Title- Exploring Kali Linux and the inbuilt tools for reconnaissance and ethical hacking.

What is Kali Linux?

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.Kali Linux was released on the 13th March, 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, adhering completely to Debian development standards.

- **More than 600 penetration testing tools included:** After reviewing every tool that was included in BackTrack, we eliminated a great number of tools that either simply did not work or which duplicated other tools that provided the same or similar functionality. Details on what’s included are on the Kali Tools site.
- **Free (as in beer) and always will be:** Kali Linux, like BackTrack, is completely free of charge and always will be. You will never, ever have to pay for Kali Linux.
- **Open source Git tree:** We are committed to the open source development model and our development tree is available for all to see. All of the source code which goes into Kali Linux is available for anyone who wants to tweak or rebuild packages to suit their specific needs.
- **FHS compliant:** Kali adheres to the File-system Hierarchy Standard, allowing Linux users to easily locate binaries, support files, libraries, etc.
- **Wide-ranging wireless device support:** A regular sticking point with Linux distributions has been supported for wireless interfaces. We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.
- **Custom kernel, patched for injection:** As penetration testers, the development team often needs to do wireless assessments, so our kernel has the latest injection patches included.
- **Developed in a secure environment:** The Kali Linux team is made up of a small group of individuals who are the only ones trusted to commit packages and interact with the repositories, all of which is done using multiple secure protocols.

Tools for reconnaissance

1. Nmap
2. AngryIP Scanner
3. WPScan
4. Nessus

Nmap

Nmap ("Network Mapper") is a free and open source utility 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. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Steps:

1. Nmap is preinstalled in kali linux, If you are on windows platform,Download and install Nmap https://nmap.org/download.html
2. Some basic commands on nmap.

Usage	Command
TCP SYN port scan-	nmap -sS <ip address>
To find UDP Ports -	nmap -sU <ip address>
OS fingerprinting -	nmap -O <ip address>

Angry IP Scanner

Angry IP scanner is a very fast IP address and port scanner. It can scan IP addresses in any range as well as any their ports. It is cross-platform and lightweight. Not requiring any installations, it can be freely copied and used anywhere.

1. Download angryip from following URL. https://angryip.org/download/
2. Type range of ip address to get resut.

WPScan

WPScan is an open source WordPress security scanner. You can use it to scan your WordPress website for known vulnerabilities within the WordPress core, as well as popular WordPress plugins and themes.

Command

```
wpscan --url <url of wordpress site >
```

Scan QR-CODE for video demonstration

Blogspot URL - http://phcet.rohanparab.com/BEIT/1

Video URL -https://youtu.be/wb4fJcZo6cI