Assignment 6

Lavanya Bhambure MITU20BTCS0150 LY ISA 1

**Title:** Kali Linux

**Problem Statement**: Downloading and installing Kali Linux on the system

**Theory:**

Kali Linux is a popular and widely used open-source Linux distribution specifically designed for penetration testing, digital forensics, and ethical hacking purposes. It is maintained and funded by Offensive Security, a cybersecurity training company.

Here are some key features and characteristics of Kali Linux:

1. Penetration Testing Tools: Kali Linux comes pre-installed with a vast array of cybersecurity tools and software used for various aspects of penetration testing and ethical hacking. These tools help security professionals and ethical hackers identify vulnerabilities in computer systems, networks, and applications.

2. Debian-Based Distribution: Kali Linux is built on top of the Debian Linux distribution, which provides a stable and well-maintained foundation for the operating system.

3. Regular Updates: Kali Linux is actively maintained, and its developers regularly release updates and new versions to ensure that it stays up to date with the latest security tools and vulnerabilities.

4. Customization: Kali Linux is highly customizable, allowing users to install additional tools or remove unnecessary ones according to their specific needs.

5. Live Boot Capability: You can run Kali Linux as a live system from a bootable USB drive or DVD without installing it on your computer. This makes it convenient for security professionals to carry out security assessments on various systems without leaving any trace.

6. Forensics Tools: In addition to penetration testing tools, Kali Linux includes a wide range of forensic tools for analyzing and recovering data from computer systems and storage devices.

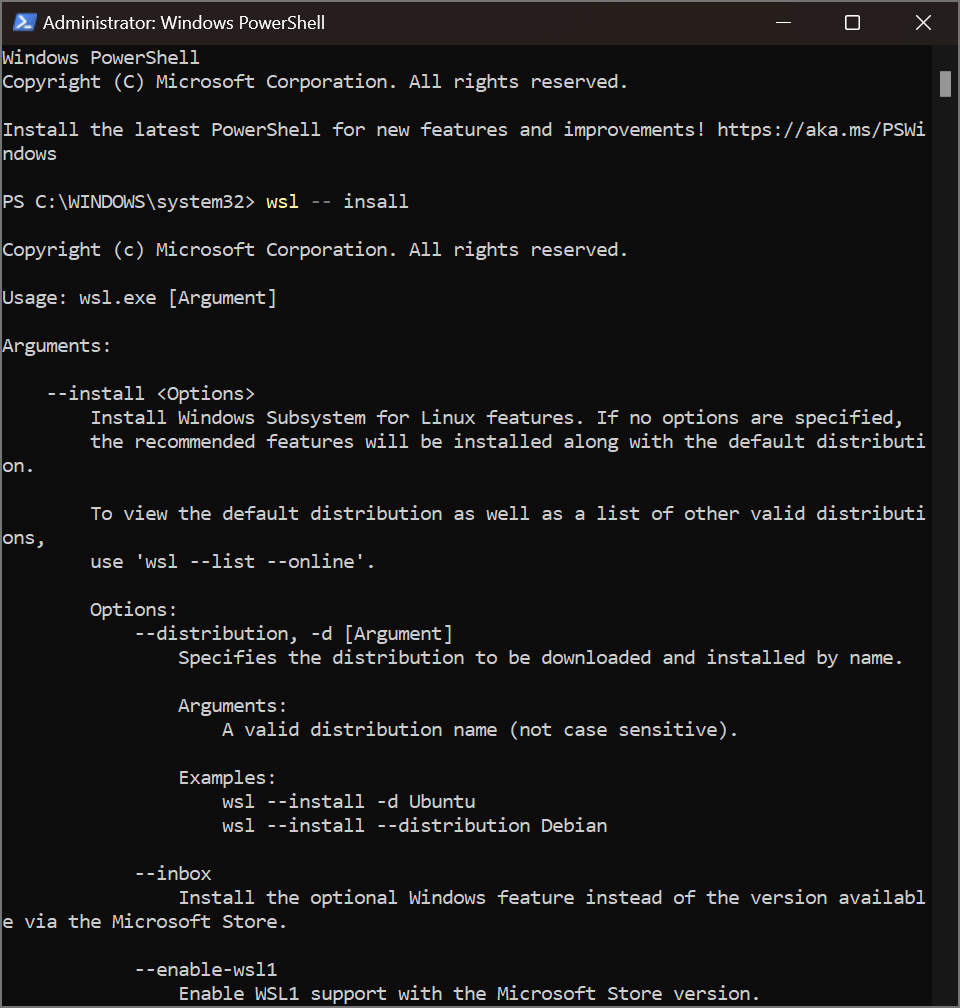
7. Community and Documentation: Kali Linux has a large and active user community, which provides support, tutorials, and documentation to help users make the most of the distribution.

It's important to note that while Kali Linux is a powerful tool for cybersecurity professionals and ethical hackers, it should only be used for legitimate and legal purposes, such as security assessments and testing on systems and networks that you have permission to access. Unauthorized use of Kali Linux or its tools for malicious purposes is illegal and unethical. Always ensure that you have the necessary permissions and follow ethical guidelines when using Kali Linux or any other cybersecurity tools.

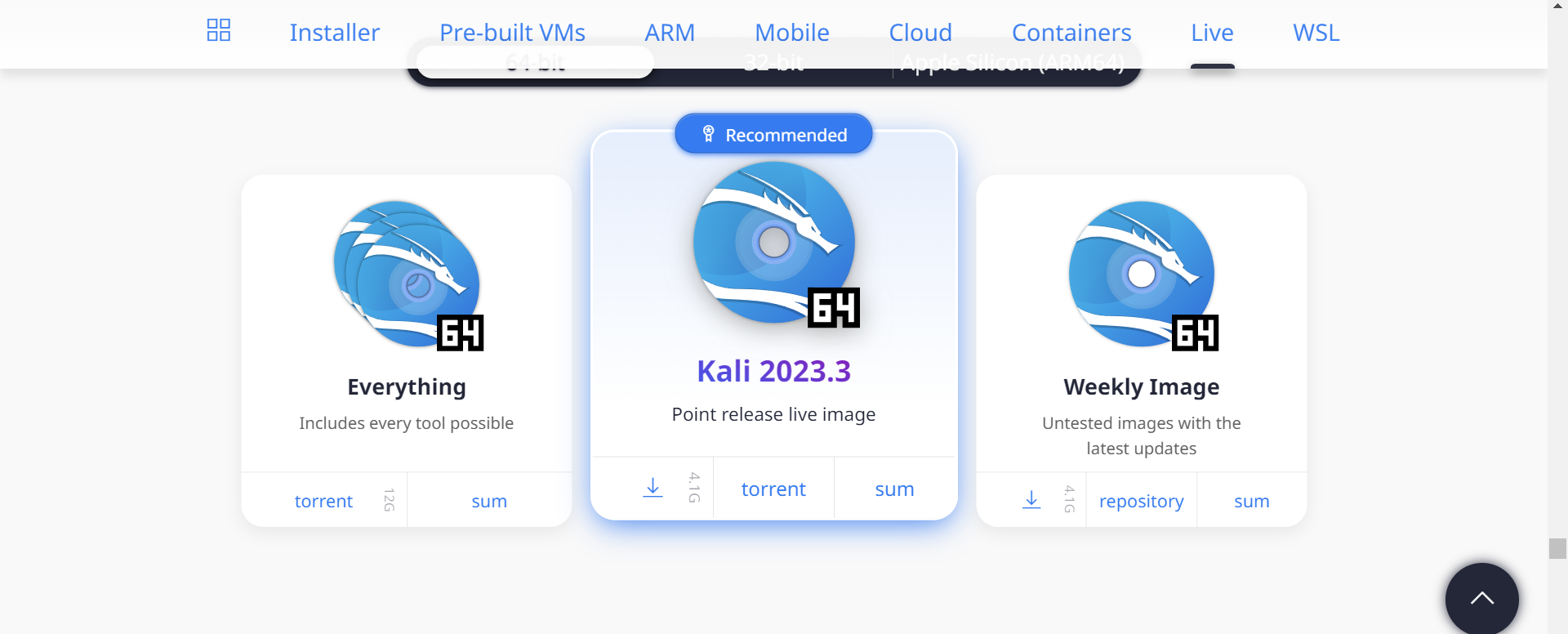
**Steps to install Kali Linux on windows**

1. Open opowershell in administrator mode and run

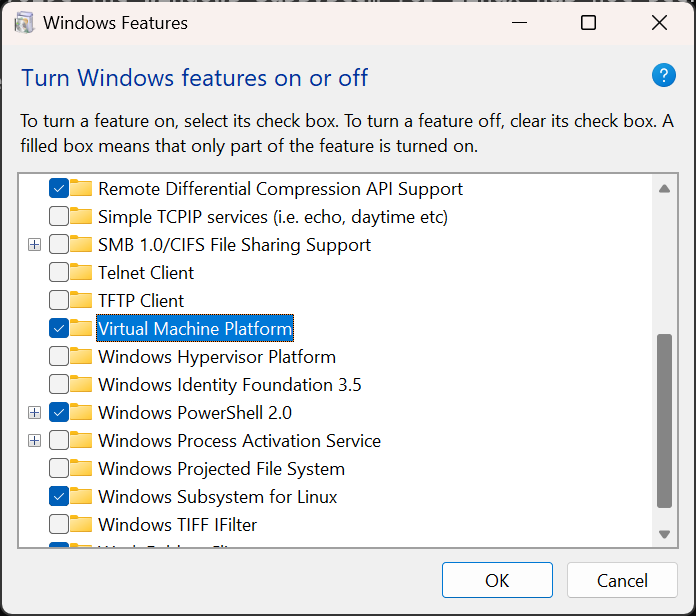
wsl – install

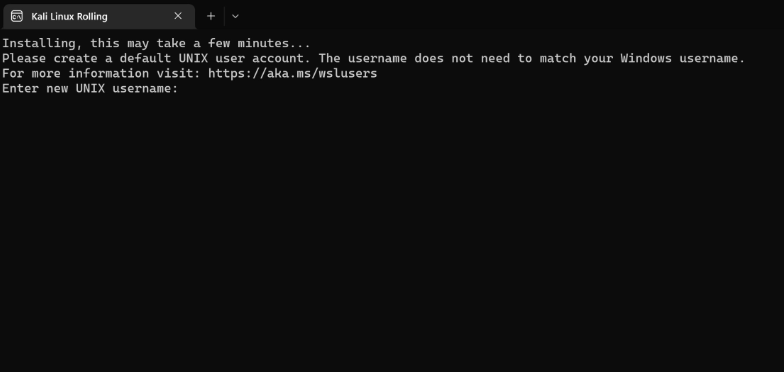


1. Now go to https://www.kali.org/get-kali and select WSL.

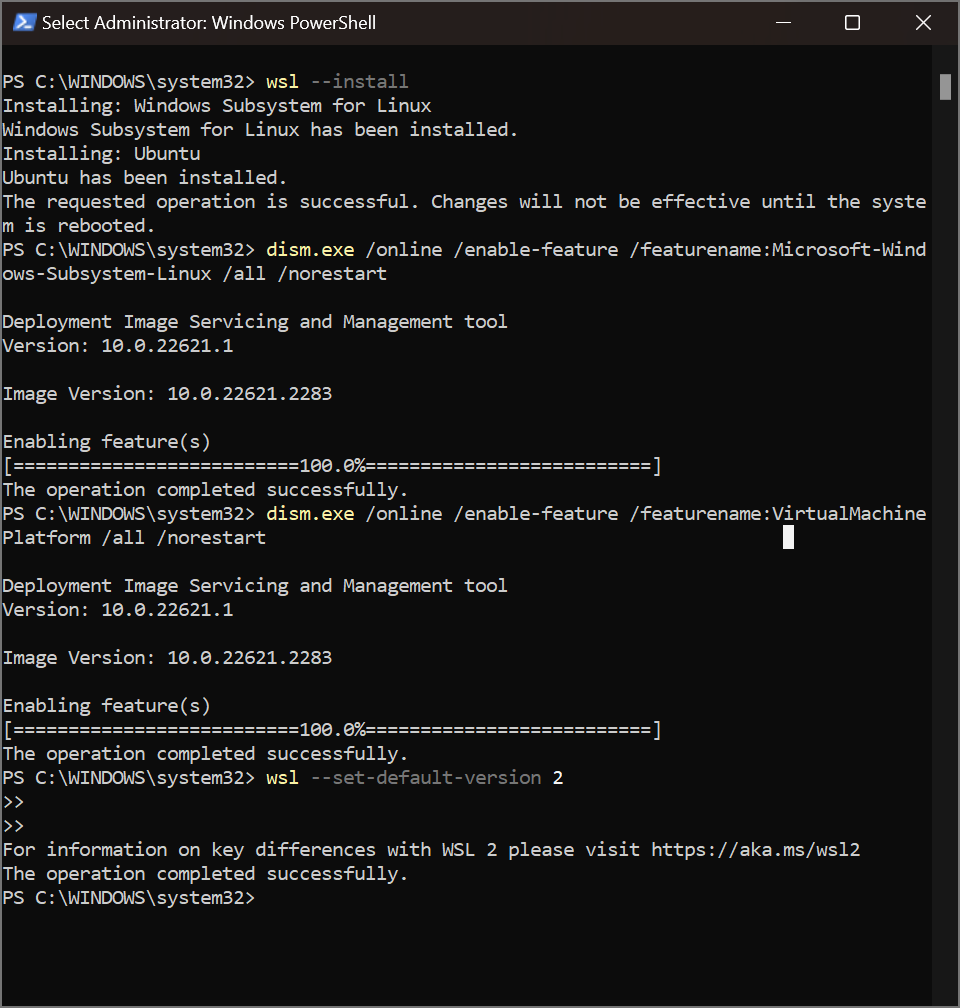


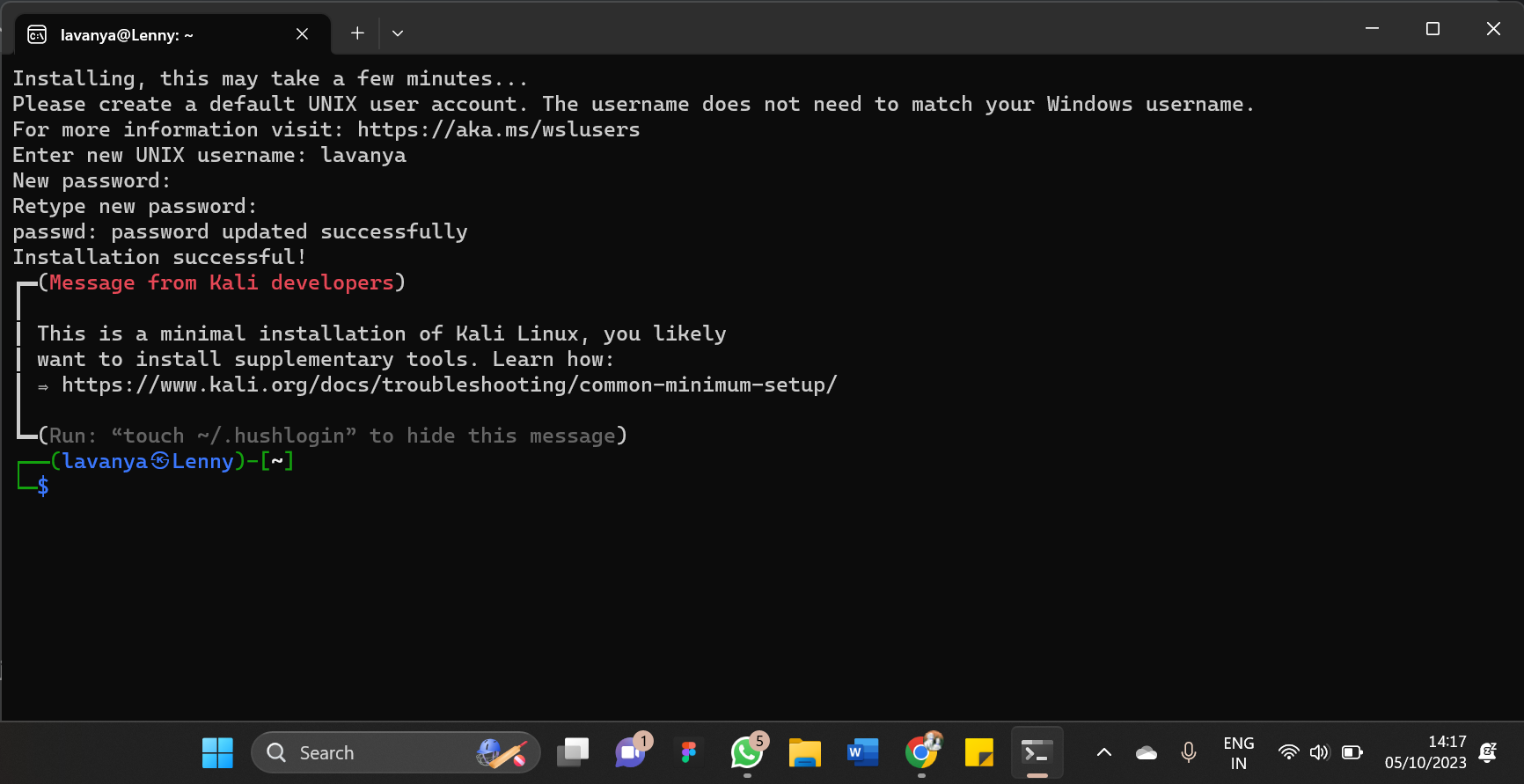
1. Now run sudo apt update and then run sudo apt install -y kali-win-kex By default, Kali will only run in terminal mode, but by using Kex, we can use Kali as normal. It may take a few minutes for Kex to install, so be patient. Once complete, run kex --win -s Now enter the password you set a few moments ago and for demo purposes, say no on the view-only password option.



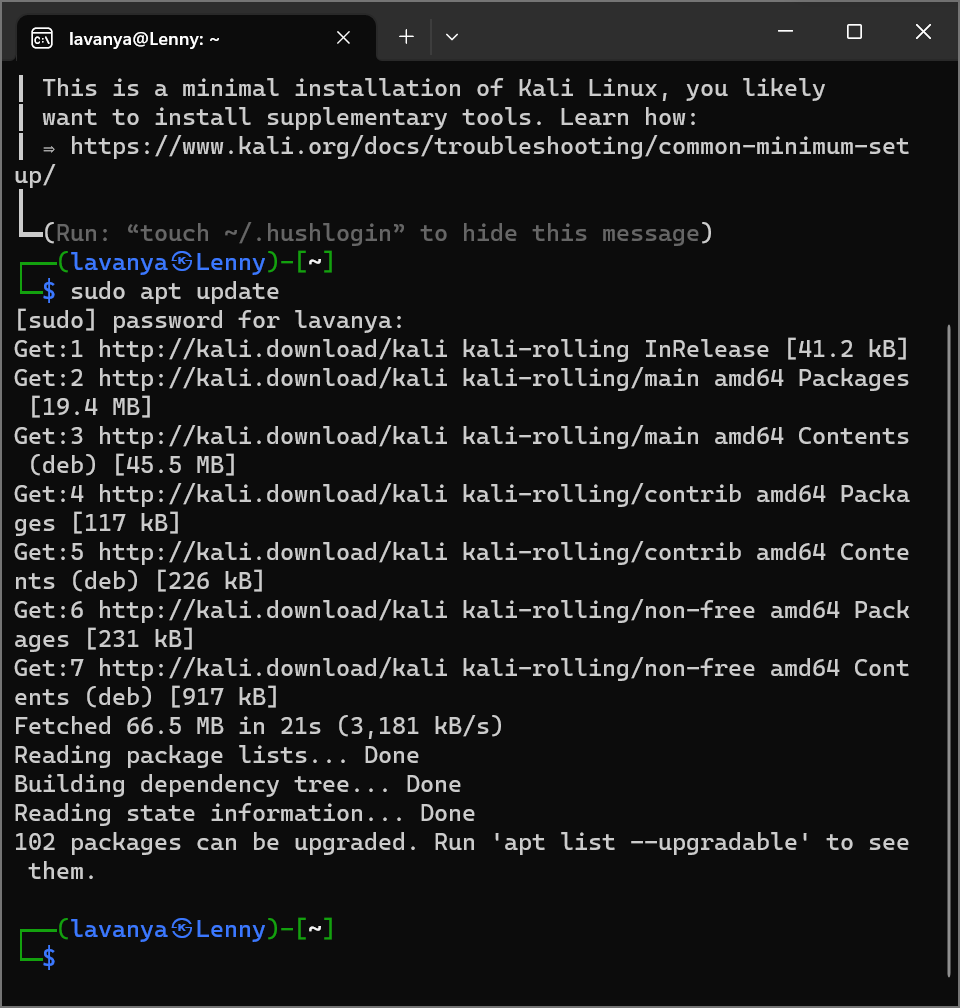


Installing the requirements

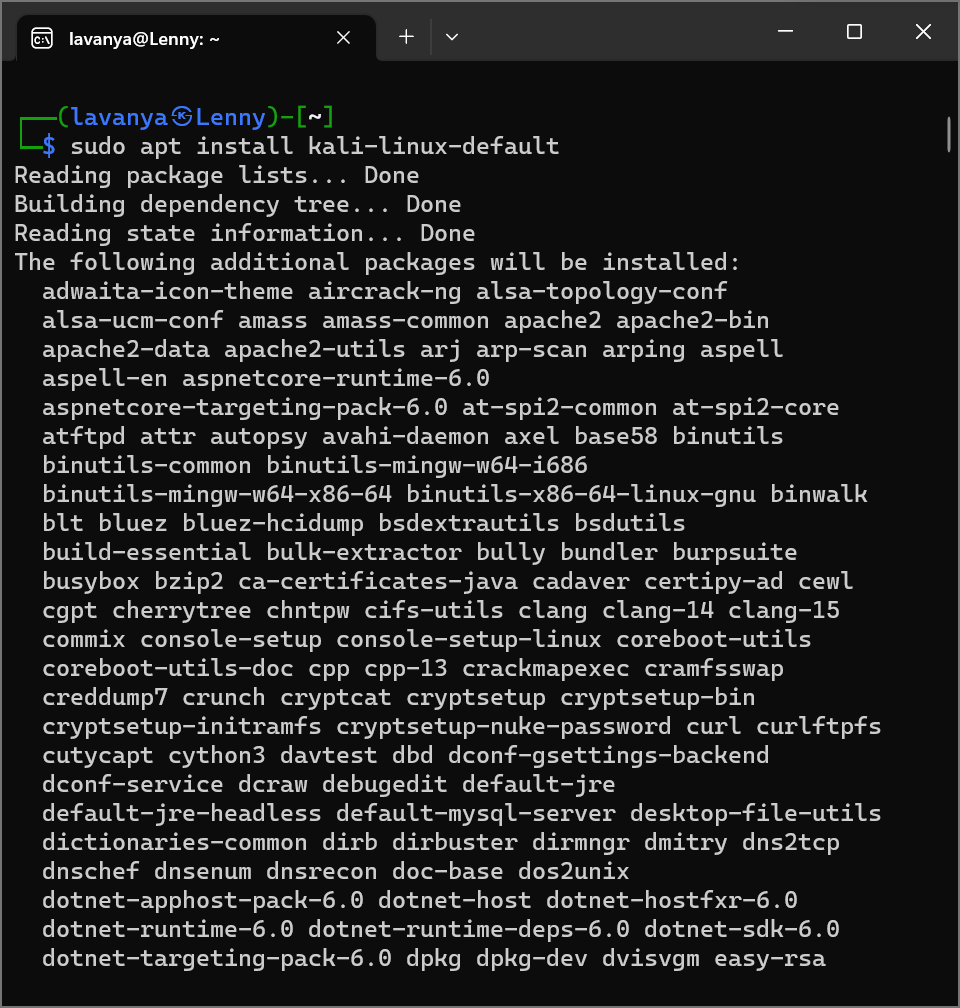




Sudo apt update



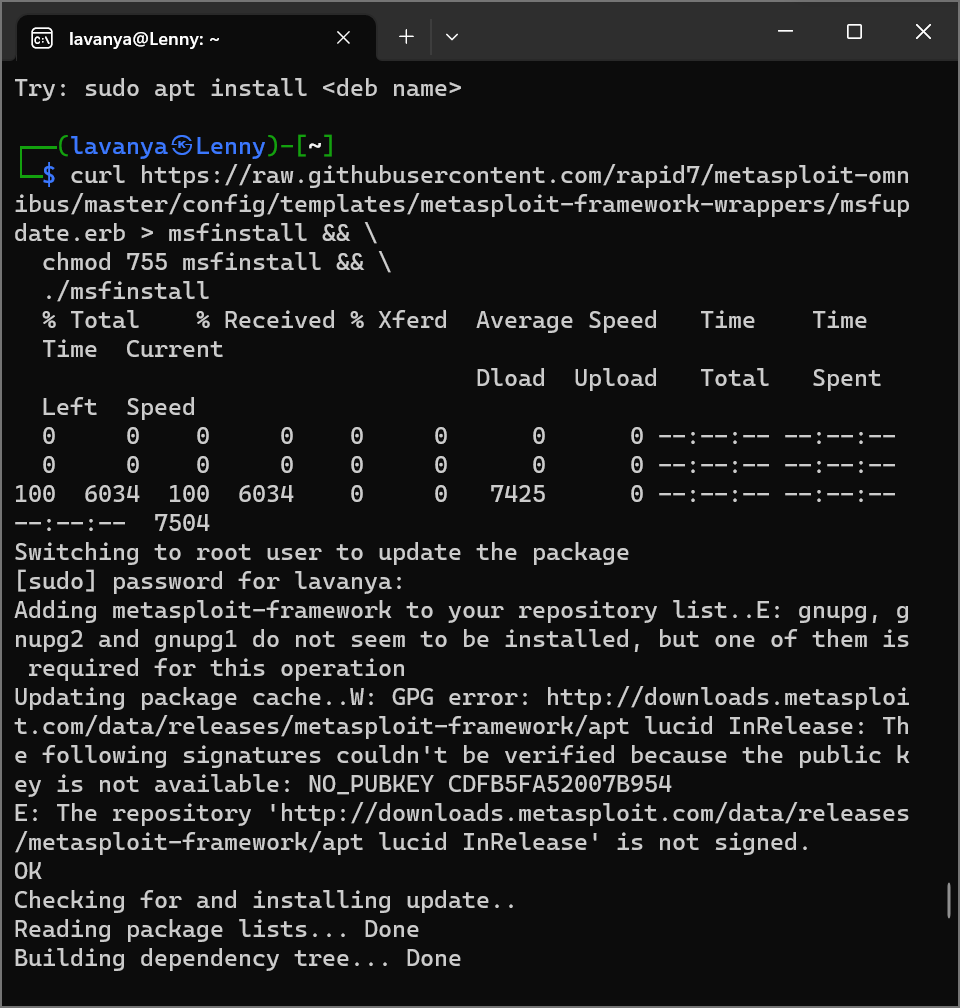
1. Installing additional tools



**Virtual Box**

****

**Installing Metasploit**

****

**Conclusion:**

We have successfully downloaded kali linux.