**Lab #1: Kali Linux Installation**

Points: 100

Task 1: Installation

Install Kali Linux.

Ensure the system has 2-4 GB of RAM.

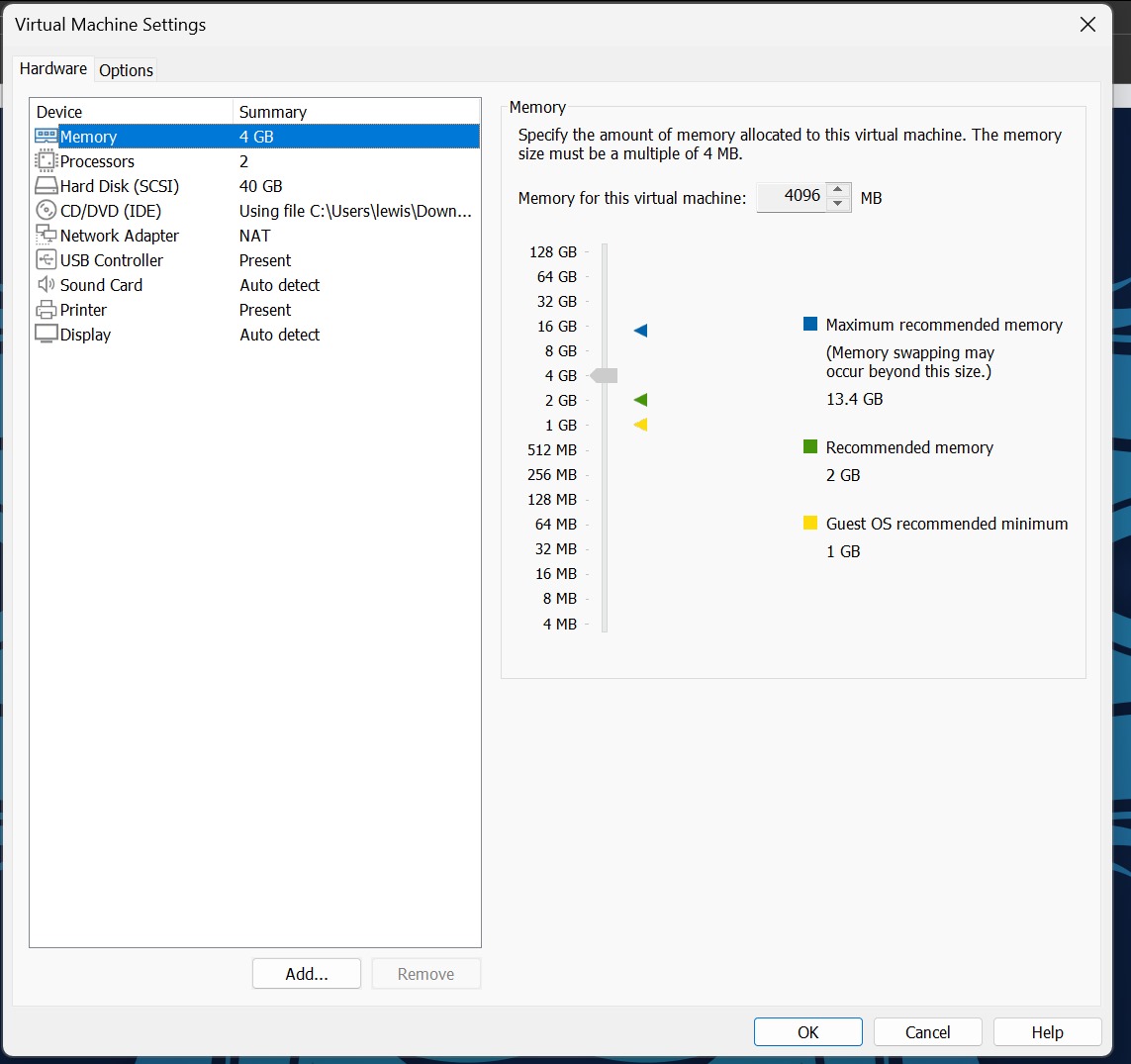
Allocate 40-60 GB of storage for Kali Linux.

Set up the Network Adapter as NAT.

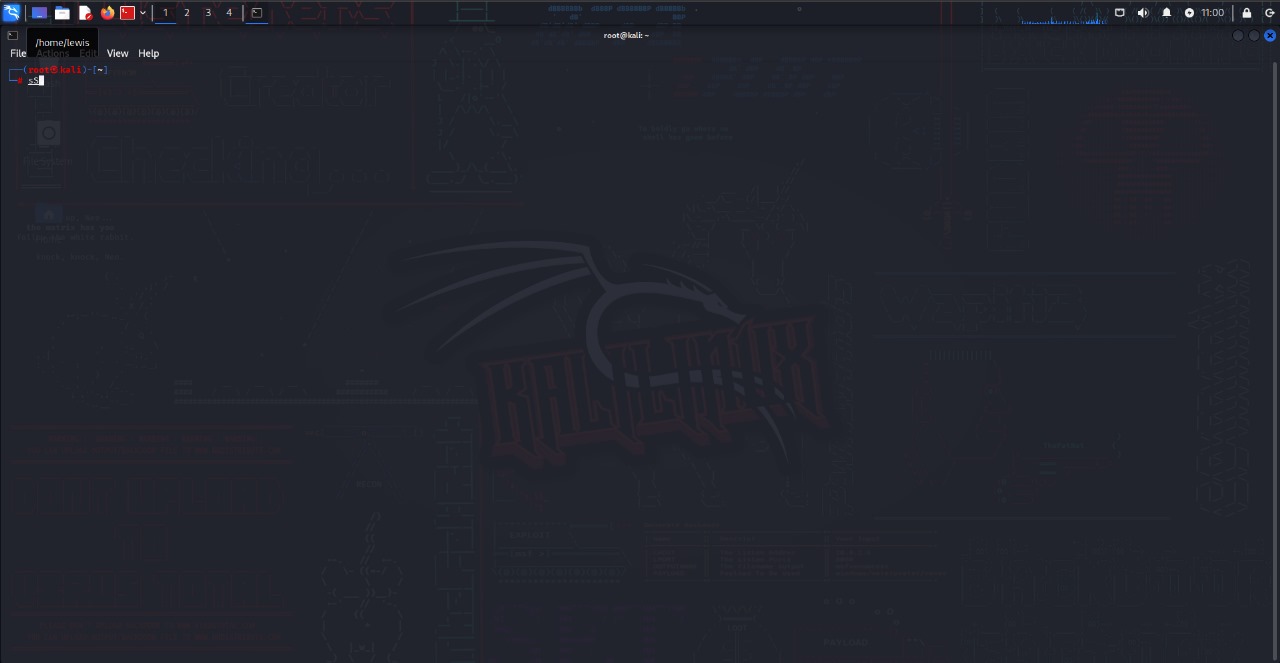
Update the system.

Task 2: Screenshots

Print Screen 1.0: VMware Settings.



Print Screen 2.0: Kali Linux has been installed.



**Theoretical Part**

**Describe in 300-350 words the purpose of Kali Linux.**

Kali Linux, previously known as BackTrack Linux, stands as a potent and specialized open-source Linux distribution meticulously crafted for advanced Penetration Testing and Security Auditing. This robust operating system serves as a dedicated toolkit, empowering security professionals to assess and evaluate the security of diverse systems, networks, and applications.

In the realm of Penetration Testing and Security Auditing, Kali Linux proves its worth by providing security experts with an extensive toolkit. This toolkit encompasses a rich array of tools, configurations, and automations, streamlining the testing process and allowing users to focus on the task at hand instead of grappling with intricate setup and configuration procedures.

Kali Linux is not limited to a singular information security task; rather, it caters to a broad spectrum of activities. In the domain of Penetration Testing, it aids in the identification of vulnerabilities and their subsequent exploitation to assess system security comprehensively. Additionally, security professionals utilize Kali Linux for Security Research, delving into security flaws, vulnerabilities, and emerging threats.

Moreover, the operating system plays a crucial role in Computer Forensics, enabling the analysis of digital evidence in legal investigations. It also serves in Reverse Engineering, providing the tools needed to dissect software and hardware, unraveling their inner workings. Furthermore, Kali Linux is a go-to platform for Vulnerability Management, aiding in the identification and remediation of security weaknesses. Red Team Testing is yet another facet where Kali Linux shines, allowing the simulation of real-world attacks to evaluate the effectiveness of defenses.

Key features that set Kali Linux apart include an extensive toolset of over 600 carefully curated penetration testing tools, all available for free and open-source use. The operating system is customizable, empowering users to tailor it to their preferences, from the kernel to the user interface. With wide-ranging wireless device support, compatibility with various hardware is assured. The Kali Linux team operates in a secure development environment, ensuring trust and integrity through GPG-signed packages, maintaining authenticity and security. The inclusion of true multilingual support further accommodates users worldwide, solidifying Kali Linux as a cornerstone in the arsenal of cybersecurity professionals.

Sources:

[FAQ - Frequently Asked Questions | Kali Linux](https://www.kali.org/faq/)

[▷ What is Kali Linux | A Complete Beginner's Guide (mindmajix.com)](https://mindmajix.com/what-is-kali-linux)

[What is Kali Linux? | Kali Linux Documentation](https://www.kali.org/docs/introduction/what-is-kali-linux/)