Vulnerability Scan Report

Table of Contents

I. Executive Summary

The report finds important weaknesses in the organisation's computer systems. Many serious issues were located that present critical risks to the security and operation of these systems. Here are the main problems identified:

1. **Memory Handling Issue (Critical)**: A few servers are not managing memory properly, which could result in attackers taking control of the system.
2. **Web Browser Security Problems (High)**: There are many vulnerabilities in the web and JavaScript components that could be taken advantage by harmful websites. This may lead to unauthorised actions, system crashes, or provide the opportunity attackers to send harmful code.
3. **Outdated Windows Systems (Critical)**: A few versions of Windows are out of date and lack necessary updates. This greatly increases the risk of the system being compromised.
4. **Remote Procedure Call (RPC) Vulnerability (Medium)**: There is a problem with specific communication protocols that could provide unauthorized access through improper authentication.

Potential Impact

These vulnerabilities could result to unauthorized access to systems, data breaches, and downtime, which could stop business operations and ruin the organization's reputation.

Recommended Actions

To address these issues, immediate actions are needed, including:

- **Applying the latest security updates**
- **Upgrading outdated systems**
- **Disabling outdated communication protocols**

Taking these steps is important to stop potential attacks and ensure the security of the organisation's IT infrastructure. While current security measures are somewhat effective, quick action is necessary to address these identified risks.

II. Vulnerabilities

The table below provides descriptions of the vulnerabilities found on the Nessus Essentials for black box and white box as well as the Common Vulnerability Scoring System (CVSS) that provides a score from 0.0 to 10.0 on the severity of the vulnerability. The descriptions provided will help provide a concise understanding on the vulnerabilities of the assets.

Vulnerability Number	Description	Criticity (CVSS)	Scan (black/white)
1	Server incorrectly handled memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs.	Critical (9.8)	White
2	Incorrectly handled certain file names refers to vulnerabilities that arise when a software application does not properly manage or validate file names provided by users or external systems resulting in data lose and security vulnerabilities. The file systems have restrictions on certain characters such as (\/:*?”<>|) as well as file names being case sensitive.	Critical(9.8)	White
3	It was discovered that Wget incorrectly handled semicolons in the userinfo subcomponent of a URI. A remote attacker could possibly trick a user into connecting to a different host than expected.	High(9.1)	White
4	It was discovered that libde265 could be made to dereference invalid memory. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service.	high(8.8)	White
5	Several security issues were discovered in the WebKitGTK and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.	High(7.4)	White

6	A memory corruption vulnerability exists that can be triggered by an attacker sending a specially crafted NAPTR query.	Critical (10)	Black
7	The remote version of Microsoft Windows is either missing a service pack or is no longer supported.	Critical (10)	Black
8	Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests.	High (10)	Black
9	The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels.	High (8.1)	Black
10	The Microsoft DNS server running on the remote host does not properly handle objects in memory when looking up the resource record of a domain.	Medium (5)	Black

III. Mitigations

The table below show the kind of actions that need to be taken when noticing the vulnerabilities and when it is appropriate to take action as well as the priority of applying the mitigations to the vulnerabilities.

Critical priority (1-2): Requires Immediate action, most likely to be exploited with a big impact.

Moderate priority (3-5): Needs attention, but not serous, risk is present but can be managed.

Low (6-10) priority: Small risk; no immediate action is required but needs to be monitored.

Vulnerability Number	Mitigation description	Priority (1-10)
9	Configure network firewalls to restrict RPC traffic to only trusted hosts. Firewalls should be kept on to prevent unwanted traffic. The action should be taken immediately to make sure that the attacker does not.	1
5	Update Python installations to the latest versions. The action should be taken when prompted for an update.	2
4	To resolve the security issues with Thunderbird is to update to the latest version and disable untrusted features so that attackers cannot use script-based attacks.	3
3	Have the latest versions of libxml2. To do this, write the command prompt ‘sudo apt update’ and then upgrade libxml2 using ‘sudo apt upgrade libxml2’. Once you have identified the vulnerability make sure to do this straight away and monitor any strange activities happening.	4
6	Apply security updates provided by Microsoft for affected Windows Domain Name Server (DNS) servers and monitor authorised access attempts. Take action when a security update is available and monitor all the time to prevent attacker from taking advantage of vulnerability.	5
7	Install any available service packs for the current version of Windows. This should be done when service packs are available.	6
10	Make sure that Windows servers running the Domain Name Server role updated with the latest patches. This should be done straightaway.	7

2	Ensure that you are using the most up-to-date version of Wget, as developers often release security patches that address known vulnerabilities. Check for and apply any available updates.	8
8	Disable SMBv1 completed due to it being an outdated protocol with significant security vulnerabilities. This should be done as soon as possible as to stop attackers from exploiting the vulnerabilities.	9
1	Apply latest security updates by the operating system. The action should be taken as soon as there is a security update available.	10

IV. ChatGPT Use

With the help of ChatGPT, summarised the execute summary to explain the vulnerabilities scan report in a concise way while focusing on the main points.

A. Prompts:

Provide an execute summary designed for non-technical stakeholders summarising the key findings and potential risks as well as highlight critical vulnerabilities, their potential impact on the organisation and offers a high-level perspective on the overall security expected based on this PDF file.

Make it one half of a page long.

Remove jargon so that a non-technical reader can understand.

B. Description:

The vulnerability scan report highlights important weaknesses in the organization's computer systems. Several serious issues were found that pose significant risks to the security and operation of these systems. Here are the main problems identified:

1. **Memory Handling Issue (Critical)**: Some servers are not managing memory correctly, which could allow attackers to take control of the system.
2. **Web Browser Security Problems (High)**: There are multiple vulnerabilities in the web and JavaScript components that could be exploited by harmful websites. This may lead to unauthorized actions, system crashes, or allow attackers to run harmful code.
3. **Outdated Windows Systems (Critical)**: Some versions of Windows are outdated and lack necessary updates. This greatly increases the risk of the system being compromised.
4. **Remote Procedure Call (RPC) Vulnerability (Medium)**: There is a problem with certain communication protocols that could allow unauthorized access through improper authentication.

Potential Impact

These vulnerabilities could lead to unauthorized access to systems, data breaches, and downtime, which could disrupt business operations and damage the organization's reputation.

Recommended Actions

To address these issues, immediate actions are needed, including:

- **Applying the latest security updates**
- **Upgrading outdated systems**
- **Disabling outdated communication protocols**

Taking these steps is crucial to prevent potential attacks and ensure the security of the organization’s IT infrastructure. While current security measures are somewhat effective, quick action is necessary to address these identified risks.

Glossary

Terms	**Definitions**
Application Programming Interface (API)	APIs, or Application Programming Interfaces, are sets of rules and protocols that allow different software applications to communicate and interact with each other. They define the methods and data formats that applications can use to request and exchange information.
Arbitrary code execution	Arbitrary code execution is a security vulnerability that allows an attacker to run any code of their choosing on a target system or application. This capability can lead to a wide range of malicious activities, including data theft and the installation of malware.
Communication protocols	A communications protocol is a set of formal rules describing how to transmit or exchange data, especially across a network.
Crafted file	The term "crafted file" typically refers to a file that has been intentionally created or modified in a specific way, often for malicious purposes.
Cross-site scripting attacks	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.
Denial of service attack	A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.
Dereference	Dereference means to obtain the address of a data item held in another location from a pointer.
DeviceFocusEvent	A DeviceFocusEvent typically refers to an event that occurs when a device (such as a mouse, keyboard, or touch device) gains or loses focus within an application.

Domain Name Server	A Domain Name System (DNS) turns domain names into IP addresses, which allow browsers to get to websites and other internet resources.
Handled memory	The term "handled memory" typically refers to how memory is managed, allocated, and deallocated in a software application or system.
Improper handling of certain requests.	Improper handling of certain requests refers to the failure to correctly process, respond to, or manage specific types of requests in a system, application, or service.
Invalid memory	Invalid memory refers to memory locations that are not currently allocated to a program or are no longer valid for use. Accessing invalid memory can lead to various issues, including crashes, data corruption, and security vulnerabilities.
IT infrastructure	IT infrastructure refers to the composite of physical and virtual resources that support the management and delivery of IT services within an organization. It encompasses the hardware, software, network resources, and services required for the operation and management of IT environments.
JavaScript engines	JavaScript engines are software components that execute JavaScript code. They parse, interpret, and execute the code, enabling web applications and services to perform dynamic tasks in a browser or server environment.
libde265	libde265 is an open-source software library designed for decoding HEVC (High Efficiency Video Coding), also known as H.265. This video compression standard is used for encoding and decoding video data, providing higher compression rates than its predecessor, H.264, without compromising video quality.
Local Security Authority	The Local Security Authority (LSA) is a crucial component of Windows operating systems responsible for enforcing the security policy on the local computer. It manages various security-related tasks and plays a key role in authentication and access control.

Memory corruption	Memory handling issues refer to problems that arise during the allocation, usage, and deallocation of memory in software applications. These issues can lead to inefficient memory usage, data corruption, application crashes, and security vulnerabilities.
Memory Handling Issue	Memory handling issues refer to problems that occur during the management of memory in software applications, particularly in how memory is allocated, accessed, and released.
Microsoft Server Message Block 1.0 (SMBv1)	Microsoft Server Message Block 1.0 (SMBv1) is a network file sharing protocol used for providing shared access to files, printers, and other resources on a network.
NAPTR query	A NAPTR query refers to a type of DNS (Domain Name System) query that is used to retrieve NAPTR (Naming Authority Pointer) records. NAPTR records are a part of the DNS system and are primarily used to facilitate the resolution of service types and protocols, especially in applications like Voice over IP (VoIP) and other multimedia services.
Network firewalls	Network firewalls are tasked with defining and securing network boundaries. To accomplish this, they offer various capabilities, such as: IP and Domain Filtering: Even the simplest firewalls can manage packets based on their source or destination IP addresses.
OpenSSH	OpenSSH (also known as OpenBSD Secure Shell) is a suite of secure networking utilities based on the Secure Shell (SSH) protocol, which provides a secure channel over an unsecured network in a client–server architecture.
Outdated Windows Systems	An outdated operating system is a software system that is no longer receiving official support and updates from its manufacturer or developer.
ProcXIQueryPointer	ProcXIQueryPointer is a function used in the context of the X Window System, specifically within the X Input Extension (XI). It is designed to query the current state of a pointer device, such as a mouse or a touchscreen.

Python installations	Python installations refer to the process of setting up the Python programming language on a computer or server, enabling users to execute Python code and run applications written in Python.
Remote host	A remote host refers to a computer or server that is located on a different network or geographical location than the user's local machine. It can be accessed over a network, such as the internet or a local area network (LAN), and is commonly involved in client-server architecture.
Remote Procedure Call (RPC) Vulnerability	A Remote Procedure Call (RPC) vulnerability refers to a security flaw that arises in systems utilizing the RPC protocol, which allows programs to execute procedures (functions) on remote systems as if they were local.
Remote Procedure Call Channels	Remote Procedure Call (RPC) channels refer to the communication pathways established for transmitting requests and responses between a client and a server in an RPC system.
Remote version of Microsoft Windows	The remote version of Microsoft Windows typically refers to the capability of Windows operating systems to be accessed and managed remotely, often through various remote access technologies.
Remote Windows host	A remote Windows host refers to a Windows-based computer or server that is accessed over a network (such as the internet or a local area network) rather than being directly connected to the user's local machine.
RPC traffic	RPC traffic refers to the data packets exchanged between a client and a server when using the Remote Procedure Call (RPC) protocol. This protocol allows a program to execute a procedure (function) on a remote system as if it were local, facilitating communication in distributed computing environments.
Security Account Manager	The Security Account Manager (SAM) is a database file in Windows operating systems that stores user account information, including passwords and security descriptors.

Service pack	A service pack is a collection of updates, fixes, and enhancements for a software product, typically an operating system or application. Service packs are released by software vendors to improve functionality, enhance security, and resolve issues that users may encounter.
sudo apt upgrade libxml2	The command ‘sudo apt upgrade libxml2’ is used in Debian-based Linux distributions (like Ubuntu) to upgrade the libxml2 library to its latest available version from the configured package repositories.
sudo apt upgrade openssh-client openssh-server	The command sudo apt upgrade openssh-client openssh-server is used in Debian-based Linux distributions (like Ubuntu) to upgrade the OpenSSH client and server packages to their latest available versions from the configured package repositories.
Trusted hosts	Trusted hosts refer to computers or servers that are considered secure and reliable within a network or security context. These hosts are typically granted special permissions or access rights because they are recognized as safe sources of communication or data exchange.
Unwanted traffic	Unwanted traffic refers to network data packets that are not desired or intended by the network's users or administrators. This type of traffic can negatively impact network performance, security, and resource availability.
Web Browser Security Problems	Web browser security problems refer to vulnerabilities, weaknesses, or issues that can compromise the security and privacy of users while they browse the internet. These problems can arise from various sources, including browser software itself, web applications, user behavior, and external threats.
WebKitGTK	WebKitGTK is a web rendering engine that provides a set of tools for embedding web content in applications built with the GTK (GIMP Toolkit) framework. It is based on the WebKit engine, which is used by major web browsers like Safari and earlier versions of Google Chrome.