Kali:

A Comprehensive Guide for Beginner

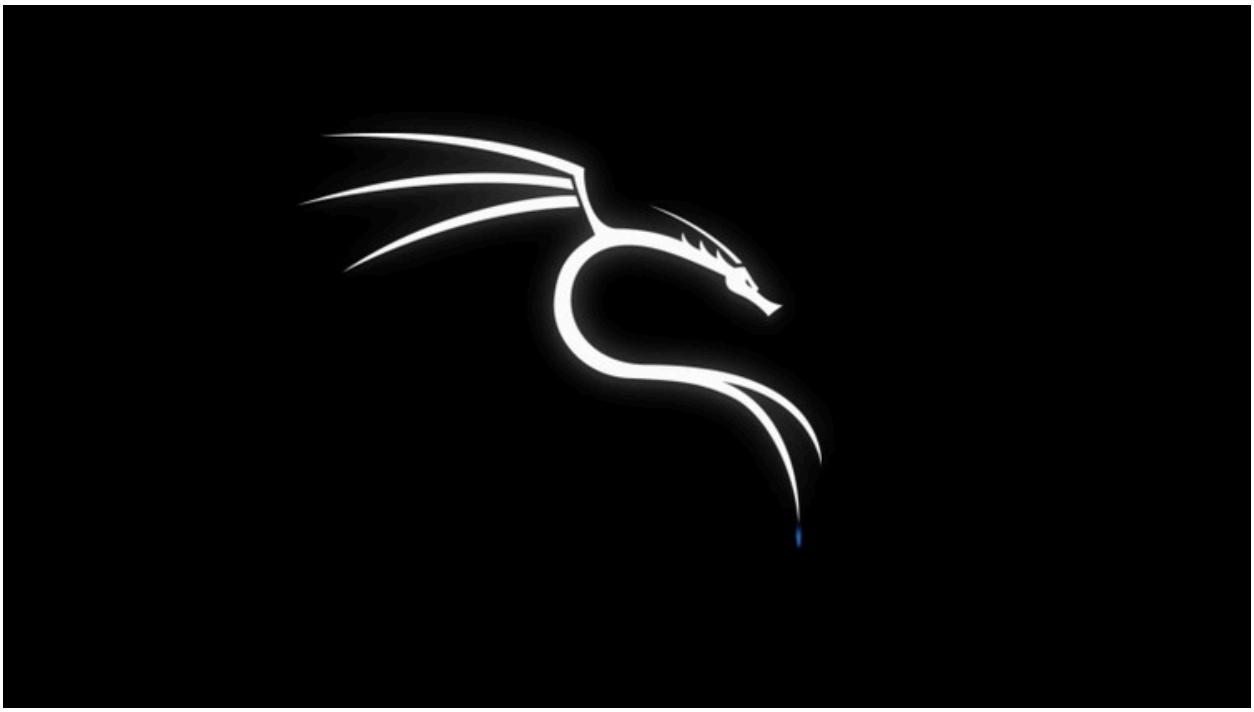

Table of content

1. Introduction to Kali Linux

Kali Linux is a specialized operating system designed for digital forensics and penetration testing. Developed and maintained by Offensive Security, Kali is based on Debian and is packed with a wide range of security tools that make it the go-to platform for ethical hackers and cybersecurity professionals.

One of the key features of Kali is its flexibility. It can be installed on a wide variety of hardware, from powerful servers to low-resource devices like Raspberry Pi. Additionally, Kali supports various platforms, including ARM, virtualized environments, and cloud instances, making it accessible in almost any environment.

Visit this website for further more information

https://www.kali.org/docs/

2. Basic Setup kali Linux

Visit this website for further more information

https://www.geeksforgeeks.org/how-to-install-kali-linux-in-vmware/

3. Basic kali linux Commands

3.1. Basic File Operations

3.1.1. Command: ls

- Command used to list directories and file

3.1.2. Command: cd <directory_name>

- Command used to navigate through directory

3.1.3. Command: mv <source_file_name> <destination_directory>

- Command used to move files to a defined destination directory.

3.1.4. Command: cp<source_file_name> <destination_directory>

- Command used to copy files.

3.1.5. Command: pwd

- Command used to display working directory.

3.1.6. Command: whoami

- Command used to return the current user's username.

3.2. Managing Files and Directories (rm, mkdir, rmdir)

3.2.1. Command: touch <file_name>

- Command used to create files in a directory.

3.2.2. Command: rm <file name>

- Command used to delete files and folders from directory.

3.2.3. Command: mkdir

- Command used to create a directory.

3.2.4. Command: rmdir

- Command used to remove the existence directory.

3.2.5. Command: nano/gedit

- Command used to open files in nano.It is like a notepad in kali linux.

3.2.6. Command: grep

- Command used to find words in files.
- Eg**: nano <file_name> | grep "<word>"**

4. Introduction to kali linux tools

4.1. Installation Process of tools

4.1.1. upgrade and update apt

- Command: **sudo apt update && sudo apt upgrade**

4.1.2. Installing file

a. Download with apt

- Command: **sudo su**
- **apt install <file _name>**

b. Download with official website

- Command: **sudo su**
- Download with it from it's official website the downloaded file is in .deb prefix and open it's file path on terminal and use command;
- **ls**
- **dpkg -i <file_name.deb>**

c. Download wit github or any third party site

- Copy the github link of file and use command:
- **Git clone <github-link>**

4.2. Tools most used in kali

4.2.1. Nmap

- NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

4.2.2. Wireshark

- Wireshark is a widely-used network protocol analyzer that captures and displays data traveling over a network in real-time. It allows users to inspect network traffic at a

granular level, making it invaluable for troubleshooting, analyzing network performance, and investigating security issues. Wireshark supports a wide range of protocols, making it a versatile tool for network administrators and security professionals.

4.2.3. Metasploit

- Metasploit is a comprehensive framework for penetration testing and security research. It provides tools for exploiting known vulnerabilities in systems, allowing security professionals to assess the security of networks and applications. Metasploit includes a vast database of exploits, payloads, and auxiliary modules, making it an essential tool for ethical hacking and vulnerability assessment.

4.2.4. Burp Suite

- Burp Suite is a powerful platform for web application security testing. It includes a set of tools for performing various security tests, such as vulnerability scanning, attack simulations, and penetration testing. Burp Suite's user-friendly interface and extensive features make it a popular choice for both beginners and experienced security professionals in identifying and mitigating web application vulnerabilities.

4.2.5. Hydra

- Hydra is a fast and flexible password-cracking tool used to perform brute force attacks on login pages and network services. It supports numerous protocols and can be used to test the strength of passwords by attempting to log in with various username and password combinations. Hydra is often employed in security assessments to identify weak or compromised credentials, helping to strengthen system security