Practical No. 1

Aim: Introduction to Kali Linux.

1. Introduction:

Operating System is the main system software which is responsible for the flawless working of the machine. Some Operating Systems are designed for some specific purposes. Though we could use them for anything we want to, but they have some special tools or services available feasibly to its users which makes it a good OS for the specific purpose. Like we generally prefer Windows in case of gaming as most of the games are available for windows itself. Likewise, we prefer mac OS for designing related purposes as most of the designing software is easily available for mac and can be used flawlessly. In the same way when we have an OS for Network Security, Digital Forensics, Penetration testing, or Ethical Hacking named Kali Linux.

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts, Penetration testers, or in simple words, it is for those who work under the umbrella of cybersecurity and analysis. The official website of Kali Linux is Kali.org. It gained its popularity when it was practically used in Mr. Robot Series. It was not designed for general purposes, it is supposed to be used by professionals or by those who know how to operate Linux/Kali.

2. Advantages:

a. It has 600+ Penetration testing and network security tools pre-installed.
b. It is completely free and open source. So, you can use it for free and even contribute for its development.
c. It supports many languages.
d. Could be easily used with Raspberry Pi.

3. Disadvantages:

a. It is not recommended for those who are new to linux and want to learn linux.(As it is Penetration Oriented)
b. It is a bit slower.
c. Some software may malfunction.

Kali Linux is to be used by those who are professional penetration testers, cybersecurity experts, ethical hackers, or those who know how to operate it. In simple words, if you know how to use Linux and its terminal commands, architecture, system, and file management then you are good to go with Kali Linux. And if you are not, then we will recommend you first start with ubuntu distribution and get your hands-on Linux and after sufficient practice, you could give Kali Linux a try. This

will not only save your time of searching on the internet but also will make you use it with ease. However, if you're a professional penetration tester or studying penetration testing, there's no better toolkit than Kali Linux.

4. **Why Kali Linux?**

If you are interested in penetration testing or cybersecurity stuff you need some specific tools to perform some tasks which come pre-installed and settled up in Kali Linux so you may directly use them without doing any configuration. Or in case if one wants to check the vulnerabilities on a website or want to know security-related bugs in any application then it is great to go with Kali Linux.

Many people think that Kali is a tool for hacking or cracking social accounts or web servers. This is one of the biggest myths about Kali Linux. Kali Linux is just another Debian distribution with a bunch of networking and security tools. It is a weapon to train or defend yourself not to attack anyone. Kali Linux was designed mainly for professionals. It is for those who want to get their hands in Penetration Testing, Cyber Security, or Ethical Hacking. It is a powerful tool and in case, not used properly, it may lead to losses even.

5. **Kali Linux Tools**

Kali Linux is a Linux based operating system, mostly used in penetration testing. *Kali.org* has recently released its new update with some extra functionalities. There are different types of tools that are present in Kali Linux to perform different operations.

Types of tools in Kali Linux

i. **Information Gathering:** These software or applications have a job of collecting and formatting the data in a form that could further be used. This is similar to cookies used by different websites or your browsing history used by Google to personalize every advertisement and providing the best services to you. Kali operating system provides these tools to the developer and penetration testing community to help in gathering and formulating captured data.
Some of the tools are:

- Nmap
- Zenmap
- Stealth scan

Nmap is the most famous in these tools. Go to "Applications" then in "Information Gathering", you will find these tools.

ii. **Vulnerability Analysis:** Vulnerability is a state or condition of being exposed to the possibility of being attacked or harmed in one or the other way. These tools are used to check a system or machine for any kind of flow and vulnerability available in them, which could lead to any security breach and data loss. These

tools also help in fixing those vulnerability as identification make the user aware of the flow.

For example: If windows release its new operating system, before providing it into the end-user they send for vulnerability analysis and fixes.

Some of the tools:

- Bed
- Ohrwurm
- Powerfuzzer
- Sfuzz
- Siparmyknife

All these tools are very common in the community. Go to "Applications" then in "Vulnerability Analysis", you will find these tools.

iii. **Web Application Analysis:** Web Application is a dynamic response web page that helps in a better and interactive client-server relationship. These tools identify and access websites through the browser to check any bug or loophole present, which could lead any information or data to lose.

For example, there is a website with a payment gateway then these web analyzers check if sufficient authentication and authorization present of the site.

These web application uses:

Some of the tools are:

- Burpsuite
- Httrack
- Sqlmap
- Vega
- Webscarab
- Wpscan

Burpsuite, vega, and web scarab are some most famous tools. Go to "Applications" then in "Web Application Analysis", you will find these tools.

iv. **Database Assessment:** These applications are made to access the database and analyse it for different attacks and security issues. These assessment shows some opportunities for improvement and changes. They develop a report of the analysis done on the database system. They perform: Configuration checking, examining user account, privilege and role grants, authorization control, key management, data encryption.

Some of the tools are:

- Bbqsl
- Jsql injection
- Oscanner
- Sqlmap
- Sqlninja

- Tmscmd10g

Sqlmap is the most famous database assessment tool. This tool injects SQL injection for scanning, detecting, and exploitation. Go to "Applications" then in "Database Assessment", you will find these tools.

v. **Password Attacks:** These are basically a collection of tools that could handle the wordlist or password list to be checked on any login credentials through different services and protocols. Some tools are wordlist collectors and some of them are the attacker. Some of the tools are:
   - Crewl
   - Crunch
   - Hashcat
   - John
   - Medusa

   John the Ripper and Medusa are the most famous tools. Go to "Applications" then in "Password Attacks", you will find these tools.

vi. **Wireless Attacks:** These tools are wireless security crackers, like breaking wifi – routers, working and manipulating access points. Wireless attacks are not limited to password cracking these are also used in information gathering and knowing behavior of victims over the internet.
   For example, the Victim is connected to a compromised access point or a fake access point then it can be used as a Man-in-The-Middle attack.
   Some of the tools are:
   - Aircrack-ng
   - Fern- wifi –cracker
   - Kismet
   - Ghost Phisher

   Aircrack-ng and Ghost Phisher are the most famous tools. Go to "Applications" then in "Wireless Attacks", you will find these tools.

vii. **Exploitation Tools:** These tools are used to exploit different systems like personal computers and mobile phones. These tools can generate payloads for the vulnerable system and through those payloads information from the devices can be exploited.
   For example, the Victim's system is compromised using payloads over internet or installing it if physically accessible. Some of the tools are:
   - Armitage
   - Metasploit
   - Searchsploit
   - Beef xss framework

   The most famous tool is Metasploit (there are courses to learn Metasploit alone). Go to "Applications" then in "Exploitation Tools", you will find these tools.

viii. **Sniffing and Spoofing:** Secretly accessing any unauthorized data over network is sniffing. Hiding real identity and creating fake identity and use it for any illegal or unauthorized work is spoofing. IP spoofing and MAC spoofing are two famous and mostly used attacks. Some of the tools are:

- Wireshark
- Bettercap
- Ettercap
- Hamster
- Driftnet

The most used tool is Wireshark. Go to "Applications" then in "Sniffing and Spoofing", you will find these tools.

ix. **Forensics:** These tools are used by forensic specialist to recover information from any system or storage devices. This helps in collecting information during evidence searching for any cybercrime. Some of the tools are:

- Autopsy
- Binwalk
- Galleta
- Hashdeep
- Volafox
- Volatility

The most famous tool is Autopsy, it has also been used by security forces, many judicial and investigating officials. Go to "Applications" then in "Forensics", you will find these tools.

x. **Social Engineering:** As the name suggests these tools generate similar services that people use in daily life and extract personal information using those fake services. These tools use and manipulate human behaviour for information gathering.
For example, Phishing is one of the examples of social engineering, in this, a similar looking home page of any social platform is created and then login details are compromised. Some of the tools are:

- SET
- Backdoor-f
- U3-pwn
- Ghost Phisher

The most famous social engineering tool is SET. Go to "Applications" then in "Social Engineering Tools", you will find these tools.

Conclusion: Thus we have studied the basics of Kali Linux.