LOVELY PROFESSIONAL UNIVERSITY

Academic Task-3

INT301: Open Source Technologies

Name: Saurabh Rawat

Registration No: 11914249

Roll No: 64

Section: KE023

Git hub link - https://github.com/saurabh080701/Discovering-Missing-Security-Updates-and-Analyzing-Hardware-and-Software-with-Free-Tools

Discovering Missing Security Updates and Analyzing Hardware and Software with Free Tools

1. Introduction

It is crucial to make sure that your operating system and software programs are up to date with the most recent security upgrades in the connected world of today. Millions of people use the Windows operating system, which is among the most well-liked ones. However, fraudsters frequently target it in order to obtain unauthorized access and steal private data by taking advantage of flaws in the system.

It's crucial to keep your Windows operating system updated with the most recent security patches in order to guarantee system security and shield it from threats. However, finding outdated security patches might be difficult, especially if your computer is running many software applications. Open-source software tools are helpful in this situation. We will look at some of the well-known open-source software programmers in this area, including as OpenVAS, Secunia PSI, and MBSA, that can assist you in finding Windows OS security upgrades that are missing. Utilizing these tools will make it simple for you to monitor your system for any necessary security upgrades and keep it safe.

Microsoft Baseline Security Analyzer (MBSA) is a free tool from Microsoft that can help you identify missing security updates on your Windows OS. It scans your system for missing security updates, weak passwords, and other security issues. The tool also provides recommendations on how to resolve the identified security issues.

Maintaining and troubleshooting your system depend on your ability to identify the specific hardware and software components installed on your computer. Having access to precise and thorough system information is essential whether you wish to improve your system or fix any problems. Thankfully, there are a number of free programmers that can provide you comprehensive details on the hardware and software that are installed on your computer.

1.1 Objective of the project

The goal of this project is to offer a thorough tutorial on how to use open-source software tools for locating Windows OS security updates that are missing, as well as free system information tools for discovering the hardware and software that are already installed on your machine.

Section 1: Open Source Software for Windows OS Missing Security Update Detection
We will look at some of the well-liked open-source software solutions for locating missing security updates on your Windows OS in this part. OpenVAS, Secunia PSI, Microsoft Baseline Security Analyzer (MBSA), Qualys Browser Check, CIS-CAT, and OVAL are some of the tools in this group.

Section 2: Free System Information Tools for Locating Installed Hardware and Software
We'll look at some of the well-liked, free system information applications in this part that may help you find out what hardware and programmers are installed on your computer. These programmers include PC Wizard, Belarc Advisor, AIDA64, CPU-Z, Speccy, HWiNFO, and HWiNFO.

You may find out if your Windows OS needs any security updates by utilizing these open-source software tools and free system information tools, and you can also learn a lot about the hardware and software parts of your system. You may use this information to keep your system up to date and safe, solve any issues you encounter, and decide whether to upgrade your hardware or software.

1.2 Description of the project –

Making sure that all required security updates are installed is critical to protecting the security of your Windows operating system. However, it might be difficult to keep up with the frequent security updates and patches that Microsoft releases. Thankfully, there are a number of open-source software applications that can find missing security updates for your Windows operating system.

We will look at some of the well-liked open-source software tools for locating missing security updates on your Windows OS in this project. OpenVAS, Secunia PSI, Nmap, Microsoft Baseline Security Analyzer (MBSA), and OVAL are some of the tools in this group.

We will also provide a list of some of the well-liked free system information tools for locating the installed hardware and software on your computer. The CPU, memory, storage, graphics card, and other hardware elements of your system, as well as their specs, may be identified with the use of these tools. They can also provide you information about the drivers, apps, and operating system version of the software that is already installed on your computer.

AIDA64, Belarc Advisor, CPU-Z, Speccy, HWiNFO, AIDA64, and PC Wizard are a few of the free system information utilities we'll discuss.

You may find out if your Windows OS needs any security updates by utilizing these open-source software tools and free system information tools, and you can also learn a lot about the hardware and software parts of your system. You may use this information to keep your system up to date- and safe, solve any issues you encounter, and decide whether to upgrade your hardware or software.

1.3 Scope of the project -

The goal of this project is to provide a thorough manual for utilizing open-source software tools to find Windows OS security updates that are missing, as well as free system information tools to find out what hardware and software are installed on your machine.

The objective of the initiative is to give users a thorough tutorial on how to use these tools, assist them in maintaining and troubleshooting their systems, help them decide whether to upgrade their hardware or software, and make sure their systems are safe and current.

Detailed instructions on how to install and utilize these tools will not be included in this project. To assist users in getting started, we will include links to the official documentation and resources for each program. The goal of the project is to give a general overview of the capabilities, features, and advantages of these free system information tools and open-source software tools.

Overall, this project will serve as a useful resource for anybody wishing to learn more about their computer's hardware and software components and find any security upgrades that are missing from their Windows OS.

2. System Description

2.1 Target system description -

Any machine with Windows as its operating system is the project's target system. The goal of the project is to provide consumers insight into their system's hardware and software by assisting them in identifying missing security updates for their Windows OS.

Anyone utilizing a Windows-based computer, whether for personal or commercial usage, can use this project. It is especially useful for users who are in charge of keeping their system's security and functionality up to par, such system administrators or IT specialists.

The project's goal is to give consumers a thorough tutorial on how to utilize free system information tools to learn about their system's hardware and software components and open-source software tools to find needed security upgrades. Users may maintain their system's security and performance with the use of the project's information, which will also help them, address typical problems like missing security updates and software and hardware compatibility.

The project's overall goal is to offer a useful resource for Windows users who want to make sure their system is current, safe, and operating at its peak performance.

2.2 Assumptions and Dependencies –

For this project, there are a few presumptions and dependencies:

Access to a Windows-based computer: In order to install and utilize the free system information tools and open-source software tools, the project expects the user has access to a Windows-based computer.

Internet connectivity is required: for the user to obtain the free system information tools and open-source software tools, as well as to check for security updates.

Administrator rights: In order to install and utilize several open-source software tools, you must have administrator rights. The project thus requires that the user is logged in as the administrator on a Windows PC.

Compatibility: The project assumes that the open-source software tools and free system information tools are compatible with the user's Windows OS. Some software tools may not be compatible with older versions of Windows OS, and some may not work with the latest Windows OS updates.

Availability of security updates: The project assumes that security updates are available for the user's Windows OS. In some cases, security updates may not be available for outdated Windows OS versions, or some security updates may require additional software or hardware requirements.

User knowledge: The project assumes that the user has a basic understanding of how to install and use software tools on their Windows-based computer.

Open-source software dependencies: In order to work properly, some open-source software tools may require other software or libraries. As a result, the project presumes that the user has installed all the dependencies for the open-source software tools that they want to utilize.

Overall, these assumptions and dependencies must be considered while utilizing open-source software tools to find missing security updates and free system information tools to gather information on the hardware and software components of a Windows-based device.

2.3 Functional/Non-Functional Dependencies –

Functional Dependencies:

Open-Source Software Tools: To find missing security updates on a Windows-based machine, the project requires the usage of particular open-source software tools. To download and install the essential open-source software tools, the user must have access to a good internet connection.

Security Update Database: To find missing security updates on a Windows-based machine, open-source software applications rely on a security update database. For the software tools to perform properly, the security update database must be up to date and accurate.

System Information Tools: The project involves the usage of particular free system information tools to obtain information on the hardware and software components of a Windows-based machine. To download and install the necessary system information tools, the user must have access to a stable internet connection.

Hardware and Software Components: The system information tools rely on accurate hardware and software component information to deliver accurate information on the hardware and software components of a Windows-based machine. As a result, it is critical to guarantee that the hardware and software components are properly installed and operating.

Non-Functional Dependencies:

The following non-functional requirements are necessary for the project to be completed successfully:

Performance: To guarantee the best performance, open-source software tools and system information tools must be properly installed and configured.

Reliability: Open-source software tools and system information tools must be dependable and accurate.

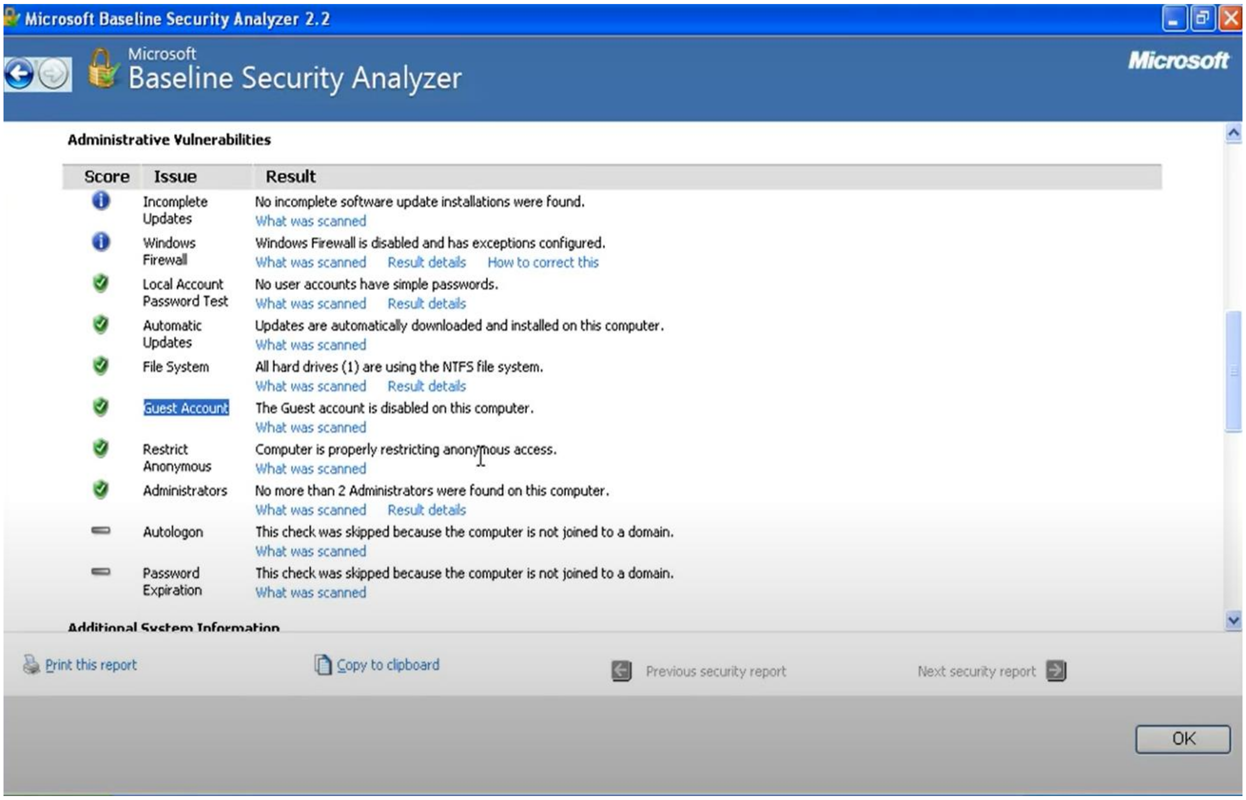
Usability: Open-source software tools and system information tools must be simple to use.

Overall, these functional and non-functional dependencies must be considered while utilizing open-source software tools to find missing security updates and free system information tools to gather information on the hardware and software components of a Windows-based device.

3. Analysis Report –

Using open-source software tools to find missing security updates and free system information tools to gather information on the hardware and software components of a Windows-based machine can give useful insights into the system's security and performance. Some essential issues to examine in the analysis report are as follows:

Missing Security Updates: The open-source software tools will scan the system for missing security updates and provide a report that identifies all of them. The notification should specify the severity of each missing update and offer instructions on how to download and install them.

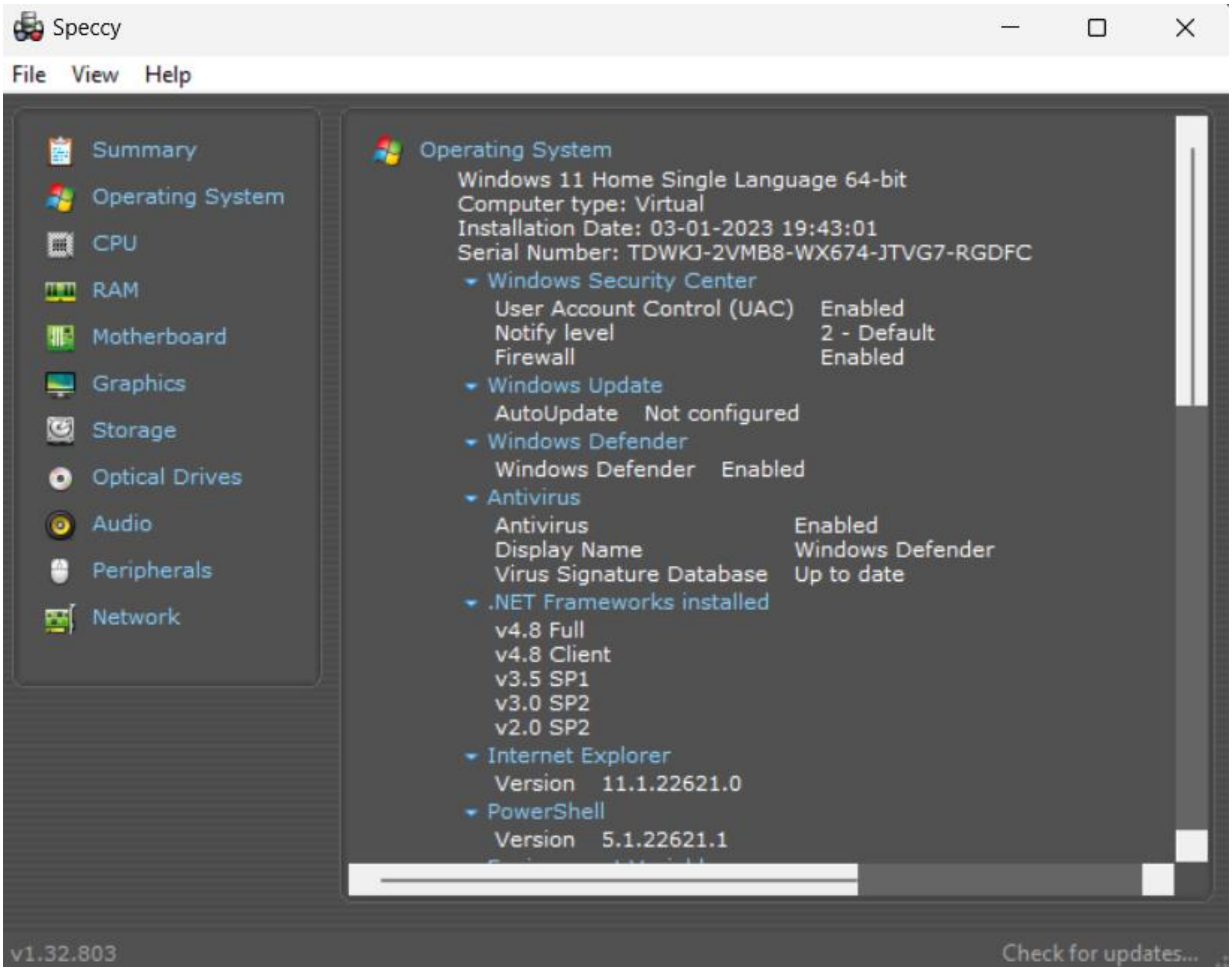


Administrative Vulnerabilities

Score	Issue	Result
ⓘ	Incomplete Updates	No incomplete software update installations were found. What was scanned
ⓘ	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
—	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
—	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned

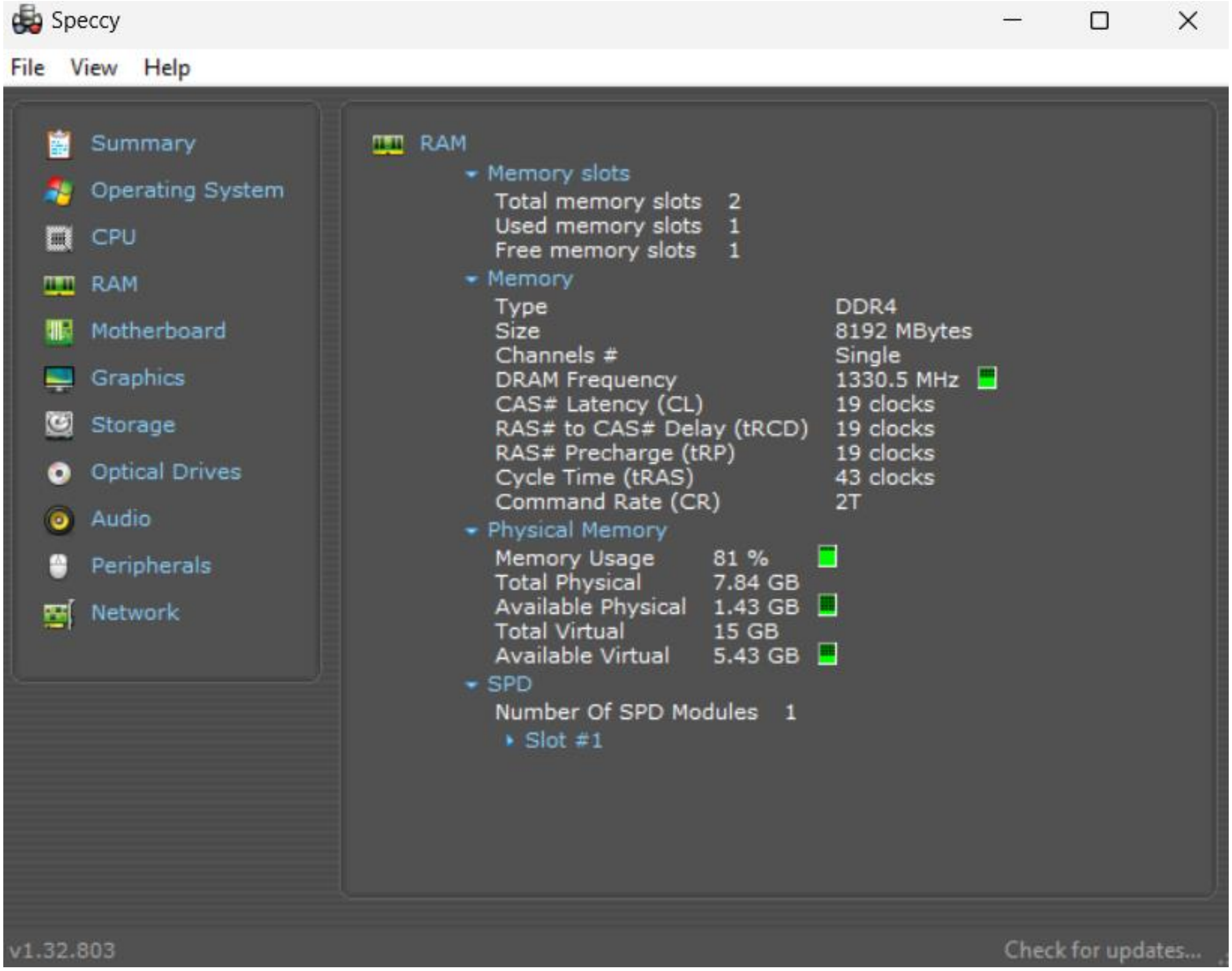
Additional System Information

Software Components: The free system information tools will collect information on the software components installed on the system, such as the operating system, drivers, and applications. A list of all installed software components, their versions, and their status should be included in the report. (i.e., up-to-date or out-of-date).



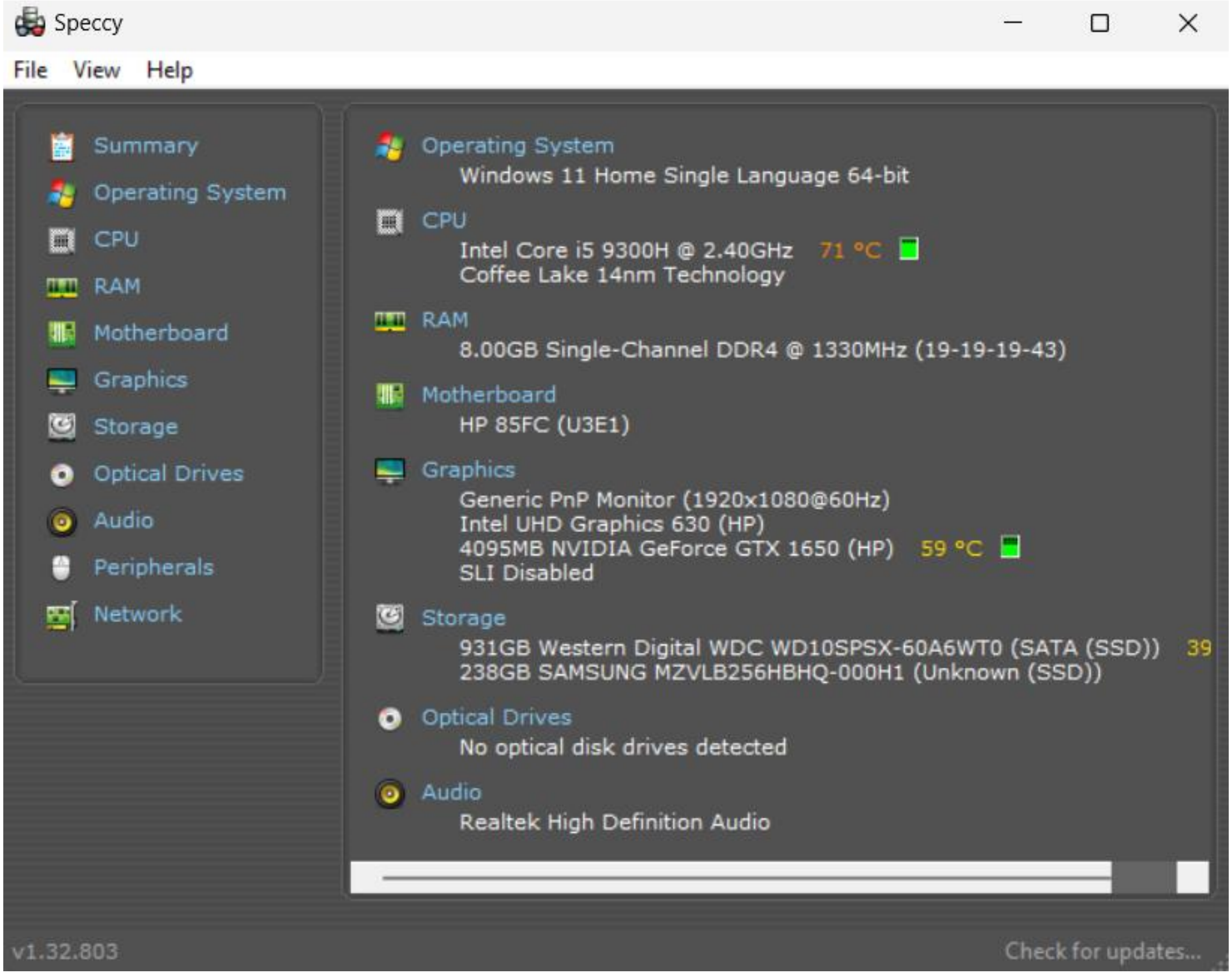
```
Operating System
    Windows 11 Home Single Language 64-bit
    Computer type: Virtual
    Installation Date: 03-01-2023 19:43:01
    Serial Number: TDWKJ-2VMB8-WX674-JTVG7-RGDFC
      Windows Security Center
        User Account Control (UAC)   Enabled
        Notify level                 2 - Default
        Firewall                     Enabled
      Windows Update
        AutoUpdate    Not configured
      Windows Defender
        Windows Defender    Enabled
      Antivirus
        Antivirus                 Enabled
        Display Name              Windows Defender
        Virus Signature Database  Up to date
      .NET Frameworks installed
        v4.8 Full
        v4.8 Client
        v3.5 SP1
        v3.0 SP2
        v2.0 SP2
      Internet Explorer
        Version    11.1.22621.0
      PowerShell
        Version    5.1.22621.1
```

Hardware Components: The free system information tools will also collect information about the system's hardware components, such as the CPU, RAM, hard drive, and graphics card. A list of all installed hardware components, their specs, and their status should be included in the report. (i.e., functioning correctly or not).



```
RAM
    Memory slots
        Total memory slots   2
        Used memory slots    1
        Free memory slots    1
    Memory
        Type                           DDR4
        Size                           8192 MBytes
        Channels #                     Single
        DRAM Frequency                 1330.5 MHz 🟩
        CAS# Latency (CL)              19 clocks
        RAS# to CAS# Delay (tRCD)      19 clocks
        RAS# Precharge (tRP)           19 clocks
        Cycle Time (tRAS)              43 clocks
        Command Rate (CR)              2T
    Physical Memory
        Memory Usage        81 %     🟩
        Total Physical      7.84 GB
        Available Physical  1.43 GB  🟩
        Total Virtual       15 GB
        Available Virtual   5.43 GB  🟩
    SPD
        Number Of SPD Modules   1
          Slot #1
```

System Performance: The report should contain an analysis of the system's performance based on the information received from the hardware and software components. The investigation should identify any bottlenecks or areas for improvement that might improve the performance of the system.



```
Operating System
    Windows 11 Home Single Language 64-bit
CPU
    Intel Core i5 9300H @ 2.40GHz   71 °C 🟩
    Coffee Lake 14nm Technology
RAM
    8.00GB Single-Channel DDR4 @ 1330MHz (19-19-19-43)
Motherboard
    HP 85FC (U3E1)
Graphics
    Generic PnP Monitor (1920x1080@60Hz)
    Intel UHD Graphics 630 (HP)
    4095MB NVIDIA GeForce GTX 1650 (HP)   59 °C 🟩
    SLI Disabled
Storage
    931GB Western Digital WDC WD10SPSX-60A6WT0 (SATA (SSD))   39
    238GB SAMSUNG MZVLB256HBHQ-000H1 (Unknown (SSD))
Optical Drives
    No optical disk drives detected
Audio
    Realtek High Definition Audio
```

<u>Recommendations:</u> Based on the study, the report should provide recommendations for enhancing the system's security and performance. Installing missing security updates, updating out-of-date software components, upgrading hardware components, or optimizing system settings may be among the suggestions.

Overall, employing open-source software tools to find missing security updates and free system information tools to gather information on the hardware and software components of a Windows-based machine can give useful insights into the system's security and performance. The study report should be thorough and contain recommendations for enhancing the security and performance of the system.

4. Reference

1. L. Angelis, "Code Quality Analysis in Open Source Software Development", *Information Systems J.*, vol. 12, no. 1, pp. 43-60, 2002.

2. P. Ruckebusch et al., "Modelling the Energy Consumption for Over-the-Air Software Updates In LPWAN Networks: Sigfox Lora and IEEE 802.15. 4g", *Internet of Things J.*, vol. 3, pp. 104-19, 2018.

3. Santi Pattanavichai,Rajamangala University of Technology Thanyaburi, RMUTT, Thanyaburi, Pathumthani, Thailand.

4. S. Chimmanee, T. Veeraprasit and C. Srisa-An, "A Performance Evaluation of Vulnerability Detection: NetClarity Audito Nessus and Retina", *IJCSNS International Journal of Computer Science and Network Security*, vol. 14, no. 3, pp. 34-40, March 2014.

5. V. Mee *et al.* The windows registry as a forensic artefact: illustrating evidence collection for internet usage.

6. S. Hejazi *et al.*Extraction of forensically sensitive information from windows physical memory Digital Investigation(2009)

7. B. Dolan-Gavitt Forensic analysis of the windows registry in memory Digital Investigation (2008).
8. C. Maartmann-Moe *et al.* The persistence of memory: forensic identification and extraction of cryptographic keys Digital Investigation (2009).

Github link - https://github.com/saurabh080701/Discovering-Missing-Security-Updates-and-Analyzing-Hardware-and-Software-with-Free-Tools