

**Forensic analysis using Open source technologies**

**By**

**Abhishek Ranaut**

**11910703**

**Roll no.64**

**INT301 CA3**

# Index

1. Introduction
   1. [Objective of the project 5](#_TOC_250002)
   2. [Description of the project 5](#_TOC_250001)-6
   3. [Scope of the project 5](#_TOC_250000)-6
2. System Description
   1. Target system description 7
   2. Assumptions and Dependencies (If applicable) 7-8
3. Analysis Report
   1. Final result of the Nessus 9-12
   2. Final result of the HWiNFO64 13-14
4. Reference/ Bibliography 15
5. Github-link 16

# Chapter 1

### Introduction

#### What is computer forensics?

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

#### Why is computer forensics important?

In the civil and criminal justice system, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence -- and the forensic process used to collect, preserve and investigate it -- has become more important in solving crimes and other legal issues.

The average person never sees much of the information modern devices collect. For instance, the computers in cars continually collect information on when a driver brakes, shifts and changes speed without the driver being aware. However, this information can prove critical in solving a legal matter or a crime, and computer forensics often plays a role in identifying and preserving that information.

#### Types of computer forensics

There are various types of computer forensic examinations. Each deals with a specific aspect of information technology. Some of the main types include the following:

* **Database forensics.** The examination of information contained in databases, both data and related metadata.
* **Email forensics.** The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.
* **Malware forensics.** Shifting through code to identify possible malicious programs and analyzing their payload. Such programs may include Trojan Horses, ransomware or various viruses.
* **Memory forensics.** Collecting information stored in a computer’s random-access memory (RAM) and cache.
* **Mobile forensics.** The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.
* **Network forensics.** Looking for evidence by monitoring network traffic, using tools such as a firewall or intrusion detection system.

**1.1 Malware Forensics**

#### Malware forensics is the process of identifying, analyzing, and containing malware infections on a computer system or network. The goal of malware forensics is to gather evidence of malicious activity, determine the extent of the infection, and mitigate its impact.

#### The following are some of the steps involved in malware forensics:

#### Identification: The first step is to identify the malware infection. This can be done through antivirus software, intrusion detection systems, or other security tools.

#### Isolation: Once the malware has been identified, it needs to be isolated to prevent it from spreading further. This can be done by disconnecting the infected computer from the network, shutting it down, or using other isolation techniques.

#### Analysis: The next step is to analyze the malware to determine its behavior, capabilities, and impact. This can involve reverse engineering the malware code, examining system logs, and using other forensic techniques.

#### Containment: After the malware has been analyzed, the next step is to contain its impact. This can involve removing the malware from infected systems, patching vulnerabilities, and implementing other security measures.

#### Recovery: Once the malware has been contained, the final step is to recover from the attack. This can involve restoring data from backups, repairing damaged systems, and improving security measures to prevent future attacks.

#### Overall: malware forensics is a complex process that requires specialized knowledge and tools. It is an essential part of any comprehensive cybersecurity strategy, as it helps organizations to detect and respond to malware attacks quickly and effectively.

#### Overall, malware forensics is a complex process that requires specialized knowledge and tools. It is an essential part of any comprehensive cybersecurity strategy, as it helps organizations to detect and respond to malware attacks quickly and effectively.

#### Objective of the project:

List all the security updates missing in your Windows OS

#### Description of the project

A popular open source software for finding the missing security updates in Windows OS is Nessus. Nessus is a vulnerability scanner that is used to identify security vulnerabilities and misconfigurations in computer systems, networks, and applications. It is developed and maintained by Tenable, Inc.

Nessus is a widely used tool in the cybersecurity industry, and it is used by organizations of all sizes to improve their security posture. It can be integrated with other security tools, such as security information and event management (SIEM) systems, to automate vulnerability management and response processes.

#### Scope of the project

To use Nessus, you must have the software installed on your computer and connected to the storage device you wish to analyze. Once you are done, you can use the software to create a vulnerability scan of your device which is an exact replica of all the data stored on it.

Nessus performs automated scans of network assets, including servers, workstations, network devices, and cloud infrastructure, to identify vulnerabilities that can be exploited by attackers. It uses a variety of techniques to identify vulnerabilities, including port scanning, service identification, vulnerability detection, and exploitation.

Nessus can be used to perform both internal and external scans, allowing organizations to identify vulnerabilities from both inside and outside their network perimeter. It provides detailed reports on the vulnerabilities it identifies, including severity ratings, recommended remediation steps, and links to external resources for further information.

**1.2 Memory Forensics**

Memory forensics is a technique used to investigate and analyze digital memory for evidence of malicious activity on a computer system or network. It involves extracting information from volatile memory, such as RAM, to identify processes, network connections, and other artifacts that may not be visible through traditional file system analysis.

Memory forensics is becoming increasingly important as attackers become more sophisticated in their methods of hiding malicious activity. Malware can often avoid detection by hiding in memory and only executing its malicious code when certain conditions are met. Memory forensics allows investigators to identify and analyze this type of activity.

The process of memory forensics involves capturing a memory image of the target system, analyzing the image using specialized tools, and searching for indicators of compromise (IOCs) that may indicate the presence of malicious activity. This can include analyzing network connections, identifying malicious processes or services, and examining registry keys and other system artifacts.

Memory forensics is a complex and specialized field that requires specialized knowledge and tools. There are many open-source and commercial tools available for conducting memory forensics, including Volatility, Rekall, and Redline, among others. It is an essential part of any comprehensive incident response or digital forensics program and is often used in conjunction with other investigative techniques to build a complete picture of an incident.

#### Objective of the project:

List all free system information about hardware and software installed

#### Description of the project

A popular open source software for listing all free system information about hardware and software installed is HWiNFO64.

HWiNFO64 is a hardware diagnostic tool that provides detailed information about the hardware and software components of a Windows computer. It is developed by REALiX, a software development company based in Slovakia.

HWiNFO64 is available as a free download for personal use and also offers a commercial license for businesses and organizations. It is compatible with all versions of Windows, including Windows 10, and supports both 32-bit and 64-bit architectures.

#### Scope of the project

To use HWiNFO64, you must have the software installed on your computer and connected to the storage device you wish to analyze. HWiNFO64 can identify and provide information on a wide range of hardware components, including the CPU, GPU, motherboard, RAM, hard drives, and peripherals such as printers and scanners. It can also provide real-time monitoring of hardware performance, including temperature, fan speed, and power consumption.

HWiNFO64 is commonly used by system administrators, IT professionals, and PC enthusiasts to diagnose hardware issues, monitor system performance, and optimize system settings. It can generate detailed reports that can be used for troubleshooting and system maintenance.

**Chapter 2**

### System Description

#### Target system description

* + - A computer with sufficient processing power and memory to run the open-source software, such as Nessus and HWiNFO64.
    - The target storage device or devices that need to be analyzed.
    - A write-blocker device or hardware write-blocking capability to ensure that the data on the storage devices is not altered during the extraction process.
    - An understanding of the file system on the storage device and how the data is organized, such as NTFS, FAT32, or ext4.
    - An understanding of the open-source software being used and its capabilities for analyzing data.
    - The necessary permissions or legal authority to analyze the data on the storage devices.
    - Proper documentation of the extraction process and any findings, to ensure that the extracted data can be used as evidence in legal proceedings if necessary.

#### 2.2 Assumptions and Dependencies (If applicable)

* + - The storage devices being analyzed are functioning and can be accessed by the computer running the open-source software.
    - The open-source software being used is compatible with the operating system and file system of the storage devices being analyzed.
    - The write-blocker device or hardware write-blocking capability is functioning properly and

is preventing any changes to the data on the storage devices.

* + - The storage devices being analyzed do not have any hardware or firmware-based encryption that would prevent the open-source software from extracting the data.
    - The open-source software being used is configured correctly and is capable of accurately extracting and analyzing the data on the storage devices.
    - The forensic examiner using the open-source software has the necessary technical knowledge and expertise to operate the software effectively and to interpret the results of the analysis.
    - The forensic examiner using the open-source software has the necessary legal authority or permissions to extract and analyze the data on the storage devices.

## 3.Analysis Report

#### This is the final result of the Nessus:

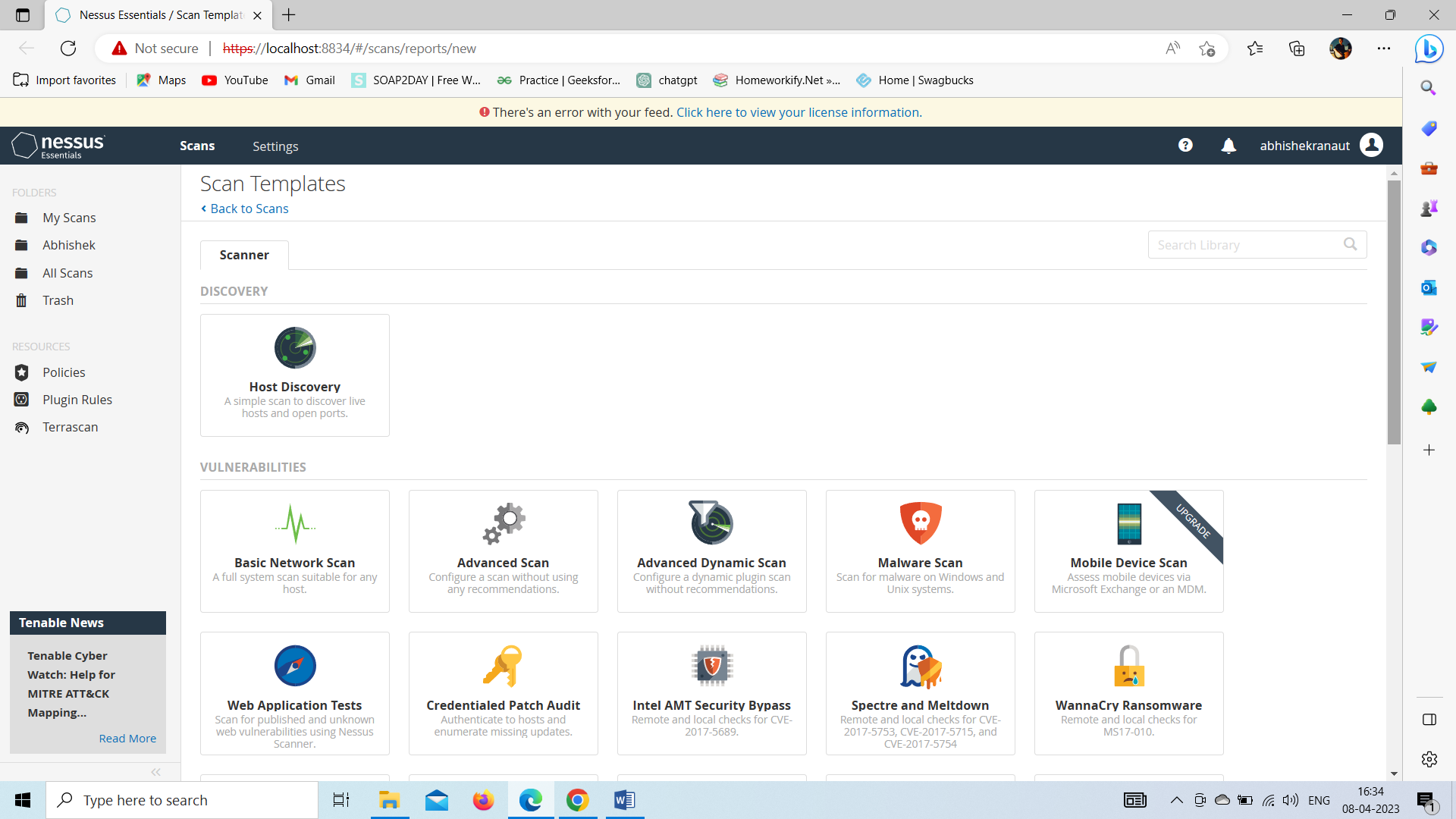
****

Figure.1 Nessus login window

Configure your scan settings: In the Nessus interface, select the "New Scan" option and choose the target system or network that you want to scan. You can configure various settings for your scan, such as the scan type, timing, and policy.

Start the scan: Once you have configured your scan settings, click on the "Launch" button to start the scan.

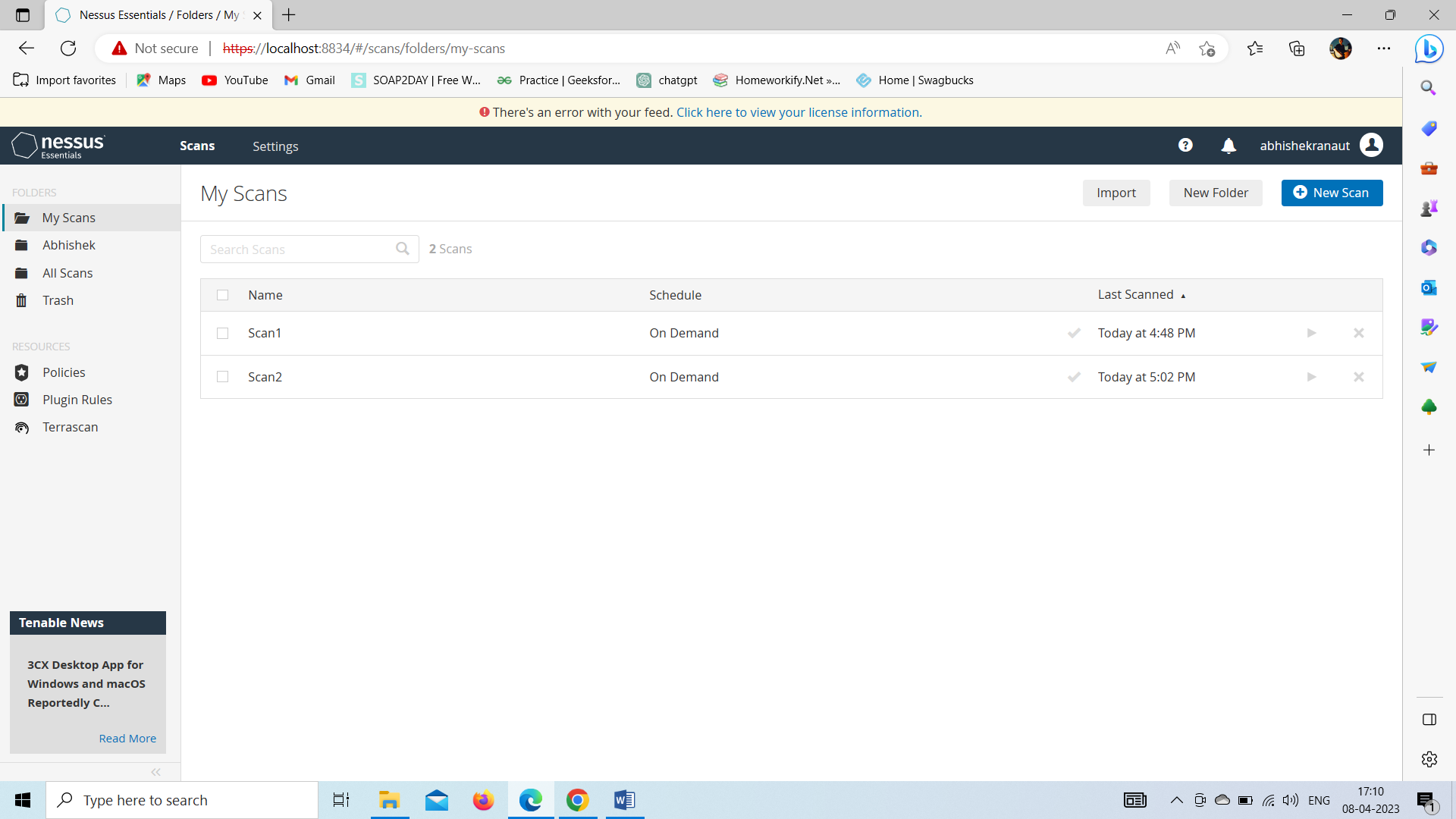


Figure. 2 Nessus Vulnerability Scans

Review scan results: Once the scan is complete, Nessus will provide a detailed report of any vulnerabilities that it found. Review the report and prioritize any vulnerabilities that require immediate attention.

Remediate vulnerabilities: Work with your IT team to remediate any vulnerabilities that were identified during the scan.

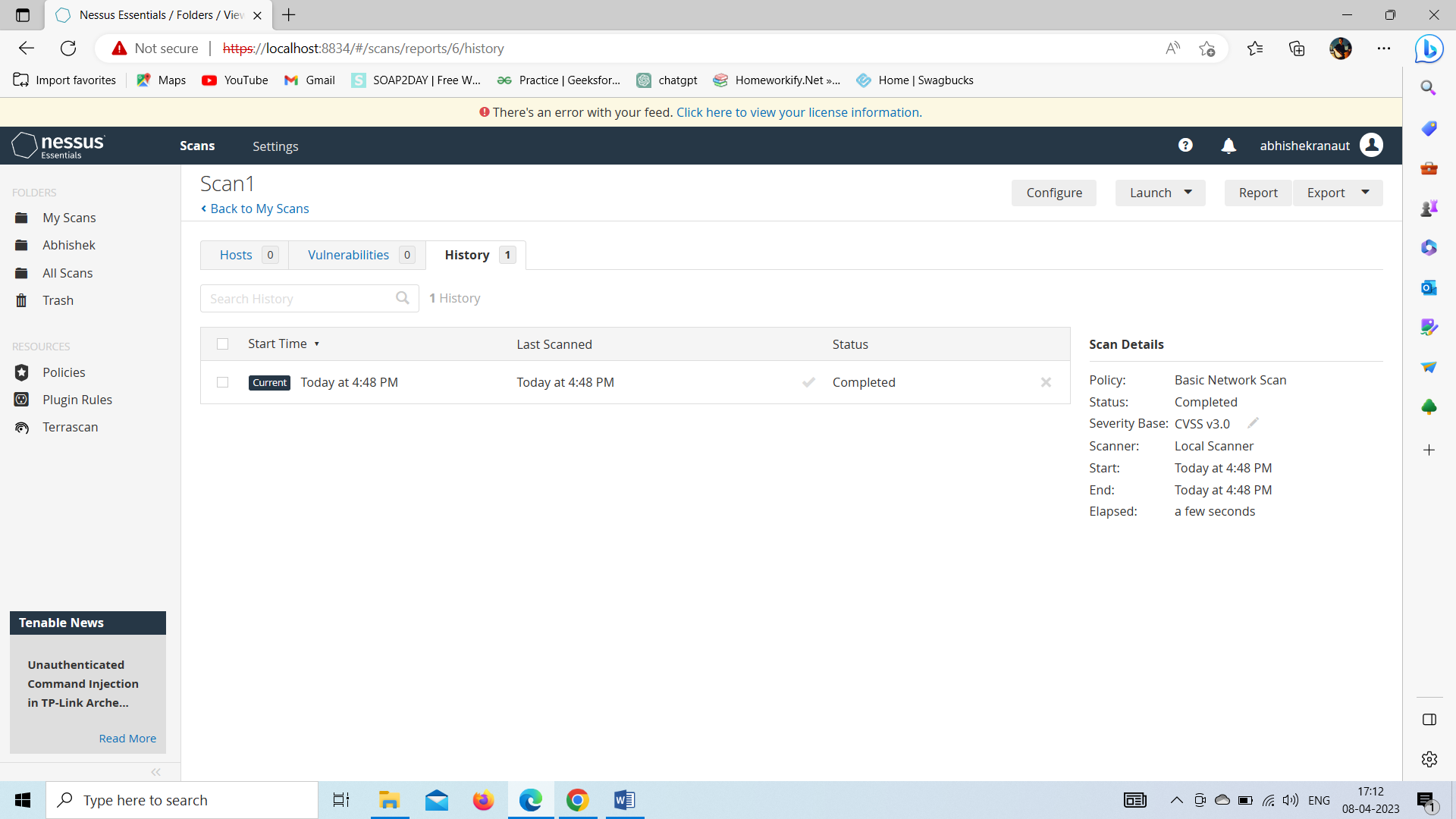


Figure.3 Result of Scan 1

No Vulnerability Found

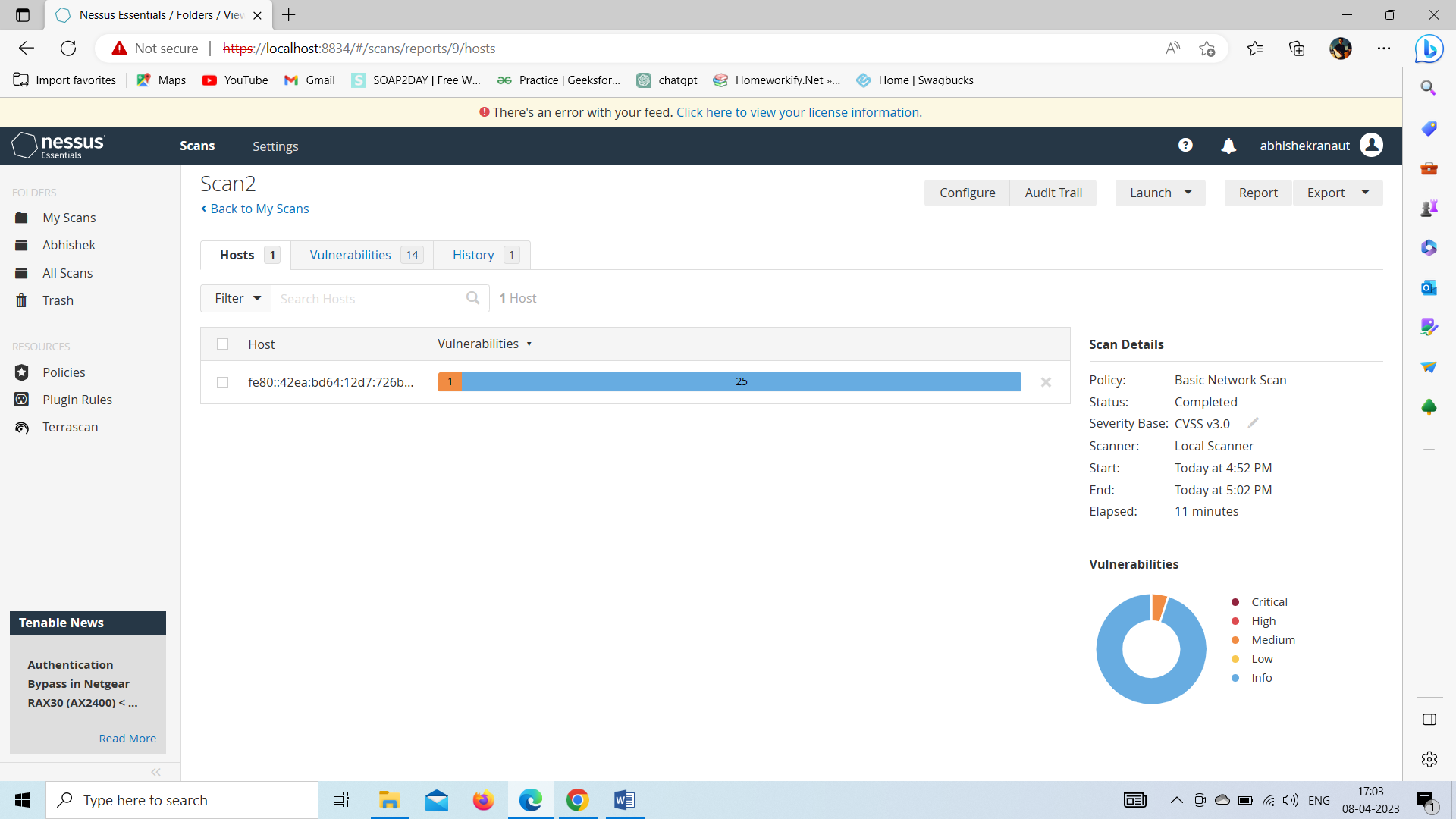


Figure 4 Result of Scan 2

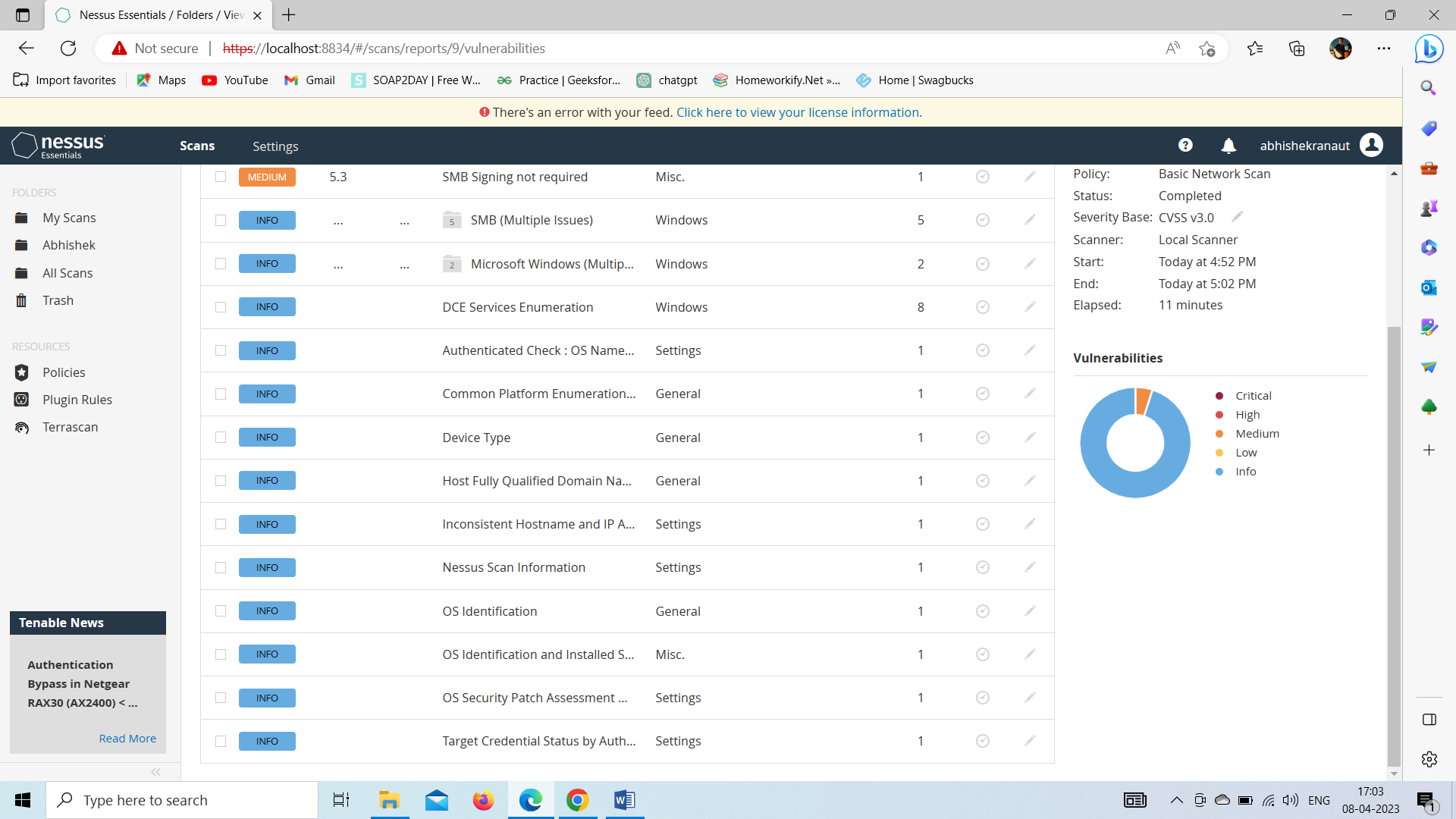


Figure 5 Vulnerabilities found in Scan 2

Identify the affected systems: Once you have identified the vulnerabilities to remediate, identify the systems that are affected by the vulnerabilities. This will help you to determine the scope of the remediation efforts.

Develop a remediation plan: Develop a plan to remediate the vulnerabilities. This plan should include steps to fix the vulnerabilities and a timeline for completion.

Patch systems: Install patches or updates to fix the vulnerabilities. Ensure that all affected systems are patched and that the patches are tested before being applied to production environments.

Update configurations: Update the configurations of the affected systems to prevent the vulnerabilities from being exploited. For example, disable unnecessary services or ports, configure firewalls, or implement access controls.

**3.2 This is the final result of HWiNFO64**

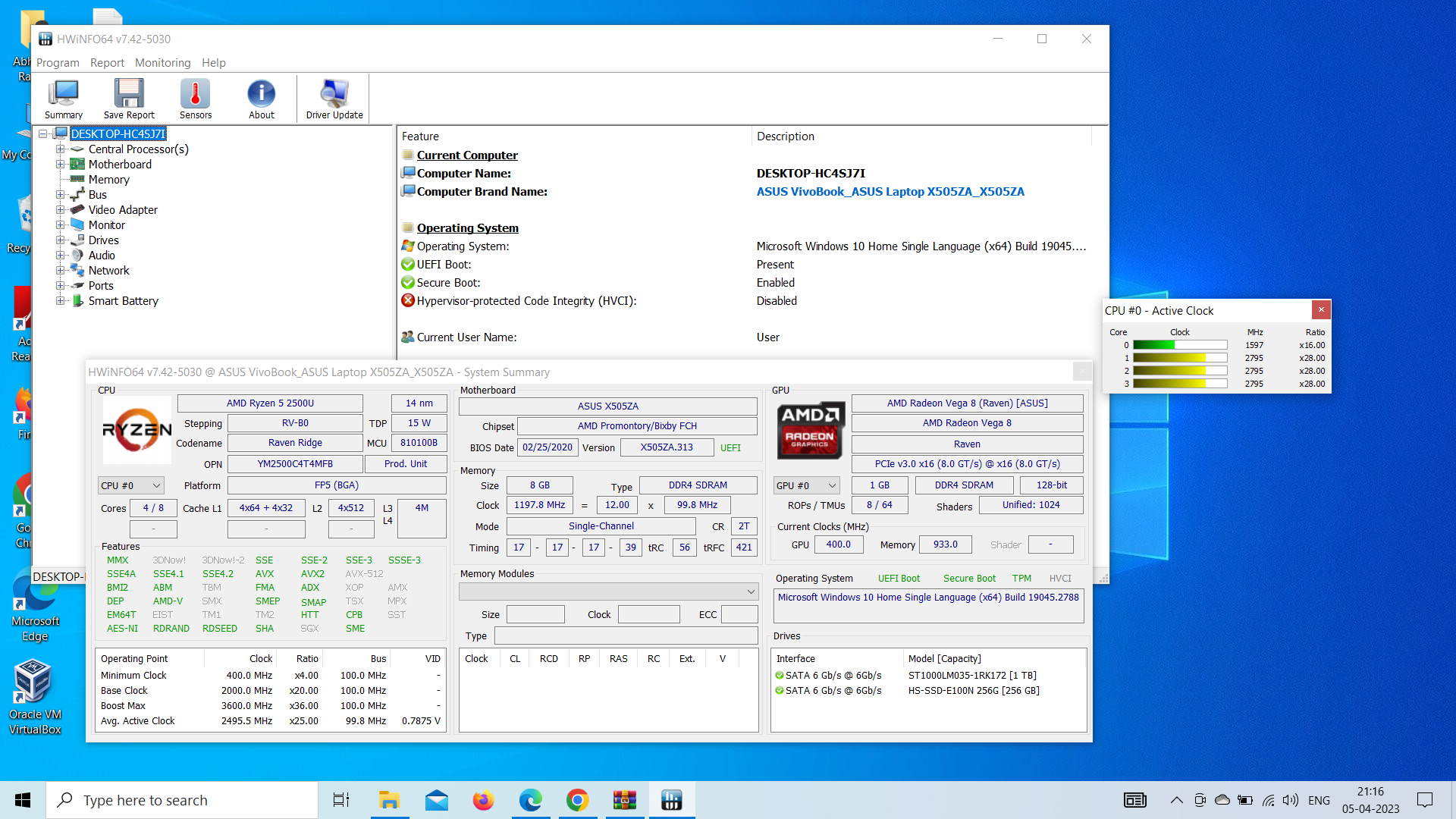
****

Figure 1 This shows the software installed in your Windows

1. Launch HWiNFO64 and select "Sensors-only" mode to avoid unnecessary information.
2. Once the scan is complete, you will see a list of your hardware and software components and their details.
3. You can navigate through the different categories and subcategories to view the detailed information.
4. You can also customize the display of information by selecting the sensors and values you want to see.

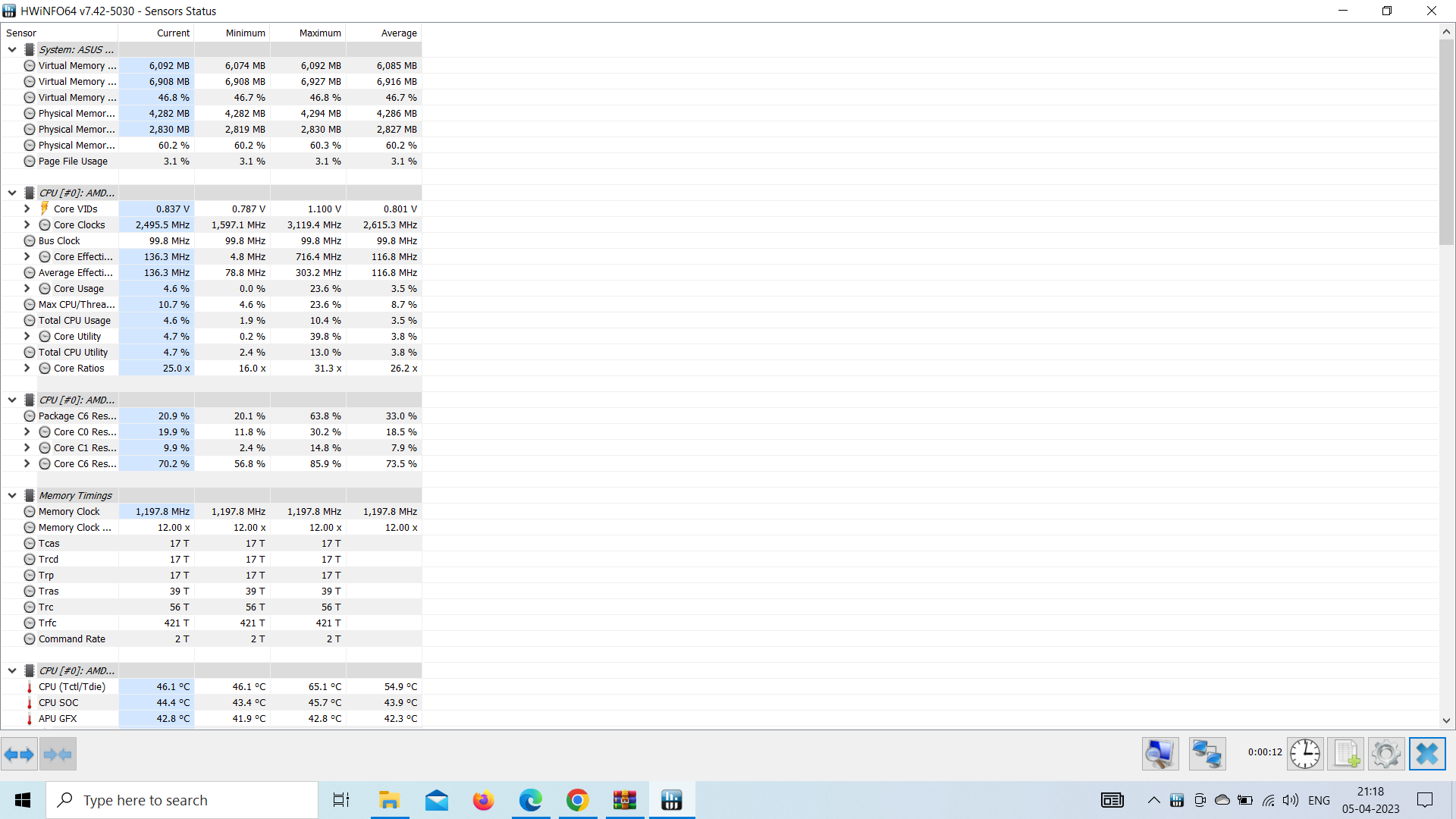


Figure 2 This shows the hardware installed in your Windows

It's important to be cautious while using HWiNFO64, as incorrect use can cause hardware damage. Make sure you read the warnings and instructions provided by the program before making any changes.

## 4.Reference/ Bibliography

1. https://h11dfs.com/the-best-open-source-digital-forensic-tools/
2. https://[www.techtarget.com/searchsecurity/definition/computer-forensics](http://www.techtarget.com/searchsecurity/definition/computer-forensics)
3. <https://eforensicsmag.com/forensic-investigation-of-storage-media/>
4. Tenable website: <https://www.tenable.com/products/nessus-vulnerability-scanner>
5. Nessus user guide: <https://docs.tenable.com/nessus/Content/UserGuide.htm>
6. HWiNFO64 review on TechRadar: <https://www.techradar.com/reviews/hwinfo64>

## 5. Github-link