

**Using desired Open-Source Software list all the security updates missing in your Window OS. Also, list all free system information about the hardware and software installed.**

**BY**

**Ankit Kumar**

**11914358**

**Roll No. :- 64**

**CA-3**

**Index**

**1. Introduction**

**1.1Objective of the project**

**1.2Description of the project**

**1.3Scope of the project**

**2. System Description**

**2.1 Target system description**

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

**3. Analysis Report**

**3.1 System snapshots and full analysis report**

**4. Reference/ Bibliography**

**1.Introduction**

**What is Open-Source Software?**

*Software for which source code is freely available with a license to study, change and further distributed to any other individual for any purpose is called open-source software. Open-Source Software is something which you can modify as per your needs, share with others without any licensing violation burden. When we say Open Source, source code of software is available publicly with Open-Source licenses which allows you to edit source code and distribute it.* *Open-source software is unique in that it is always released under a license that allows users to access, modify and redistribute the source code.*

**History of Open-Source**

*In the middle of the 20th century, computer software was included in the hardware and was not paid for separately. Early Unix versions were distributed free of charge to researchers, but could not be redistributed or modified. In the 1980s, AT&T stopped offering free and paid systems. Before 1974, software was not copyrighted. There is a difference in distributing only executable code and not source code. Richard Stallman protested, arguing that it was wrong not to edit programs written by others. Their concerns led to the creation of the Free Software Foundation and the concept of open source software.*

**About Open-Source Community**

*The open-source community is a collaborative network of individuals and organizations who create, maintain, and improve open-source software, characterized by openness, transparency, and inclusivity. It operates on a decentralized, peer-to-peer model with communication and collaboration through various channels. The community follows shared values and principles such as transparency, meritocracy, diversity, and inclusivity, fostering a culture of innovation and continuous improvement. The community has contributed to the development of popular software applications like Linux, Apache, and WordPress, and has been instrumental in advancing technologies such as cloud computing, big data, and AI.*

**Advantages of Open-Source Software’s**

* Open-Source Software is cost-effective and free to use, making it accessible for organizations or individuals with limited resources.
* It is customizable, allowing users to modify the software to collect specific information as required.
* Open-Source Software is flexible and can adapt to work with different hardware and software configurations.
* It provides transparency, as users have access to the source code and can verify the software's security and reliability.
* Open-Source Software is often supported by a community of developers, offering ongoing support and updates, and is compatible with different operating systems and software platforms.
  1. **Objective of the project**

*The objective of this project is to create a comprehensive list of security updates that are missing in the Windows operating system, as well as compiling a list of all available free system information about the hardware and software installed on the computer. The goal is to improve the overall security of the system by identifying and addressing any missing security updates, and to provide a detailed overview of the system's hardware and software components for troubleshooting and maintenance purposes.*

* 1. **Description of the project**

*This project involves creating a list of all the security updates that are not installed in the Windows operating system and compiling a list of free system information regarding the hardware and software that is installed on the computer. The objective is to improve the system's overall security by identifying and addressing any missing security updates. Additionally, the project aims to provide a detailed report of the computer's hardware and software components to assist in troubleshooting and maintenance tasks. The project may involve the use of various tools and methods for identifying missing security updates and gathering system information.*

* 1. **Scope of the Project**

*The project involves utilizing Open-Source Software i.e.,RHEL(Red Hat) to scan a Windows operating system and create a comprehensive list of all missing security updates. Additionally, the project aims to compile a list of all available free system information regarding the computer's hardware and software. The goal is to create a detailed report that includes all identified security vulnerabilities and necessary updates. The compiled list of free system information will provide a comprehensive overview of the computer's hardware and software, including details such as the processor, RAM, hard drive capacity, and installed software. Ultimately, the project aims to improve the security and overall functionality of the Windows operating system.*

**2. System Description**

**2.1 Target system description**

* *The target system is a Windows-based operating system that requires an update of its security features.*
* *The system administrator will use RHEL (Red Hat Enterprise Linux) Open-Source Software to identify all missing security updates.*
* *RHEL will be installed on a separate system that is connected to the target Windows operating system.*
* *Once installed, RHEL will scan the target Windows operating system to identify missing security updates.*
* *RHEL will provide a comprehensive list of all security updates that are currently missing from the target system.*
* *The system administrator will review the list of missing updates and install them to improve the target system's security.*
* *RHEL will also gather free system information about the target system's hardware, including CPU, memory, and disk information.*
* *Additionally, RHEL will gather information about the software installed on the target system, including the operating system version, installed applications, and system configurations.*

*The system administrator will compile this information into a detailed report to assist in maintenance and troubleshooting tasks for the target system.*

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

* *The target system has a working internet connection to download the latest security updates.*
* *The RHEL Open-Source Software is installed and configured correctly on a separate system.*
* *The RHEL system has the latest security updates and patches installed to ensure accurate scanning of the target Windows system.*
* *The system administrator has the necessary credentials to access and scan the target Windows system.*
* *The target Windows system has no firewalls or other security measures that could block or interfere with the scanning process.*
* *The target Windows system has no critical hardware or software issues that could affect the scanning process.*
* *The system administrator has sufficient knowledge and expertise in using RHEL Open-Source Software to scan and identify missing security updates.*
* *The system administrator has sufficient knowledge and expertise in interpreting the system information gathered by RHEL to create a detailed report.*
* *The system administrator will follow best practices and industry standards when installing security updates and making system changes based on the report.*

**3. Analysis Report**

**3.1 System snapshots and full analysis report**

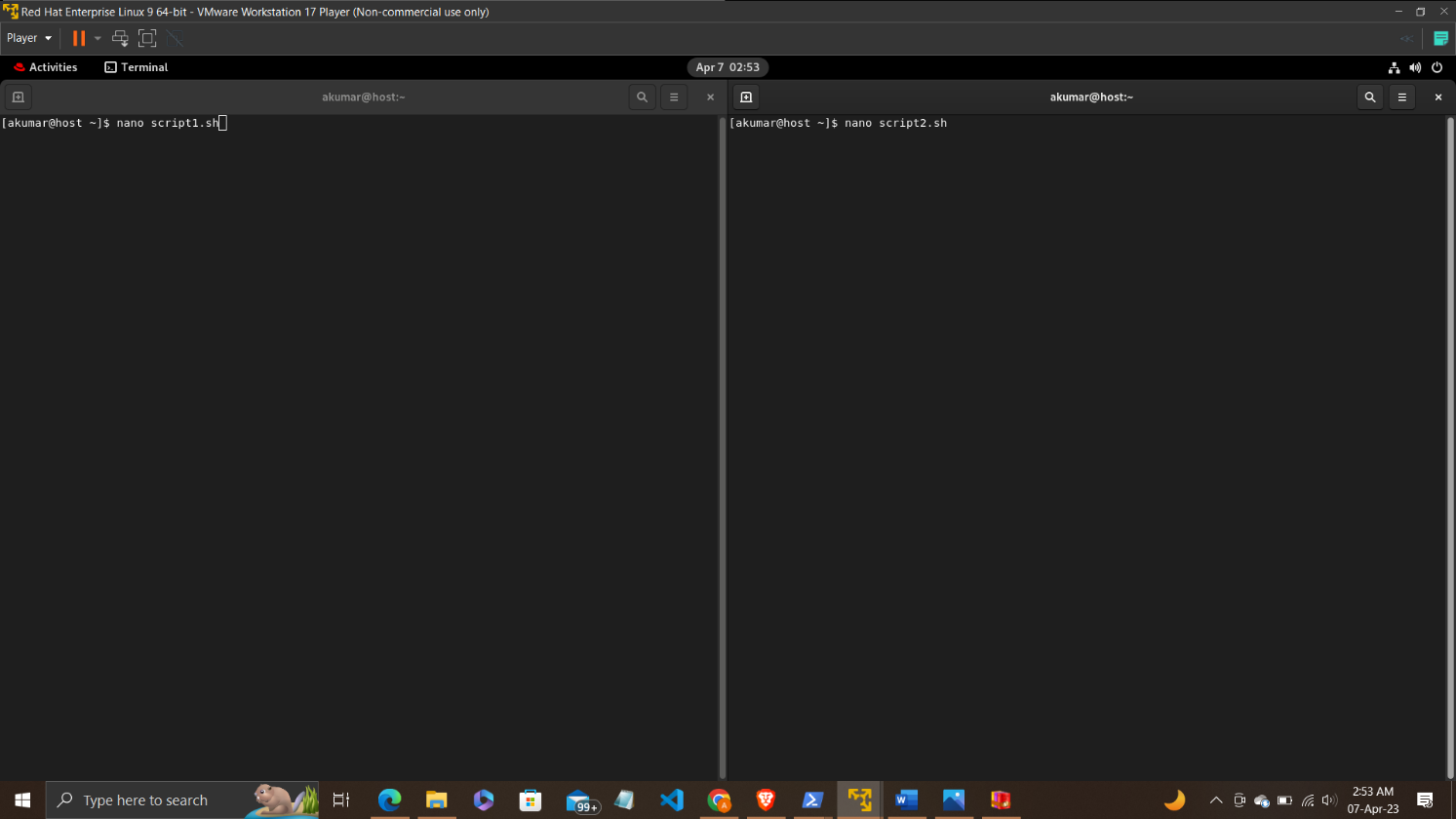
****

Figure .Creating two scripts (script1 & script2)

*Here, I have created two scripts in two different terminals in RHEL i.e., script1 & script2. Script1 is for showing list of missing security updates of my windows operating system. And Script2 is for showing the list of all free system information about the hardware and software installed.*

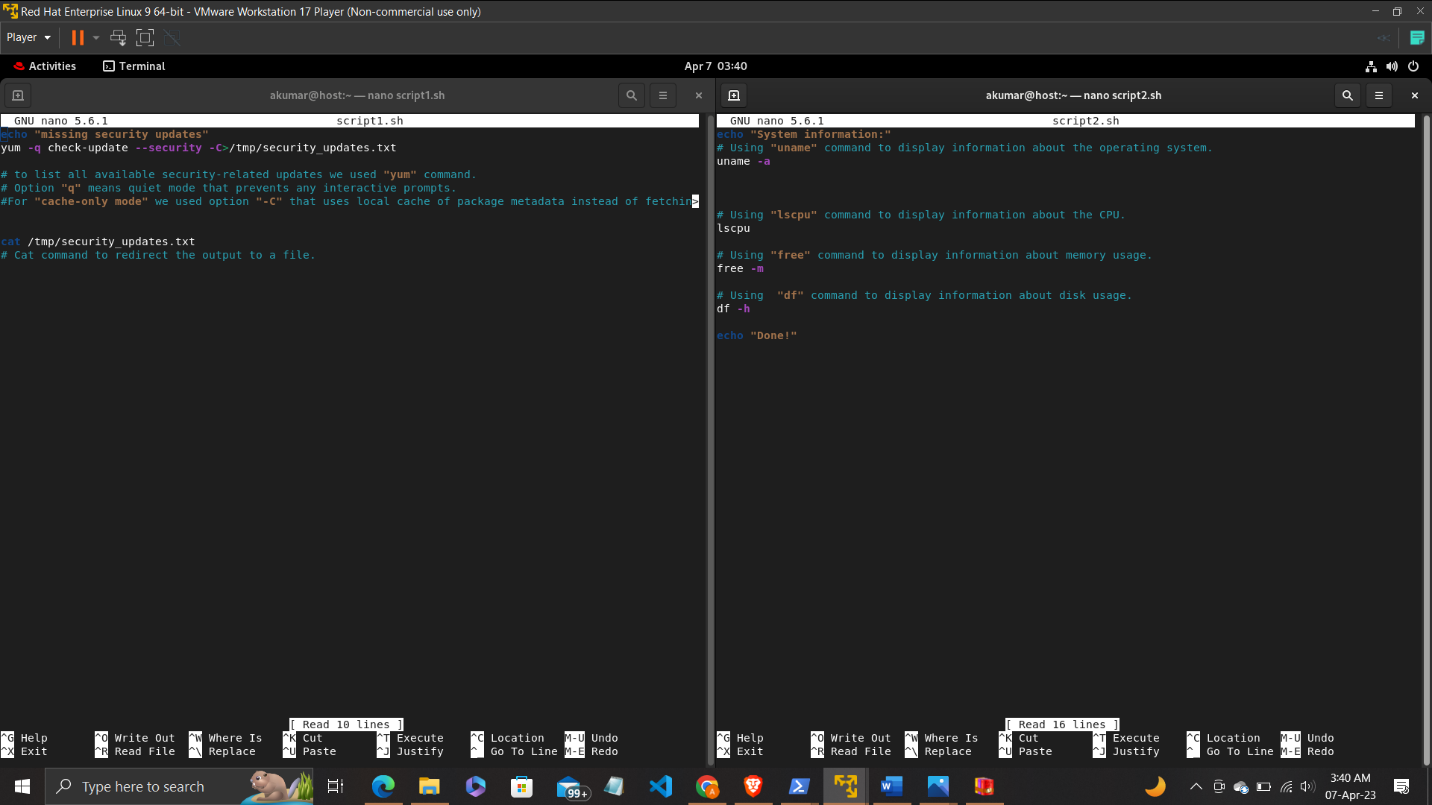


Figure .commands within both scripts

*In script1, we used command “yum -q check –security -C>/tmpsecurity\_updates.txt”.*

* *“yum” command to list all available updates that are security related.*
* *"-q" option means "quiet mode", which prevents any interactive prompts.*
* *“--security" option filters the results to show only security-related updates.*
* *"-C" option means "cache-only mode", which uses the local cache of package metadata instead of fetching new metadata from a remote repository.*

*In script2, we used commands like uname -a, lscpu, free -m & df -h.*

* *Used the "uname" command to display information about the operating system.*
* *Used the "lscpu" command to display information about the CPU.*
* *Used the "free" command to display information about memory usage.*
* *Used the "df" command to display information about disk usage.*

A screenshot of a computer

Description automatically generated with medium confidence

Figure .Granting execution Permission

*Granting script1 and script2 the execution permission*

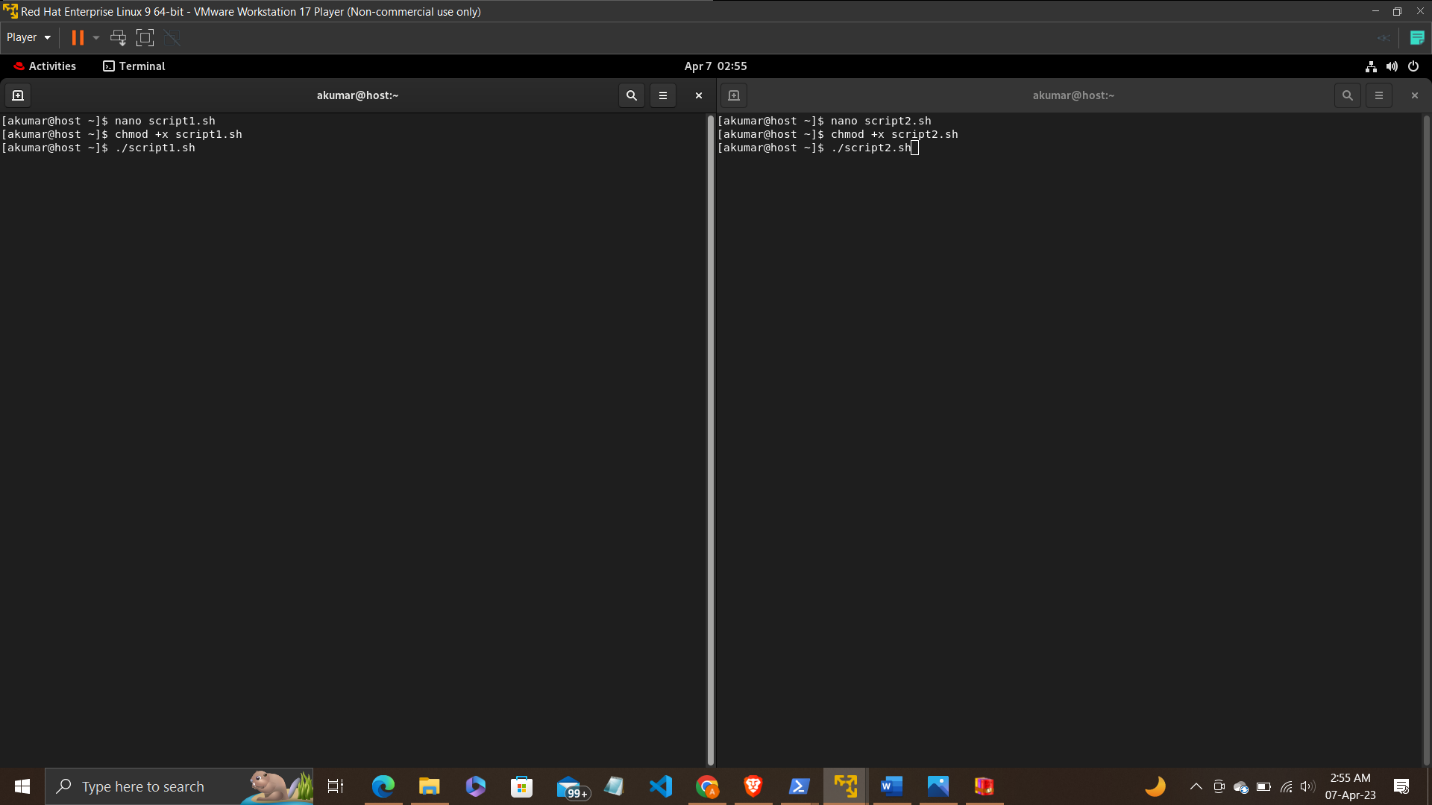
**

Figure . Execution Command

*This will execute the script and run the commands contained within it.*

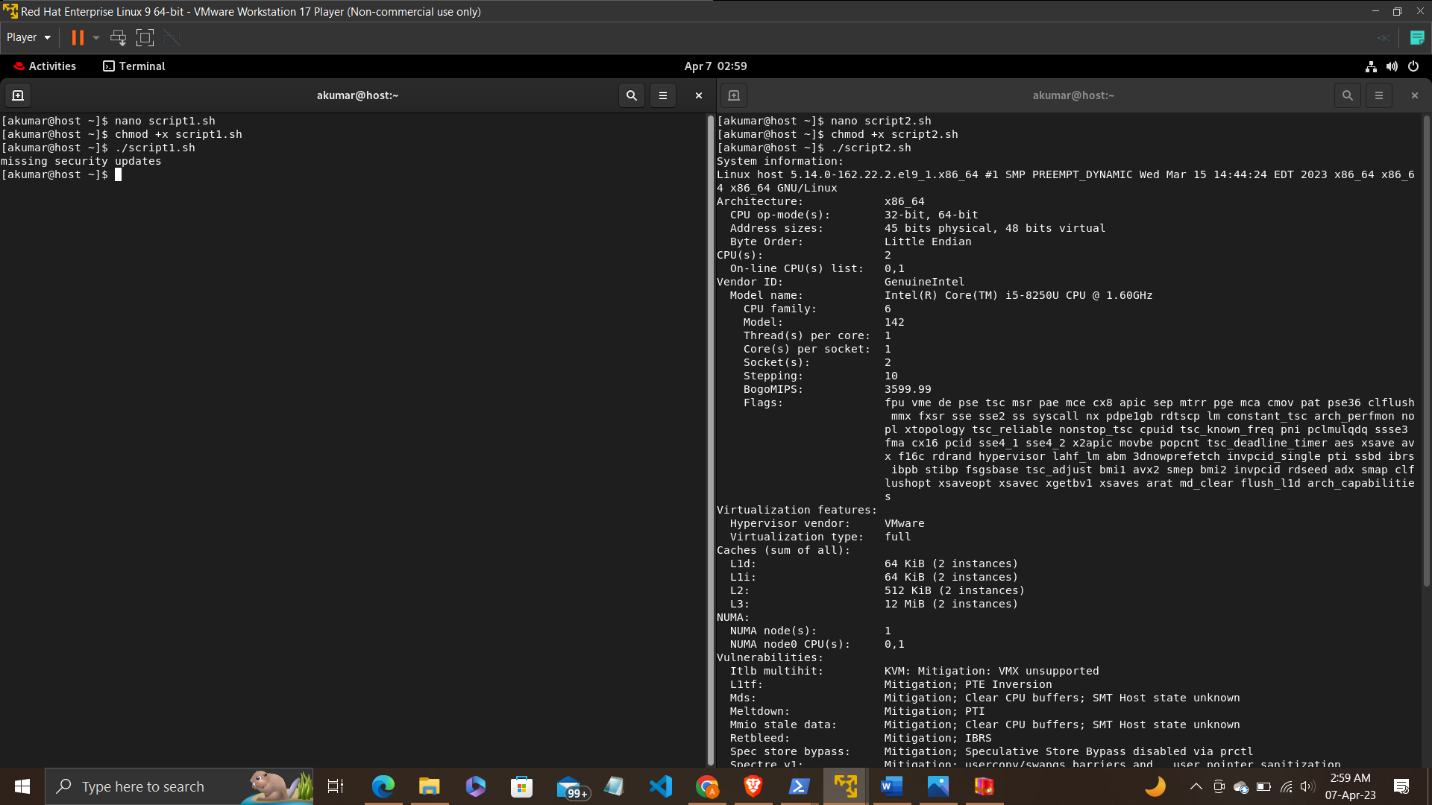
****

Figure .Output of scripts-I (script1 & script2)

Outputs of both Scripts

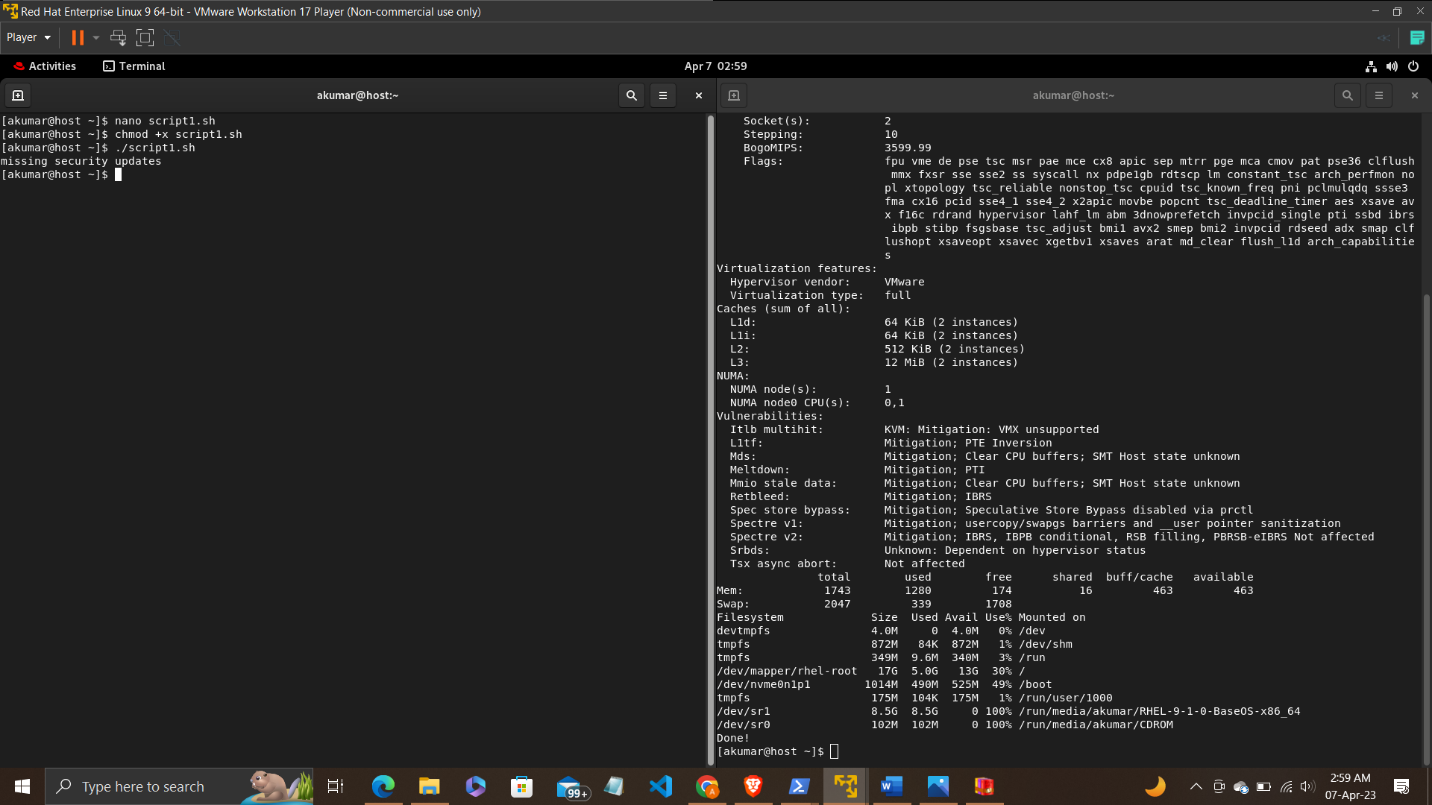
****

Figure .Output of scripts-II (script1 & script2)

These two figures show the output of both the scripts.

**4. Reference/ Bibliography**

*GitHub project link:-* [*https://github.com/Ankit045106/INT301-CA3-ANKIT-11914358*](https://github.com/Ankit045106/INT301-CA3-ANKIT-11914358)

*These references are the links for open-source software which can be used to perform the same task.*

* <https://www.wsusoffline.net/>
* <https://opmantek.com/network-management-software/open-audit/>
* <https://www.belarc.com/products/belarc-advisor>
* <https://www.flexera.com/products/software-vulnerability-management/personal-software-inspector/>