Executive Summary:

The aim of this vulnerability assessment was to gather details about the top 6 vulnerabilities existing on the 172.16.14.0 Network. From this network, we scanned 3 hosts: the Windows 1 system (172.16.14.50), the Linux system (172.16.14.52), and the Windows Server (172.16.14.53). We used OpenVAS to run a full vulnerability scan on our host as this would give us a thorough look into the vulnerabilities present.
During the scan, a total of 12 unique vulnerabilities were found. There were a mix of critical, high, medium, and low level severity vulnerabilities found across the 3 hosts.
You can find more information about the vulnerabilities below in “Risk Assessment”.

Vulnerability Severity	Count
Critical Severity Vulnerabilities	3
High Severity Vulnerabilities	2
Medium Severity Vulnerabilities	5
Low Severity Vulnerabilities	2

List of Top 6 Vulnerabilities:

Vulnerability	Severity	CVSS Score
Report Outdated/End-of-life Scan Engine/Environment (Local)	Critical	10.0
OS End of Life Detection	Critical	10.0
Microsoft Remote Code Execution Vulnerability	Critical	10.0
HTTP Brute Force Logins With Default Credentials Reporting	High	7.5
Unprotected OSSEC/Wazuh ossec-authd	High	7.5
DCE/RPC and MSRPC Services Enumeration Reporting	Medium	5.0

Many of the vulnerabilities found on the devices were due to the systems running outdated versions of their respective operating systems. There is a critical vulnerability that exists on the Windows Server that could be exploited to cause major damage to the security infrastructure of the company.
My recommendation is to take immediate action to resolve the vulnerabilities (critical and high in particular) by applying relevant security patches and other configuration changes.

Scan Results:

The following results have been ordered to display the top 6 unique vulnerabilities by severity. They are categorized by their CVSSv2 Base Score.

Vulnerability #1

Report Outdated/End-of-life Scan Engine/Environment (Local):
Severity: Critical (10.0 CVSS Base Score)
Status: Resolved
Affected Hosts: Windows 1, Linux machine, and Windows Server
Details of Vulnerability: Warning that OS has reached end of life and may lead to decreased system security

- Missing functionalities
- Missing bug fixes
- Incompatibilities within the feed

Impact: The following vulnerability could lead to a decrease in scan coverage for the system or missed detection of further vulnerabilities

- Complete impact on Confidentiality, Integrity, and Availability of target system

Vulnerability #2

Operating System End of Life Detection
Severity: Critical (10.0 CVSS Base Score)
Status: Resolved
Affected Host: Windows 1
Details of Vulnerability: The Windows 10 version installed on the host has reached the end of life and should not be used anymore. This means that the OS will not receive any more security updates and is now at an increased risk of Cyber attack.
Impact: Unfixed vulnerability may be exploited by attacker to compromise the security of the host

- Complete impact on Confidentiality, Integrity, and Availability of system

Vulnerability #3

Microsoft SMB2 Negotiation Protocol Remote Code Execution Vulnerability
Severity: Critical (10.0 CVSS Base Score)
Status: Resolved
Affected Host: Windows Server
Details of Vulnerability: Exploitation could allow attacker remote code execution if they sent specially crafted SMB packets to a computer running the server service.

- Remote code execution allows attackers to remote execute malicious code on a computer

Impact: Successful exploitation could give attackers remote access to system
Failed exploit attempt would likely cause denial of service conditions

- Complete impact on Confidentiality, Integrity, and Availability of system

Vulnerability #4

HTTP Brute Force Logins With Default Credentials Reporting
Severity: High (7.5 CVSS Base Score)
Status: Mitigation
Affected Host: Linux machine
Details of Vulnerability: Scanner discovered that it was possible to login to the remote web application using default credentials
Impact: Remote attacker could easily gain access to sensitive information or modify system configuration

- Partial impact on Confidentiality, Integrity, and Availability of system

Vulnerability #5

Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)
Severity: High (7.5 CVSS Base Score)
Status: Workaround
Affected Host: Linux machine
Details of Vulnerability: Possible to connect to remote OSSEC/Wazuh ossec-authd service without providing a password or a valid client certificate

- OSSEC is a host-based Intrusion Detection System
- Wazuh is an open source Host and Endpoint Security service

Impact: May be misused by attacker to register arbitrary agents at the remote service or overwrite the registration of existing ones (affecting system's ability to detect intrusion)

- Partial impact on Confidentiality, Integrity, and Availability of system

Vulnerability #6

DCE/RPC and MSRPC Services Enumeration Reporting
Severity: Medium (5.0 CVSS Base Score)
Status: Mitigation
Affected Hosts: Windows 1 and Windows Server
Details of Vulnerability: Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries

- In cyber security, enumeration is essentially gathering information of a target system

Impact: An attacker may used this to gain more knowledge about the remote host

- Could use exploit this vulnerability for reconnaissance to prepare to find an entry to the system network for a more severe attack
- Partial impact on Confidentiality

Methodology:

As we already knew the hosts' IP addresses, there was no need for us to conduct a host discovery scan. However, if we did not already have access to the IP addresses on the network; we could use an Nmap host discovery scan to find this information. In this case, the only scan that we had to conduct was our vulnerability assessment scan. The vulnerability scan was conducted using the Greenbone OpenVAS scanning platform. OpenVAS is a full-featured vulnerability scanner that obtains its tests for detecting vulnerabilities from a feed that has a long history and daily updates. The purpose for using this scanning method was to utilize a straightforward scanner that gives us a detailed look into the vulnerabilities of a target host and an informative database to go with it. The type of scan that I used within OpenVAS was a full and fast scan because that would give me the most informative results about all of the vulnerabilities present on the systems.

Findings:

All 3 of our intended target systems were scanned successfully giving us a thorough list of vulnerabilities to examine. Once again, the systems scanned were the Windows 1 system, the Linux system, and the Windows server. The results of these scans can be found in more detail above in the "Scan Results" section of the report. The successful scans of these machines tells us that they were switched on and working properly. If they were off, the KaliOpenVAS system would not be able to communicate with them and get results for the scans.

Risk Assessment:

Critical Severity	High Severity	Medium Severity	Low Severity
3	2	5	2

The risks identified in the scans are categorized into four different groups according to their likelihood of occurrence and the potential damage that they may cause to the organization if exploited. Below I will go into more details about the types of vulnerability severity levels.

Critical Severity Vulnerability

- Critical vulnerabilities require immediate attention. They signify a threat that is relatively easy for attackers to exploit and may result in major damages to an organization's security infrastructure
- CVSS Score of 9.0-10.0

Example of critical severity vulnerability below:

Vulnerable Target	**Description**	**Solution**	**Count**
Outdated Operating system	End-of-life detection showing that the operating system will not receive new security updates and may be more susceptible to security threats	Apply security update and update OS to most recent version	3

High Severity Vulnerability

- High vulnerabilities are often harder to exploit and may not cause as big of an impact to an affected system as a critical vulnerability.
- CVSS Score of 7.0-8.9

Example of high severity vulnerability below:

Vulnerable Target	Description	Solution	Count
Linux system	Brute force login exploitation allows attackers to gain access to system with default credentials	Apply a strong password as soon as possible and use multi-factor authentication if possible	1

Medium Severity Vulnerability

- Medium vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network.
- CVSS Score of 4.0-6.9

Example of medium severity vulnerability below:

Vulnerable Target	Description	Solution	Count
Open Ports on Windows device	Enumeration exploit that allows attacker to access more information about a target host	Filter incoming traffic on port 135 and close it if possible	9

Low Severity Vulnerability

- Low vulnerabilities do not need to patch immediately and can be resolved during the next updates maintenance window
- CVSS Score of 0.1-3.9

Recommendations:

The first thing that I would recommend is to update the systems to the latest Operating System versions. Ensure that all relevant security patches are applied through these updates or apply them manually. You should also filter all incoming traffic on open ports to monitor for bad traffic.

References

OpenVAS Scan Results. (n.d.). OpenVAS - Open Vulnerability Assessment Scanner. Retrieved July 30, 2023, from https://openvas.org

Ossec vs Wazuh | What are the differences? (n.d.). StackShare. Retrieved August 3, 2023, from https://stackshare.io/stackups/ossec-vs-wazuh

Otieno, J. (n.d.). *How to Install and Configure OpenVAS on Kali Linux*. Linux Hint. Retrieved July 31, 2023, from https://linuxhint.com/install-openvas-kali-linux/

Report Templates Review. (n.d.). LHL Compass. Retrieved July 30, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w05d4/activities/2958

SECURITY AUDIT REPORT FOR MY BUSINESS. (2021, April 5). Astra Security. Retrieved August 2, 2023, from https://www.getastra.com/blog/wp-content/uploads/2021/06/Astra-Security-Sample-VAPT-Report.pdf

Vulnerability Assessment Report. (n.d.). LHL Compass. Retrieved July 30, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w05d5/activities/2960

Vulnerability Assessment Scan. (n.d.). LHL Compass. Retrieved July 28, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w05d4/activities/2951