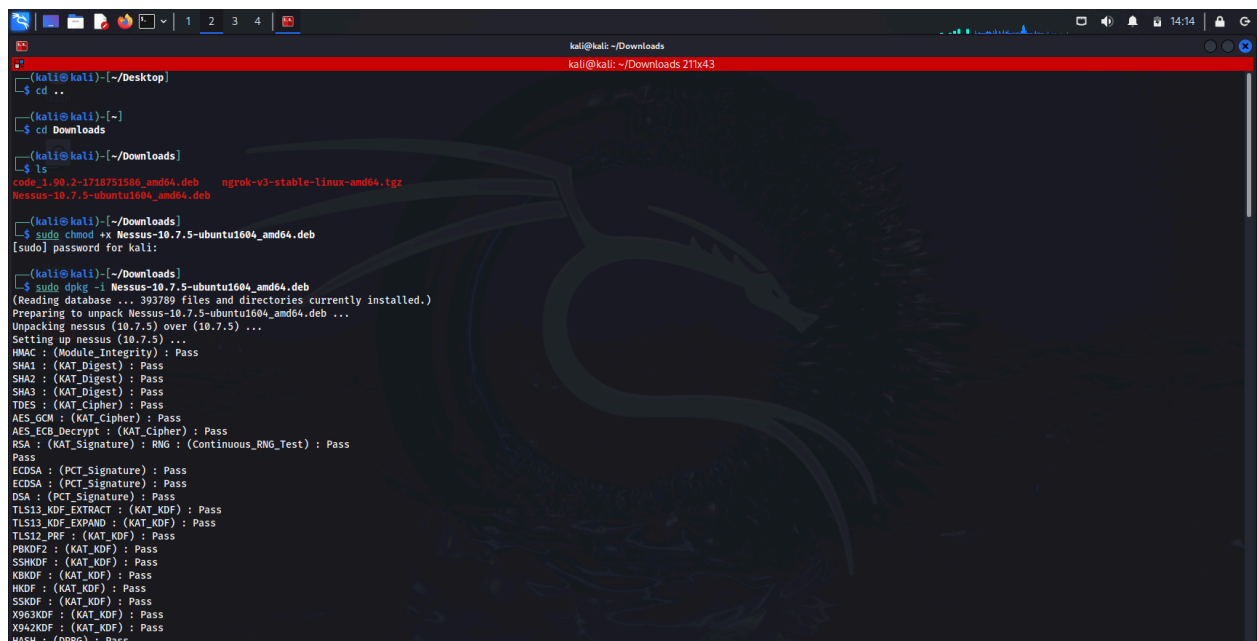
1. Download Nessus Pro(Free trial) to Kali Linux from the website
<https://www.tenable.com/downloads/nessus?loginAttempted=true>
2. Update your system before installation:

command : *sudo apt-get update*

3. Install nessus pro

Commands:

- `sudo chmod +x <filename>`
- `sudo dpkg -i <filename>`



```
(kali@kali)~[~/Desktop]
$ cd ..
(kali@kali)~[~]
$ cd Downloads
(kali@kali)~[~/Downloads]
$ ls
code_1.90.2-1718751586_amd64.deb  ngrok-v3-stable-linux-amd64.tgz
nessus-10.7.5-ubuntu1604_amd64.deb
(kali@kali)~[~/Downloads]
$ sudo chmod +x Nessus-10.7.5-ubuntu1604_amd64.deb
[sudo] password for kali:
(kali@kali)~[~/Downloads]
$ sudo dpkg -i Nessus-10.7.5-ubuntu1604_amd64.deb
(Reading database ... 393789 files and directories currently installed.)
Preparing to unpack Nessus-10.7.5-ubuntu1604_amd64.deb ...
Unpacking nessus (10.7.5) over (10.7.5) ...
Setting up nessus (10.7.5) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
```

4. Start nessusd service and check its status

Commands:

- `/bin/systemctl start nessusd.service`
- `/bin/systemctl status nessusd.service`

```
kali@kali: ~/Downloads
RSA Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner

(kali@kali)-[~/Downloads]
└─$ /bin/systemctl start nessusd.service

(kali@kali)-[~/Downloads]
└─$ /bin/systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset:➤
   Active: active (running) since Sat 2024-07-20 13:54:40 EDT; 10min ago
   Main PID: 5425 (nessus-service)
     Tasks: 25 (limit: 3439)
    Memory: 1.6G (peak: 1.8G swap: 72.0K swap peak: 59.0M)
       CPU: 31min 45.266s
    CGroup: /system.slice/nessusd.service
            └─5425 /opt/nessus/sbin/nessus-service -q
               └─8780 nessusd -q

Jul 20 13:54:40 kali systemd[1]: Started nessusd.service - The Nessus Vulnerabi
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
...skipping...
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset:➤
   Active: active (running) since Sat 2024-07-20 13:54:40 EDT; 10min ago
   Main PID: 5425 (nessus-service)
     Tasks: 25 (limit: 3439)
    Memory: 1.6G (peak: 1.8G swap: 72.0K swap peak: 59.0M)
       CPU: 31min 45.266s
    CGroup: /system.slice/nessusd.service
            └─5425 /opt/nessus/sbin/nessus-service -q
               └─8780 nessusd -q

Jul 20 13:54:40 kali systemd[1]: Started nessusd.service - The Nessus Vulnerabi
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
```

4.Enable nessusd service and check its status

Commands:

- /bin/systemctl enable nessusd.service
- /bin/systemctl status nessusd.service

```
kali@kali: ~/Downloads
(kali@kali)-[~/Downloads]
└─$ /bin/systemctl enable nessusd.service
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /usr/lib/systemd/system/nessusd.service.

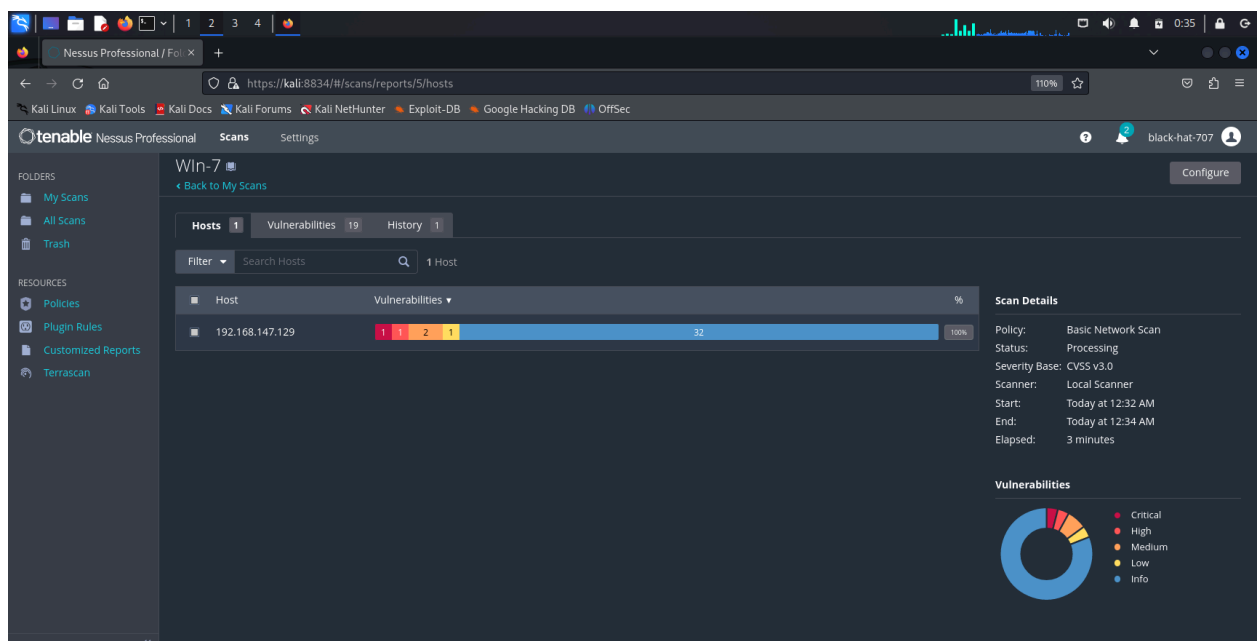
(kali@kali)-[~/Downloads]
└─$ /bin/systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: ➤
   Active: active (running) since Sat 2024-07-20 13:54:40 EDT; 11min ago
   Main PID: 5425 (nessus-service)
     Tasks: 25 (limit: 3439)
    Memory: 1.6G (peak: 1.8G swap: 68.0K swap peak: 59.0M)
       CPU: 36min 56.796s
    CGroup: /system.slice/nessusd.service
            └─5425 /opt/nessus/sbin/nessus-service -q
               └─8780 nessusd -q

Jul 20 13:54:40 kali systemd[1]: Started nessusd.service - The Nessus Vulnerabi
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
lines 1-14/14 (END) ...skipping...
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2024-07-20 13:54:40 EDT; 11min ago
   Main PID: 5425 (nessus-service)
     Tasks: 25 (limit: 3439)
    Memory: 1.6G (peak: 1.8G swap: 68.0K swap peak: 59.0M)
       CPU: 36min 56.796s
    CGroup: /system.slice/nessusd.service
            └─5425 /opt/nessus/sbin/nessus-service -q
               └─8780 nessusd -q

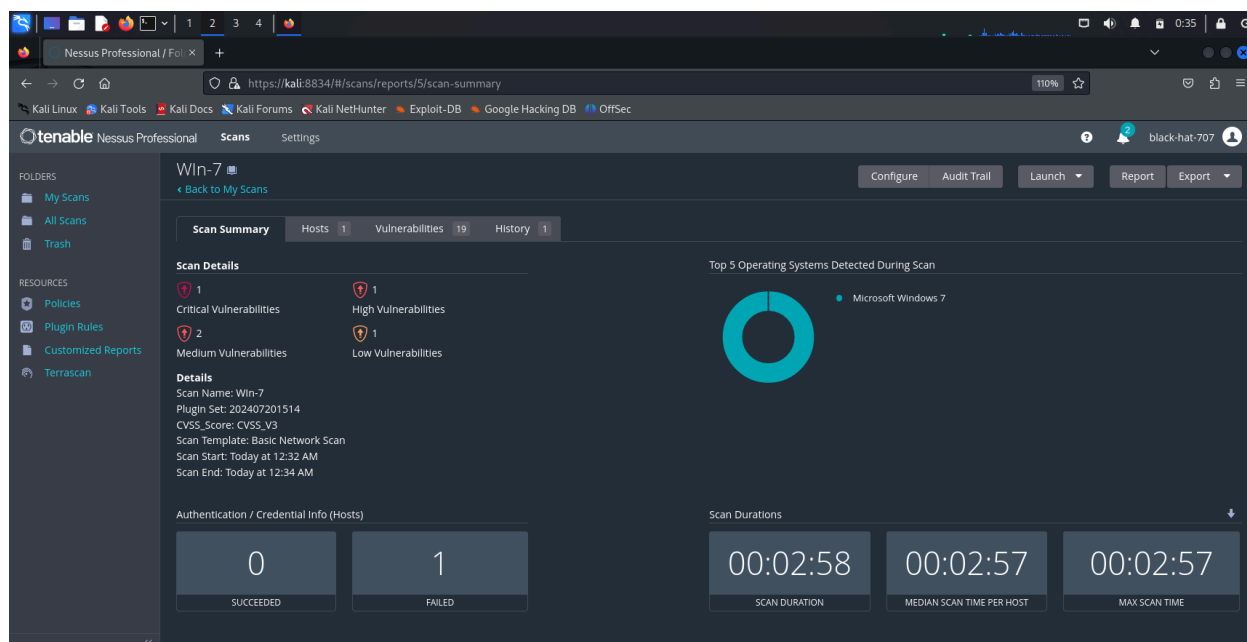
Jul 20 13:54:40 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
Jul 20 13:54:42 kali nessus-service[5427]: Cached 0 plugin libs in 0msec
```

Conducting the Scan

1. Access Nessus Pro through your web browser by navigating to <https://localhost:8834/>
2. Login with your credentials
3. Click on New Scan button and choose the required scan, For this vulnerability assessment I used Advanced Network Scan.
4. Configuration of the scan:
Name: win7-scan
IP address: 192.168.147.129
Credentials: <pwd of the windows machine>
5. Save the configuration and click on 'Launch' Button



6. Click on the scan to view the results.

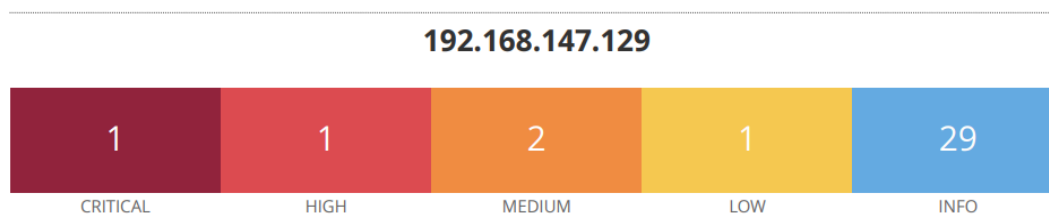


Analysis of Findings

The scan performed on the Windows 7 system identified a total of five vulnerabilities categorized by their severity:

- **Critical Vulnerabilities:** 1
- **High Vulnerabilities:** 1
- **Medium Vulnerabilities:** 2
- **Low Vulnerabilities:** 1

This distribution indicates that the system has several weaknesses that require different levels of attention.



Authentication Attempts:

- **Succeeded:** 0
- **Failed:** 1

Scan Details and Metrics

- **Scan Name:** Win-7
- **Plugin Set:** 202407201514
- **CVSS Score:** CVSS_V3
- **Scan Template:** Basic Network Scan
- **Scan Start:** 12:32 AM
- **Scan End:** 12:34 AM
- **Scan Duration:** 00:02:58
- **Median Scan Time per Host:** 00:02:57
- **Max Scan Time:** 00:02:57
- **Analysis:** The scan attempted to authenticate but failed. This indicates that authenticated scans, which provide deeper insights into system vulnerabilities, were not possible. Lack of authenticated scans might result in missing certain vulnerabilities that require credentials to be detected.

Risk Assessment

Critical Vulnerability

- **Unsupported Windows OS (remote)**
 - **Severity:** Critical
 - **CVSS V3.0:** 10.0
 - **Plugin:** 108797
 - **Description:** The system is running an unsupported version of Windows, which no longer receives security updates. This leaves it vulnerable to numerous exploits and attacks.
 - **Impact:** High risk of exploitation due to lack of security patches, leading to potential system compromise, data breaches, and further attacks.

High Vulnerability

- **MS17-010: Security Update for Microsoft Windows SMB Server**
 - **Severity:** High
 - **CVSS V3.0:** 8.1
 - **VPR Score:** 9.7

- **Plugin:** 97833
- **Description:** This vulnerability, also known as EternalBlue, allows remote code execution via the SMB protocol. It has been used in major attacks like WannaCry and Petya.
- **Impact:** High risk of remote code execution, ransomware attacks, and network-wide infection.

Medium Vulnerabilities

1. MS16-047: Security Update for SAM and LSAD Remote Protocols (Badlock)

- **Severity:** Medium
- **CVSS V3.0:** 6.8
- **VPR Score:** 6.0
- **Plugin:** 90510
- **Description:** A vulnerability in the Security Account Manager (SAM) and Local Security Authority (LSAD) remote protocols, potentially allowing privilege escalation.
- **Impact:** Moderate risk of privilege escalation and unauthorized access.

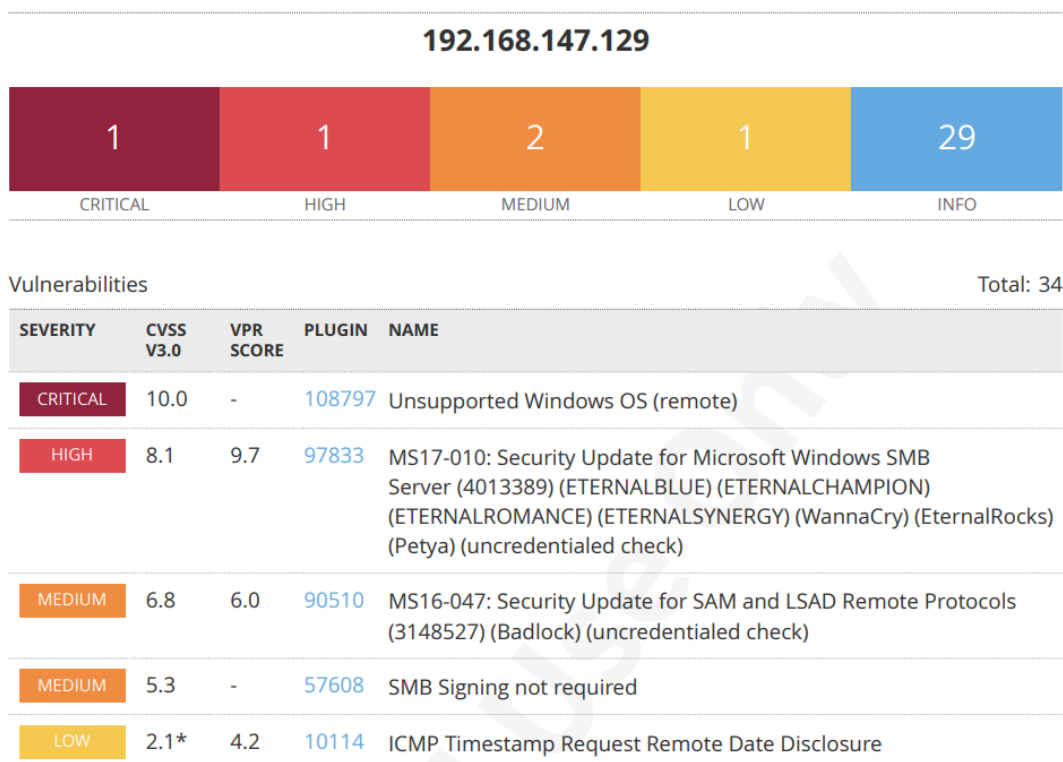
2. SMB Signing not required

- **Severity:** Medium
- **CVSS V3.0:** 5.3
- **Plugin:** 57608
- **Description:** SMB signing is not required on the server, which can allow man-in-the-middle attacks.
- **Impact:** Moderate risk of data interception and session hijacking.

Low Vulnerability

● ICMP Timestamp Request Remote Date Disclosure

- **Severity:** Low
- **CVSS V3.0:** 2.1
- **VPR Score:** 4.2
- **Plugin:** 10114
- **Description:** The system responds to ICMP timestamp requests, potentially disclosing the system's time.
- **Impact:** Low risk of information disclosure that can be used in further attacks.



Remediation Recommendations

Unsupported Windows OS (remote)

- **Recommendation:** Upgrade the operating system to a supported version that receives regular security updates. This will mitigate numerous vulnerabilities and improve overall security.

MS17-010: Security Update for Microsoft Windows SMB Server

- **Recommendation:** Apply the MS17-010 security patch immediately. Ensure that SMBv1 is disabled if not required and consider implementing network segmentation to limit exposure.

MS16-047: Security Update for SAM and LSAD Remote Protocols (Badlock)

- **Recommendation:** Apply the MS16-047 security update to patch the vulnerability. Regularly update all security patches to minimize the risk of exploitation.

SMB Signing not required

- **Recommendation:** Configure the server to require SMB signing. This can be done through Group Policy or directly on the server settings.

ICMP Timestamp Request Remote Date Disclosure

- **Recommendation:** Configure the system to ignore ICMP timestamp requests. This can typically be done through firewall rules or system settings.

Conclusion

The scan reveals several critical and high vulnerabilities that need immediate attention. Upgrading the operating system and applying security patches are crucial steps to mitigate these risks. Implementing recommended configurations will further enhance the security posture of the system. Regular vulnerability assessments and timely updates are essential for maintaining a secure environment.