

Vulnerability Assessment Report

Ibrahim Gaber

Part A: LAN Description

I. LAN Design

The virtual LAN is configured on a host machine using VirtualBox, consisting of two virtual machines:

- **Host Machine:** A physical laptop running VirtualBox (OS: Linux Ubuntu).
- **Virtual Machines (VMs):**
 - Kali Linux (Nessus Machine)
 - Windows 7 (Target)

Network Configuration

- **Network Adapter:** NAT Network (isolated subnet: 192.168.56.0/24).
- **IP Addresses:**

Device	IP Address
Kali Linux	192.168.56.4
Windows 7	192.168.56.5

Table 1: Static IP Assignment

Network Diagram

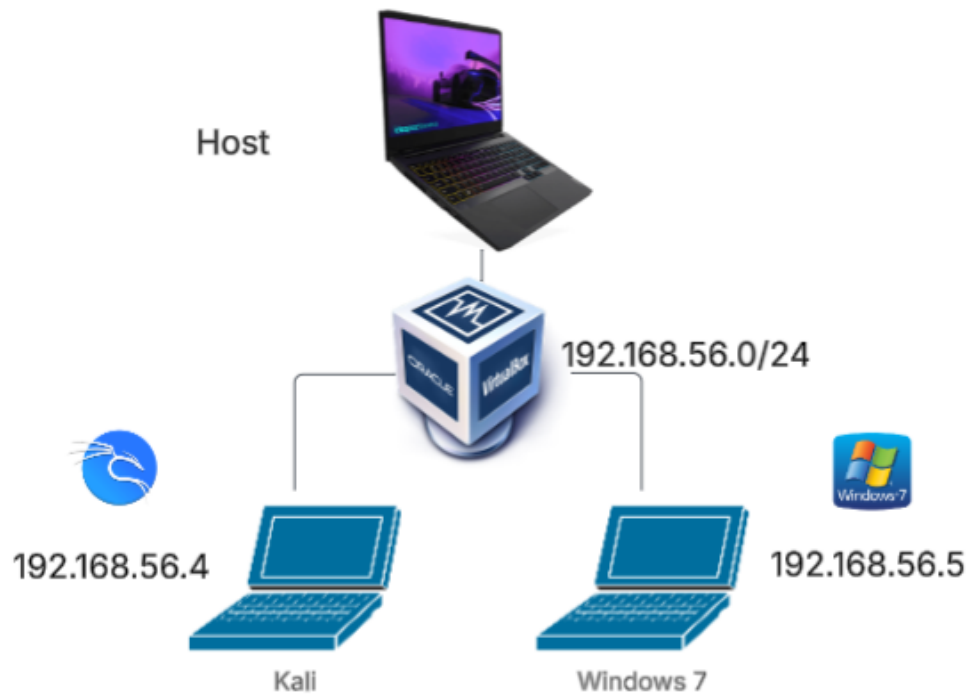


Figure 1: Virtual LAN Setup in VirtualBox

II. Connectivity Verification

To verify bidirectional network connectivity between Kali Linux and Windows 7, we conducted the following tests:

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.4 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::3d68:4a38:177d:830d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 923 (923.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 4070 (3.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(a) Kali Linux Network Configuration

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::bda1:3a75:58e:c206%11
IPv4 Address. . . . . : 192.168.56.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.56.1
```

(b) Windows 7 Network Configuration

```
(kali@kali)~$ ping 192.168.56.5 -c 4
PING 192.168.56.5 (192.168.56.5) 56(84) bytes of data:
64 bytes from 192.168.56.5: icmp_seq=1 ttl=128 time=0.519 ms
64 bytes from 192.168.56.5: icmp_seq=2 ttl=128 time=0.381 ms
64 bytes from 192.168.56.5: icmp_seq=3 ttl=128 time=0.485 ms
64 bytes from 192.168.56.5: icmp_seq=4 ttl=128 time=0.361 ms
--- 192.168.56.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.361/0.436/0.519/0.066 ms
```

(c) Ping Results from Kali to Windows

```
C:\Users\ vboxuser>ping 192.168.56.4
Pinging 192.168.56.4 with 32 bytes of data:
Reply from 192.168.56.4: bytes=32 time<1ms TTL=64
Reply from 192.168.56.4: bytes=32 time<1ms TTL=64
Reply from 192.168.56.4: bytes=32 time<1ms TTL=64
Reply from 192.168.56.4: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.56.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(d) Ping Results from Windows to Kali

Figure 2: LAN Connectivity Verification

(a) Kali Linux IP configuration (b) Windows 7 IP configuration

(c) Successful ping from Kali to Windows7 (d) Successful ping from Windows7 to Kali

The verification process confirms:

- Proper IP address assignment on both machines (Figures 2a and 2b)
- Bidirectional network connectivity through successful ICMP echo requests (Figures 2c and 2d)
- Subnet consistency with identical network masks (255.255.255.0)

This comprehensive validation ensures both systems operate on the same virtual LAN segment with functional network communication.

Part A: Vulnerability Scanning Tool Description

II. Choice of Vulnerability Scanning Tool

The chosen tool for this assessment is **Nessus** (Essentials version). Here are the reasons why I chose Nessus over OpenVAS:

- **Comprehensive Vulnerability Database:** Nessus maintains one of the largest vulnerability databases, with over 100,000 plugins updated daily. This ensures detection of even legacy vulnerabilities in older systems like Windows XP and 7, which are common targets for exploits such as **MS08-067** and **EternalBlue**.
- **User-Friendly Interface:** Nessus provides an intuitive web-based dashboard for configuring scans, analyzing results, and generating reports (see Figure 3). This is critical for beginners to navigate complex vulnerability data efficiently.
- **Customizable Scans:** The tool allows tailored scans (e.g., basic network scans, credentialed patch audits), which aligns with the need to analyze both unsecured (Windows XP) and semi-modern (Windows 7) systems in the LAN.
- **CVSS Integration:** Nessus automatically assigns Common Vulnerability Scoring System (CVSS) ratings and maps vulnerabilities to CVE IDs, simplifying risk prioritization and remediation planning.
- **Industry Recognition:** Widely adopted in cybersecurity professions, Nessus ensures the findings are relevant to real-world organizational environments, fulfilling Learning Outcome (b).

Alternatives Considered

While OpenVAS is a free alternative, it lacks Nessus' frequent plugin updates and streamlined reporting. For time-constrained academic projects, Nessus Essentials strikes the best balance between functionality and accessibility.

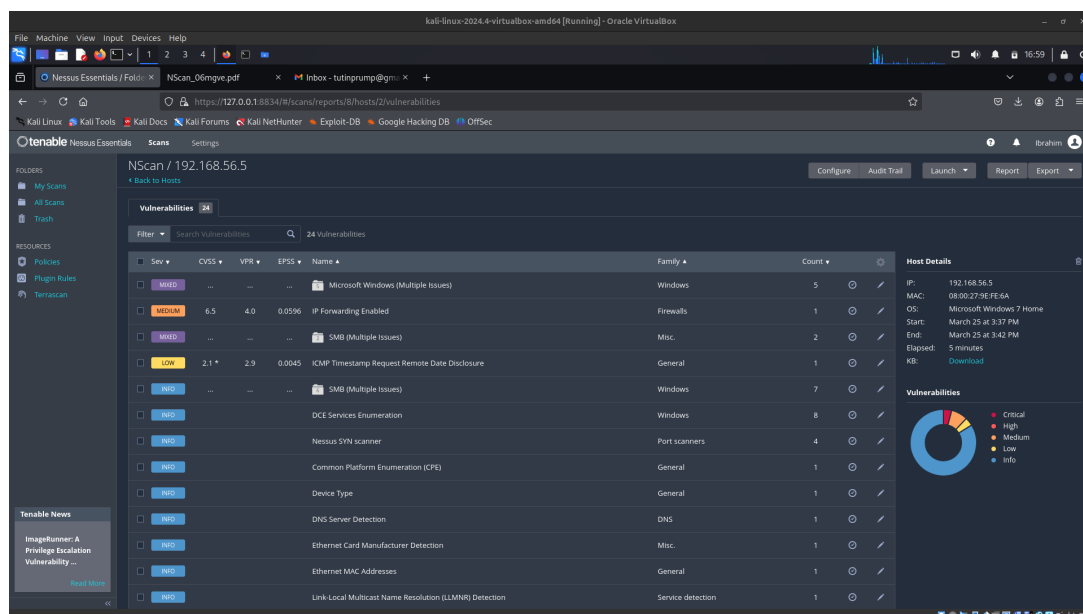
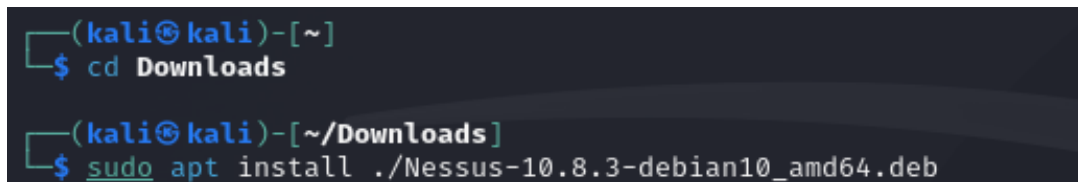


Figure 3: Nessus Web Interface Showing Scan Results

Verify Checksum to check the integrity of the file:

```
echo "SHA256_CHECKSUM_HERE Nessus-10.8.3-debian10_amd64.deb" > sha256sum_nessus
sha256sum -c sha256sum_nessus
```

Install Nessus: Change your working directory to where the downloaded package is located and install it. See Figure 4 for the terminal commands:



```
(kali㉿kali)-[~]
$ cd Downloads

(kali㉿kali)-[~/Downloads]
$ sudo apt install ./Nessus-10.8.3-debian10_amd64.deb
```

Figure 4: Changing Directory and Installing Nessus

Start the Service: Run the command to start Nessus, as shown in Figure 5:



```
(kali㉿kali)-[~]
$ sudo systemctl start nessusd.service
```

Figure 5: Starting the Nessus Service

Access Web Interface:

- Open <https://127.0.0.1:8834> in a browser.
- Bypass SSL warnings using **Advanced** ☐ **Accept Risk**. Then click **Register Offline** and **Continue** (Figure 6).

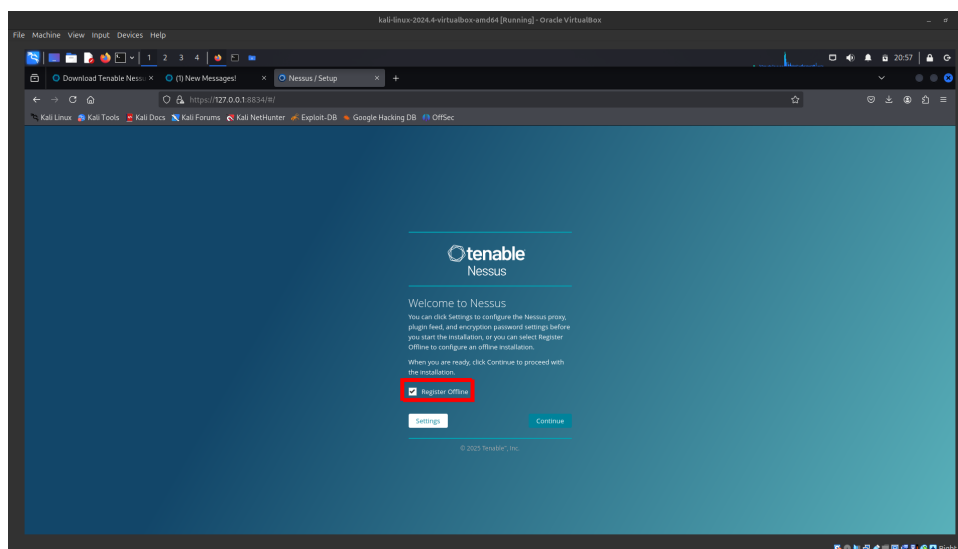


Figure 6: Register Offline and Continue

Activation:

- After clicking **Register Offline**, copy the challenge code displayed on the web interface.
- Visit [Tenable Education](#) and paste the challenge code to obtain your license.
- Enter the license key and click **Continue** (Figure 7).
- Update components manually (Figure 8).

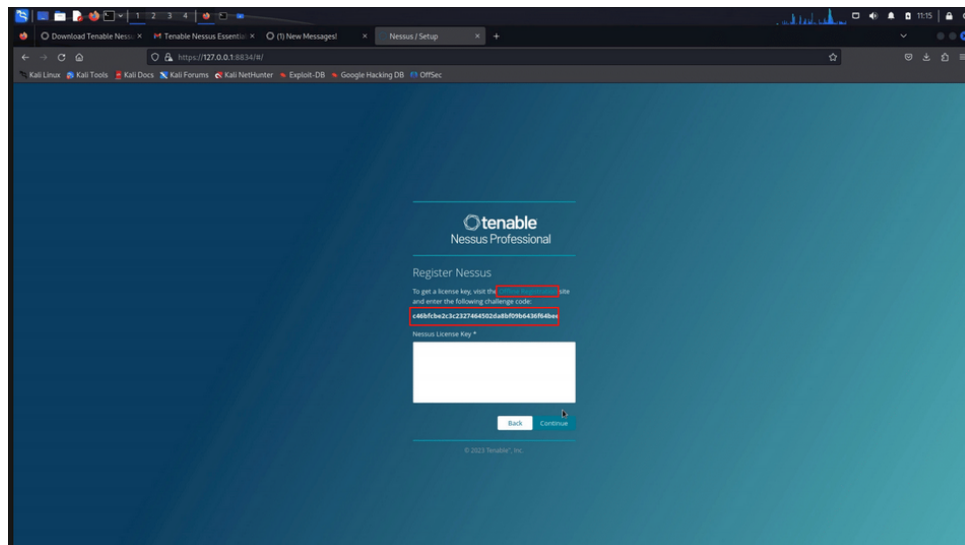


Figure 7: Nessus Activation Process

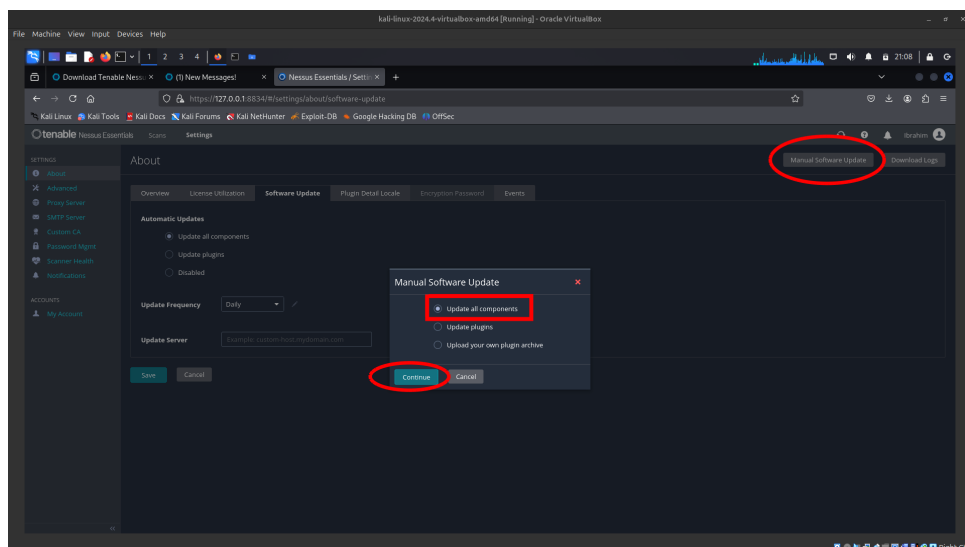


Figure 8: Manual Component Update

Software Update:

- Go to **Settings** → **Software Update** in the Nessus web interface.
- Ensure all components are up-to-date.

Part B: Working with Vulnerability Scanning Tool

This section details the process of identifying devices on the network, analyzing vulnerabilities, and proposing remediation measures. The aim is to provide a comprehensive overview of the scanning process and a detailed discussion of the identified issues.

I. Identifying Devices on the Network

A thorough network scan was conducted using Nessus to identify all active devices on the virtual LAN. The primary focus was on the Windows 7 machine with IP address **192.168.56.5**, which is the designated target for vulnerability assessment. During the scan, Nessus detected a total of **34**

vulnerabilities on this host. These vulnerabilities were automatically categorized by Nessus into different severity levels, as follows:

- 2 Critical
- 1 High
- 3 Medium
- 1 Low
- 27 Informational

This detailed categorization helped to pinpoint which issues require immediate attention versus those that are less likely to be exploited. The use of Nessus not only simplified the detection process but also provided an intuitive interface to review and analyze the results. The following figure illustrates the network scan results:

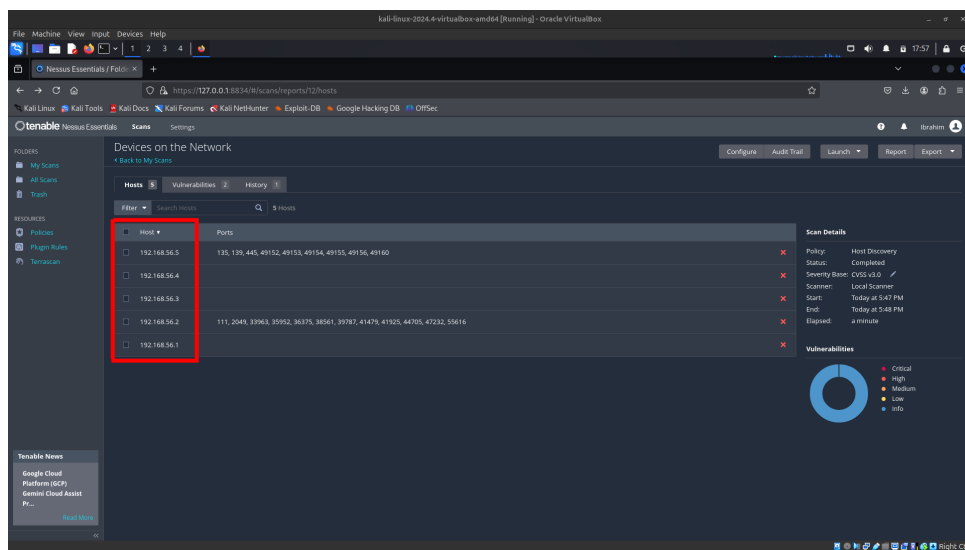


Figure 9: Network Scan Results

II. Identified Vulnerabilities

After completing the network scan, a set of key vulnerabilities were identified. These vulnerabilities have been organized in a table that lists each issue along with its CVSS score, severity, a brief description, and the potential impact on the network. The table below summarizes these critical findings:

ID / Bulletin	CVSS v3.0 / Severity	Description	Impact
Unsupported Windows OS (Plugin 108797)	10.0 / Critical	Windows 7 is no longer supported and is missing critical patches.	Elevated risk of remote exploitation due to unpatched vulnerabilities.
DNS Resolution RCE (MS11-030, Plugin 53514)	10.0 / Critical	Vulnerability in DNS Resolution could allow remote code execution (2509553) (remote check).	Remote Code Execution via Network-Service account.
MS17-010 (Plugin 97833)	8.1 / High	Security update for Microsoft Windows SMB Server (4013389) covering ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, ETernalsYNERGY, WannaCry, EternalRocks, Petya (unauthenticated check).	Potential remote code execution and data leakage.
SAM/LSAD (MS16-047) (Plugin 90510)	6.8 / Medium	Security update for SAM and LSAD Remote Protocol (3148527) (Badlock) (unauthenticated check).	Privilege escalation (local or remote).
IP Forwarding Enabled (Plugin 50686)	6.5 / Medium	System is configured to forward IP packets, which could allow internal traffic snooping.	Could facilitate man-in-the-middle or traffic diversion attacks.
SMB Signing Not Required (Plugin 57608)	5.3 / Medium	SMB traffic is not digitally signed, increasing risk of tampering or session hijacking.	Potential for replay or impersonation attacks.
ICMP Timestamp Disclosure (Plugin 10114)	2.1 / Low	System responds to ICMP timestamp requests, revealing system uptime.	Minor info leak that can aid in fingerprinting.

Table 2: Selected Vulnerabilities Identified by Nessus (Total: 34)

The table provides a concise summary, but further details about each vulnerability are discussed in the following sections.

III. Severity Profiles of Vulnerabilities

Nessus automatically assigned severity levels based on the CVSS v3.0 scoring system. The classification is as follows:

- **Critical (CVSS 9.0+):** Issues such as Unsupported Windows OS and DNS Resolution RCE are deemed critical due to their high potential for exploitation.
- **High (CVSS 7.0–8.9):** MS17-010 falls into this category given its association with major exploits like EternalBlue.
- **Medium (CVSS 4.0–6.9):** Vulnerabilities such as SAM/LSAD (MS16-047) and IP Forwarding Enabled are of moderate concern.
- **Low (CVSS 0.1–3.9):** Issues like SMB Signing Not Required and ICMP Timestamp Disclosure, while less severe, still represent potential risks.

The attached figure illustrates the distribution of these vulnerabilities and highlights the overall risk landscape.

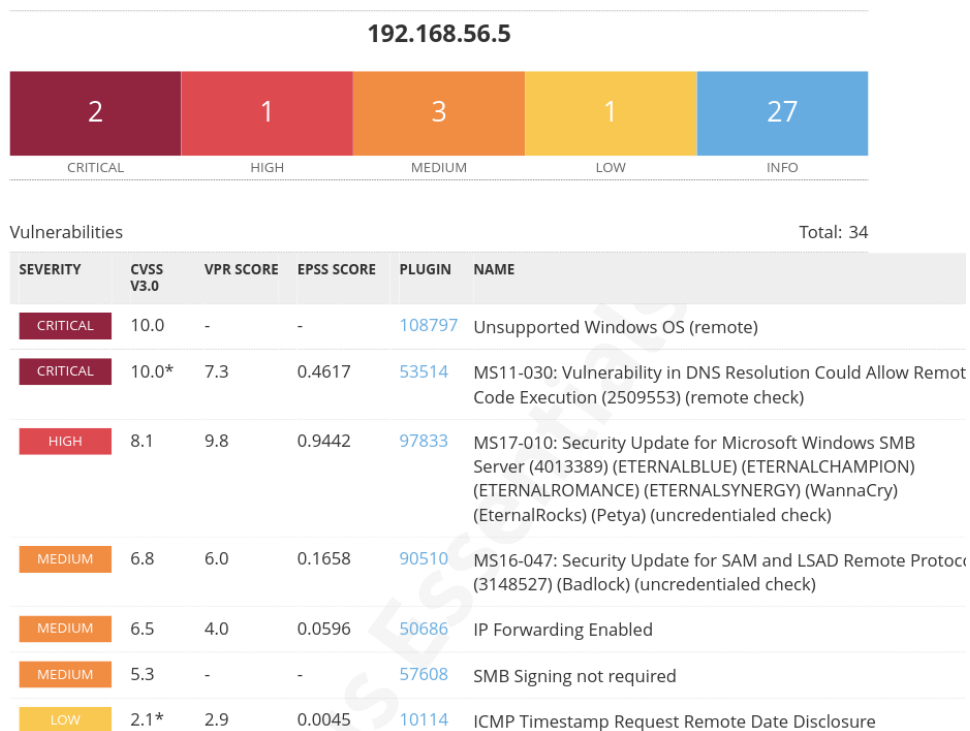


Figure 10: Nessus Report Showing Severity Distribution

IV. Ranking of Vulnerabilities by Impact

To prioritize remediation efforts, the vulnerabilities were ranked based on their exploitability and potential damage. The ranking is as follows:

1. **DNS Resolution RCE (MS11-030)** – With a CVSS of 10.0, this vulnerability poses the highest risk as it can enable remote code execution.
2. **Unsupported Windows OS** – Also scoring 10.0, this issue represents an extreme risk due to the lack of security patches.
3. **MS17-010 (EternalBlue)** – With a CVSS of 8.1, this vulnerability could lead to data leakage and remote code execution.
4. **SAM/LSAD (MS16-047)** – At a medium risk level (CVSS 6.8), this vulnerability could allow privilege escalation.
5. **IP Forwarding Enabled** – Scoring 6.5, it represents a moderate risk by potentially enabling man-in-the-middle attacks.

V. Top 5 Critical Vulnerabilities

Although only two vulnerabilities are strictly “Critical” (scoring 9.0 or higher), the top five vulnerabilities, when considering overall impact, include a mix of critical, high, and medium risks:

1. **DNS Resolution RCE (MS11-030)** – Critical
2. **Unsupported Windows OS** – Critical
3. **MS17-010 (EternalBlue)** – High
4. **SAM/LSAD (MS16-047)** – Medium
5. **IP Forwarding Enabled** – Medium

This ranking guides the prioritization for remediation efforts, ensuring that the most exploitable vulnerabilities are addressed first.

VI. Recommended Remediation Solutions

Based on the analysis, several remediation steps are recommended:

- **Apply Patches/Updates:** Ensure all critical Windows updates are installed, especially for vulnerabilities such as MS11-030, MS17-010, and MS16-047. Migrating from Windows 7 to a supported operating system is strongly advised to mitigate the risk of exploitation.
- **Disable or Restrict SMBv1:** Mitigate the risk associated with MS17-010 by disabling SMBv1 or configuring the firewall to block traffic on TCP port 445.
- **Restrict IP Forwarding:** Disable IP forwarding unless it is absolutely necessary, thereby reducing the risk of internal traffic snooping and man-in-the-middle attacks.
- **Enforce SMB Signing:** Enabling SMB signing can help prevent tampering or session hijacking, enhancing overall network security.
- **Regular Updates:** Regularly update vulnerability scanning tools like Nessus to ensure that emerging threats are promptly identified.

In summary, this section provides a detailed walkthrough of the vulnerability scanning process, from identifying devices and vulnerabilities to analyzing their severity and impact. The recommendations offered here are aimed at mitigating the highest risks and ensuring the security of the network environment. Continuous monitoring and periodic scanning are essential to maintaining a robust security posture.