

Vulnerability Assessment Report

Date of Assessment: November 14, 2025

Scope: Comprehensive Vulnerability Assessment of Metasploitable 2 and Windows 7 Targets in an Isolated Test Environment.

Team: Adejuwonlo Adeola, Ogunsola Feyisola, Paul Yohanna, Dennis Isreal

Assets:

- I. **Metasploitable 2:** 192.168.98.128 (Linux-based)
- II. **Windows 7 Professional:** 192.168.98.129 (Legacy Microsoft OS)
- III. **Ubuntu** (Test Environment)

1. Executive Summary

This report outlines the critical findings from a comprehensive vulnerability assessment conducted on two isolated internal test systems. The assessment utilized the industry-leading scanning tools **Tenable Nessus**.

The overall security posture of both targets is rated as **Critical**. The findings highlight severe, unmitigated risks that would lead to immediate remote code execution (RCE) and system compromise if these assets were deployed in a production environment and require immediate and mandatory action to address and eliminate

2. Metasploitable 2 Assessment (192.168.98.128)

Vulnerabilities 22

CRITICAL Unsupported Windows OS (remote)

Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a supported service pack or operating system

See Also
<https://support.microsoft.com/en-us/lifecycle>

Output
The following Windows version is installed and not supported:
Microsoft Windows 7 Professional

To see debug logs, please visit individual host

Port	Hosts
N/A	192.168.98.129

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:U/N:S/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Unsupported by vendor: true

2.1 Virtual Machine Setup, Installation, and Network Discovery

Virtual Machine Installation: The Metasploitable 2 operating system was installed as a virtual machine (VM) using a standard hypervisor (e.g., VirtualBox or VMware). This system is a deliberately vulnerable Linux distribution designed to train security professionals. For security and control, the VM was configured to operate within a strictly isolated, internal virtual network segment.

Network Configuration for Scanning: Crucially, the Ubuntu scanning machine and the Metasploitable 2 target VM were configured to share the same Host-Only or NAT Network virtual segment (i.e., the 192.168.98.0/24 subnet). This ensures Layer 2/3 connectivity between the scanner and the target, which is essential for successful host discovery and active scanning.

IP Address Discovery: The IP address of the Metasploitable 2 VM (192.168.98.128) was determined using the fping utility from the Ubuntu scanning platform. fping is a high-performance tool used to send parallel ICMP echo requests across a defined range of IP addresses, quickly identifying live hosts available on the local subnet.

Command Used (Ubuntu Terminal):

Using fping to scan the entire C-class subnet for live hosts.

```
$ fping -a -g 192.168.98.0/24
```

The successful execution of this command returned the active host at **192.168.98.128**.

2.2 Nessus Essentials Installation and Scan Procedure

Installation Method (Ubuntu Terminal): The Nessus Essentials scanner was installed directly on the Ubuntu machine. This involved downloading the official Debian package (.deb) and managing the service via the system's package manager and systemctl.

The screenshot shows the Nessus interface with a single vulnerability entry. The title is "Unsupported Windows OS (remote)".

Description: The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution: Upgrade to a supported service pack or operating system.

See Also: <https://support.microsoft.com/en-us/lifecycle>

Output: The following Windows version is installed and not supported: Microsoft Windows 7 Professional

To see debug logs, please visit individual host

Port	Hosts
N/A	192.168.98.129

Plugin Details:

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information:

CVSS v3.0 Base Score:	10.0
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/U:U/N:S/C:H/I:H/A:H
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS:2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information:

CPE:	cpe:/o:microsoft:windows
Unsupported by vendor:	true

- Install required packages

```
$ sudo apt update
```

```
$ sudo apt install -y curl
```

- Install the Nessus package using dpkg

```
$ sudo dpkg -i Nessus-[version_and_arch].deb
```

- Start the Nessus service to begin initialization

```
$ sudo /bin/systemctl start nessusd.service
```

Nessus Scan Initiation and Review:

- Access UI:** We navigated to the Nessus web interface URL: <https://127.0.0.1:8834>.
- Start Scan:** From the main dashboard, the "**New Scan**" button was clicked to initiate the wizard.
- Select Policy:** The "**Basic Network Scan**" template was selected. This comprehensive, unauthenticated scan profile is sufficient for identifying network-accessible services and common vulnerabilities.
- Configure Target:** Under the "Settings" section, a name ("Metasploitable 2 Scan") was provided, and the target IP address was meticulously entered into the "Targets" field: **192.168.98.128**.
- Launch and Monitor:** The configuration was saved, and the scan was initiated by clicking "**Launch**". Scan progress was tracked on the "**My Scans**" page.
- Review Report:** Upon completion (Status: "**Completed**"), the scan entry was opened. The "**Vulnerabilities**" tab provided a categorized breakdown of the 67 detected flaws, categorized by severity (Critical, High, Medium, etc.) .

Vulnerabilities 22

CRITICAL Unsupported Windows OS (remote)

Description	Plugin Details
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	Severity: Critical ID: 108797 Version: 1.16 Type: remote Family: Windows Published: April 3, 2018 Modified: October 21, 2025
Solution Upgrade to a supported service pack or operating system	Risk Information Risk Factor: Critical CVSS v3.0 Base Score: 10.0 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:C:H/I:H/A:H CVSS v2.0 Base Score: 10.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
See Also https://support.microsoft.com/en-us/lifecycle	Vulnerability Information CPE: cpe:/o:microsoft:windows Unsupported by vendor: true
Output The following Windows version is installed and not supported: Microsoft Windows 7 Professional	
To see debug logs, please visit individual host	
Port ▾	Hosts
N/A	192.168.98.129

2.3 Vulnerabilities and Mitigation Analysis (Metasploitable 2)

Fig 1.1

Vulnerability: UnrealIRCd Backdoor Detection

Severity CVSS v3.0: CRITICAL 10.0

The screenshot shows a web-based interface for viewing a specific vulnerability. At the top, there's a red button labeled 'CRITICAL' and the title 'UnrealIRCd Backdoor Detection'. Below the title, there are sections for 'Description', 'Solution', 'See Also', 'Output', and 'Plugin Details'. The 'Description' section states: 'The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.' The 'Solution' section advises: 'Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.' The 'See Also' section lists three URLs: <https://seclists.org/fulldisclosure/2010/Jun/277>, <https://seclists.org/fulldisclosure/2010/Jun/284>, and <http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>. The 'Output' section contains a terminal-like window showing the command 'uid=0(root) gid=0(root)' and the text 'The remote IRC server is running as :'. On the right side, there's a 'Plugin Details' panel with fields like Severity: Critical, ID: 46882, Version: 1.16, Type: remote, Family: Backdoors, Published: June 14, 2010, and Modified: April 11, 2022. Below the 'Plugin Details' is a 'Risk Information' section with Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Temporal Score: 8.3, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C, and CVSS v2.0 Temporal Vector: CVSS2#E:R/L:O/R/C:C.

Description and Impact: This is a highly critical flaw where the running UnrealIRC daemon (version 1.16 was detected) contains a deliberate backdoor (CVE-2010-2072). An unauthenticated attacker can execute arbitrary code on the system with the privileges of the service account, which, on this system, is often root.

Mitigation Strategy Immediate Service Removal: The UnrealIRCd package must be immediately uninstalled using the package manager (apt-get purge unrealircd). If IRC functionality is absolutely required, a different, verifiable, and modern IRC daemon should be installed, configured securely, and kept rigorously patched.

Fig 1.2

The screenshot shows another web-based vulnerability details page. At the top, there's a red button labeled 'CRITICAL' and the title 'Unsupported Windows OS (remote)'. Below the title, there are sections for 'Description', 'Solution', 'See Also', 'Output', and 'Plugin Details'. The 'Description' section states: 'The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.' The 'Solution' section advises: 'Upgrade to a supported service pack or operating system.' The 'See Also' section lists a URL: <https://support.microsoft.com/en-us/lifecycle>. The 'Output' section contains a terminal-like window showing the message 'The following Windows version is installed and not supported: Microsoft Windows 7 Professional'. On the right side, there's a 'Plugin Details' panel with fields like Severity: Critical, ID: 108797, Version: 1.16, Type: remote, Family: Windows, Published: April 3, 2018, and Modified: October 21, 2025. Below the 'Plugin Details' is a 'Risk Information' section with Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS3.0/AV:N/AC:L/PR:N/U:N/S:C:H/I:H/A:H, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C. There are also 'Vulnerability Information' and 'CPE' sections at the bottom.

Vulnerability: VNC Server 'password' Password

Severity CVSS v3.0: CRITICAL 10.0

The screenshot shows a Nessus scan report for a host with IP 192.168.98.128. The report details a critical vulnerability related to the VNC server password.

Plugin Details:

Severity:	Critical
ID:	61708
Version:	\$Revision: 1.2 \$
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015

Risk Information:

Risk Factor:	Critical
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information:

Default Account:	true
Exploited by Nessus:	true

Description: The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution: Secure the VNC service with a strong password.

Output:

```
Nessus logged in using a password of "password".  
To see debug logs, please visit individual host  
Port ▾ Hosts  
5900 / tcp / vnc 192.168.98.128
```

Description and Impact: The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Mitigation Strategy: The VNC server password must be changed from the default/weak 'password' to a complex, unique password adhering to a strong password policy (minimum 16 characters, including mixed case, numbers, and symbols).

Fig 1.3

Vulnerability: SSL Version 2 and 3 Protocol Detection

Severity CVSS v3.0: CRITICAL 9.8

The screenshot shows a Nessus scan report for a host with IP 192.168.98.128. The report details a critical vulnerability related to unsupported Windows OS.

Plugin Details:

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information:

Risk Factor:	Critical
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS3.0/AV:N/AC:L/PR:N/U:N/S:C:H/I:H/A:H

Vulnerability Information:

CPE:	cpe:/o:microsoft:windows
Unsupported by vendor:	true

Description: The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution: Upgrade to a supported service pack or operating system.

See Also: <https://support.microsoft.com/en-us/lifecycle>

Output:

```
The following Windows version is installed and not supported:  
Microsoft Windows 7 Professional  
To see debug logs, please visit individual host  
Port ▾ Hosts  
N/A 192.168.98.129
```

CRITICAL SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

Plugin Details

Severity:	Critical
ID:	20007
Version:	1.34
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	April 4, 2022

Risk Information

Risk Factor:	Critical
CVSS v3.0 Base Score:	9.8
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Description and Impact: Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

Mitigation Strategy: Eliminate the vulnerable protocols entirely. Disable Weak Protocols: Configure all server-side services (e.g., Apache, Nginx, or any service exposing these protocols) to explicitly disable support for SSLv2 and SSLv3. The system should be mandated to use only modern, secure versions of the protocol, such as TLS 1.2 and TLS 1.3.

Fig 1.4

Vulnerability: rlogin Service Detection

Severity CVSS v3.0: **HIGH 7.5**

Vulnerabilities 22

CRITICAL Unsupported Windows OS (remote)

Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a supported service pack or operating system

See Also
<https://support.microsoft.com/en-us/lifecycle>

Output
The following Windows version is installed and not supported:
Microsoft Windows 7 Professional

To see debug logs, please visit individual host

Port	Hosts
N/A	192.168.98.129

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information

Risk Factor:	Critical
CVSS v3.0 Base Score:	10.0
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE:	cpe:/o:microsoft:windows
	Unsupported by vendor: true

HIGH rlogin Service Detection

Description
The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution
Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▾	Hosts
513 / tcp / rlogin	192.168.98.128

Plugin Details

Severity:	High
ID:	10205
Version:	1.36
Type:	remote
Family:	Service detection
Published:	August 30, 1999
Modified:	April 11, 2022

Risk Information

Risk Factor:	High
CVSS v2.0 Base Score:	7.5
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Exploit Available:	true
Exploit Ease:	Exploits are available
Vulnerability Pub Date:	January 1, 1990

Exploitable With

Metasploit (rlogin Authentication Scanner)
--

Description and Impact: The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Mitigation Strategy: Immediately disable and remove the rlogin service from the host using the package manager. Replace rlogin with Secure Shell (SSH) for all remote command line access. SSH encrypts all session data, including credentials, protecting against sniffing and man-in-the-middle attacks.

CRITICAL Unsupported Windows OS (remote)

Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a supported service pack or operating system

See Also
<https://support.microsoft.com/en-us/lifecycle>

Output

```
The following Windows version is installed and not supported:  
Microsoft Windows 7 Professional
```

To see debug logs, please visit individual host

Port ▾	Hosts
N/A	192.168.98.129

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information

Risk Factor:	Critical
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/U:U/N:S:C:H/I:H/A:H
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE:	cpe:/o:microsoft:windows
Unsupported by vendor:	true

3. Windows 7 Assessment (192.168.98.129)

3.1 Virtual Machine Setup, Installation, and Network Discovery

Virtual Machine Installation: The Windows 7 Professional VM was installed using a legacy image. Like the Metasploitable 2 system, it was configured on the same isolated virtual network segment to ensure the Ubuntu scanner could reach it. This configuration isolates the unsupported OS from the company's production network.

IP Address Discovery: The IP address of the Windows 7 VM (192.168.98.129) was identified using the netdiscover utility on the Ubuntu scanning machine. netdiscover operates by sending out ARP requests and passively sniffing the local network traffic to map active hosts, which is highly effective for discovering targets on a local subnet.

Command Used (Ubuntu Terminal):

Scanning the network interface for active hosts using netdiscover

```
$ sudo netdiscover -r 192.168.98.0/24
```

This command successfully identified the active host corresponding to the Windows 7 VM at **192.168.98.129**.

3.2 Scanning Tools Installation and Detailed Usage Procedures

The installation and access methods for Nessus and OpenVAS were identical to those described in Section 2.2. The only variable changed was the target IP address in the scan configuration interfaces.

Nessus Target Configuration: 192.168.98.129

3.3 Vulnerabilities and Mitigation Analysis (Windows 7)

Fig 2.1

The screenshot shows a Microsoft security advisory page. At the top, there is a navigation bar with links for 'Vulnerabilities' (22), 'CRITICAL', and 'Unsupported Windows OS (remote)'. Below the navigation bar, there is a 'Description' section stating: 'The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.' There is also a 'Solution' section suggesting: 'Upgrade to a supported service pack or operating system'. A 'See Also' link points to <https://support.microsoft.com/en-us/lifecycle>. In the bottom left, there is an 'Output' section with the text: 'The following Windows version is installed and not supported: Microsoft Windows 7 Professional'. In the bottom right, there is a 'Risk Information' section with the following details:
Risk Factor: Critical
CVSS v3.0 Base Score: 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:U/N:S/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability: Unsupported Windows OS (remote)

Severity CVSS v3.0: CRITICAL 10.0

Description and Impact: The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Mitigation Strategy: Due to the End-of-Life (EOL) status, the Windows 7 Professional operating system no longer receives security updates or vendor support from Microsoft. This system presents an unmitigable risk and must be immediately removed from the network and decommissioned.

Fig 2.2

Vulnerability: MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Severity CVSS v3.0: CRITICAL 10.0*

The screenshot shows a Nessus scan report for the vulnerability MS11-030. The report includes sections for Plugin Details, Risk Information, and Vulnerability Information. Key details from the report include:

- Plugin Details:** Severity: Critical, ID: 53514, Version: 1.19, Type: remote, Family: Windows, Published: April 21, 2011, Modified: October 17, 2023.
- Risk Information:** Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Temporal Score: 8.3, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C, CVSS v2.0 Temporal Vector: CVSS2#E:FR/L:OF/RC:I, IAVM Severity: I.
- Vulnerability Information:** CPE: cpe:/o:microsoft:windows, Exploit Available: true, Exploit Ease: Exploits are available, Patch Pub Date: April 12, 2011, Vulnerability Pub Date: April 12, 2011.

Description and Impact: A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Mitigation Strategy: Install the Microsoft Security Update MS11-030 (KB2509553). If patching

The screenshot shows a Microsoft Support Lifecycle page for Windows 7. The page indicates that the Windows 7 Professional version is installed and not supported. It provides mitigation steps and links to Microsoft documentation. Key details from the page include:

- Description:** The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.
- Solution:** Upgrade to a supported service pack or operating system.
- See Also:** <https://support.microsoft.com/en-us/lifecycle>
- Output:** The following Windows version is installed and not supported: Microsoft Windows 7 Professional.
- Hosts:** Port: 5355 / udp / llmnr, Hosts: 192.168.98.129.
- Risk Information:** Risk Factor: Critical, CVSS v3.0 Base Score: 10.0, CVSS v3.0 Vector: CVSS3.0/AV:N/AC:L/Au:N/C:H/I:H/A:H, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C.
- Vulnerability Information:** CPE: cpe:/o:microsoft:windows, Unsupported by vendor: true.

is not an immediate option, disable the Link-Local Multicast Name Resolution (LLMNR) protocol via Group Policy or local registry settings to prevent the exploitation of this client-side vulnerability.

Fig 2.3

Vulnerability: MS17-010: Security Update for Microsoft Windows SMB Server (4013389)

Severity CVSS v3.0: HIGH 8.1

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNA...)		Plugin Details
Description The remote Windows host is affected by the following vulnerabilities : <ul style="list-style-type: none"> - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147) <p>ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.</p>		Severity: High ID: 97833 Version: 1.30 Type: remote Family: Windows Published: March 20, 2017 Modified: May 25, 2022
Solution Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.		Risk Information Risk Factor: High CVSS v3.0 Base Score: 8.1 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/Ui:N/S:U/C:H/I:H/A:H CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:0/RC:C CVSS v3.0 Temporal Score: 7.7 CVSS v2.0 Base Score: 9.3 CVSS v2.0 Temporal Score: 8.1 CVSS v2.0 Vector: CVSS:2.0/AV:N/AC:M/Au:N/C:C/I:C/A:C CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:0/RC:C IAVM Severity: I
See Also http://www.nessus.org/u?68fc8eff http://www.nessus.org/u?321523eb http://www.nessus.org/u?045561dn		Vulnerability Information

Description and Impact: Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

Mitigation Strategy: Install the Microsoft Security Update MS17-010 (KB4013389)

CRITICAL Unsupported Windows OS (remote)		Plugin Details				
Description The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.		Severity: Critical ID: 108797 Version: 1.16 Type: remote Family: Windows Published: April 3, 2018 Modified: October 21, 2025				
Solution Upgrade to a supported service pack or operating system		Risk Information Risk Factor: Critical CVSS v3.0 Base Score: 10.0 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/Ui:N/S:C:H/I:H/A:H CVSS v2.0 Base Score: 10.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C				
See Also https://support.microsoft.com/en-us/lifecycle		Vulnerability Information CPE: cpe:/o:microsoft:windows Unsupported by vendor: true				
Output The following Windows version is installed and not supported: Microsoft Windows 7 Professional						
To see debug logs, please visit individual host <table border="1"> <thead> <tr> <th>Port</th> <th>Hosts</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>192.168.98.129</td> </tr> </tbody> </table>		Port	Hosts	N/A	192.168.98.129	
Port	Hosts					
N/A	192.168.98.129					

immediately, and then disable the SMBv1 protocol entirely via registry settings or Group Policy to prevent future exploitation.

4. Conclusion and Strategic Next Steps

The findings of this vulnerability assessment confirm the successful identification of multiple critical flaws across the test infrastructure. The continued existence of an EOL operating system presents the single greatest, unmitigable risk identified.

4.1 Recommended Action Plan and Risk Remediation

The following phased action plan is recommended for immediate implementation:

I. Phase I: Critical and Urgent Remediation

- A. **Windows 7 Decommissioning:** The system at 192.168.98.129 must be removed from the network immediately. If data retrieval is required, place the VM in a temporary quarantine network without network access.
- B. **Insecure Service Mitigation:** Globally disable and/or remove the following cleartext services across all legacy internal devices: rlogin, rexec, Telnet, and FTP.
- C. **SMBv1 Prohibition:** Enforce configuration controls to disable the SMBv1 protocol across all internal network assets to eliminate the MS17-010 (EternalBlue) risk.

II. Phase II: Strategic and Policy Alignment

- A. **OS Lifecycle Policy:** Formalize and strictly enforce a policy that mandates the retirement of operating systems before they reach their official End-of-Life date, ensuring continuous vendor support and patching.
- B. **Secure Protocol Migration:** Mandate the exclusive use of encrypted protocols,

Vulnerabilities 22

CRITICAL Unsupported Windows OS (remote)

Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a supported service pack or operating system

See Also
<https://support.microsoft.com/en-us/lifecycle>

Output
The following Windows version is installed and not supported:
Microsoft Windows 7 Professional

To see debug logs, please visit individual host

Port	Hosts
N/A	192.168.98.129

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:C/H:I/H:A-H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CP: cpe:/o:microsoft:windows
Unsupported by vendor: true

specifically **SSH** and **SFTP**, for all remote administration and file transfer tasks, eliminating the threat of cleartext credential exposure.

- C. **Firewall Hardening Standard:** Integrate controls into the standard build process for all endpoints to block non-essential ports, including **UDP 5355** and other reconnaissance-friendly ports like **TCP 135** (DCE/RPC).

III. Phase III: Vulnerability Management Process Integration

- A. **Scheduled Scanning:** Integrate regular, authenticated vulnerability scans using Nessus and OpenVAS into the SOC's standard operating procedures, running comprehensive scans on all production assets at least monthly.
- B. **Configuration Audit:** Conduct a follow-up audit across the production network to identify and remediate any instances of overly permissive "world readable" file share configurations (NFS, Samba) to enforce the principle of least privilege.

Vulnerabilities 22

CRITICAL Unsupported Windows OS (remote)

Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a supported service pack or operating system

See Also
<https://support.microsoft.com/en-us/lifecycle>

Output
The following Windows version is installed and not supported:
Microsoft Windows 7 Professional

To see debug logs, please visit individual host

Port	Hosts
N/A	192.168.98.129

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:U/N:S/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Unsupported by vendor: true