**EXPERIMENT 1**

**Aim:** Study of Reconnaissance tools and utilities available in Kali Linux

**What is Kali Linux ?**

Kali Linux is a Debian-derived Linux Distribution designed for digital Forensics and penetration testing. 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](https://www.offensive-security.com/), a leading information security training company.

Kali Linux was released on the 13th March, 2013 by Mati Aharoni and Devon Kearns as a complete, top-to-bottom rebuild of [BackTrack Linux](https://www.backtrack-linux.org/), adhering completely to [Debian](http://www.debian.org/) development standards.

**Role /Use of Kali Linux :-**

**Benefits :-**

1. **Advanced Penetration Testing tools :** In the Kali Linux, more than 500+ advanced Penetration Testing tools are included. The tools of BackTrack Linux which are not up to the mark or repeated in many ways has been replaced in the Kali Linux system with the advanced Penetration testing tools.

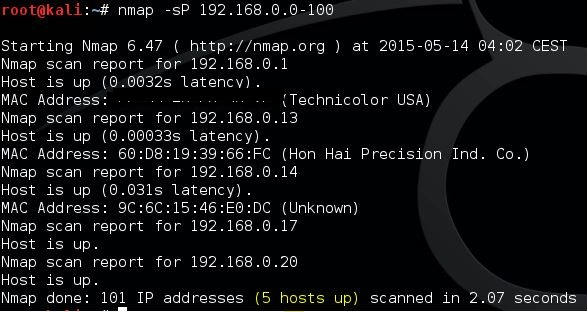
2. **Free Linux tool:** The Kali Linux system is totally free like the BackTrack Linux and will always offer their users the free life time services. This is huge plus factor which forces people to use this system.

3. **Open source Git:** This Kali Linux is openly sourced system and can be easily accessed by the users. All the codes in the Kali Linux can be viewed easily by the anyone and the open development source makes easy to view the development of coding at every step.

4. **Support:** Kali address to the File-system Hierarchy Standard, allowing Linux users to easily locate binaries, support files, libraries, etc. This is the very important feature of the Kali Linux that makes it stand out among the other Linux systems.

**List utilities used for ethical hacking typically for reconnaissance:**

**Nmap :**

****

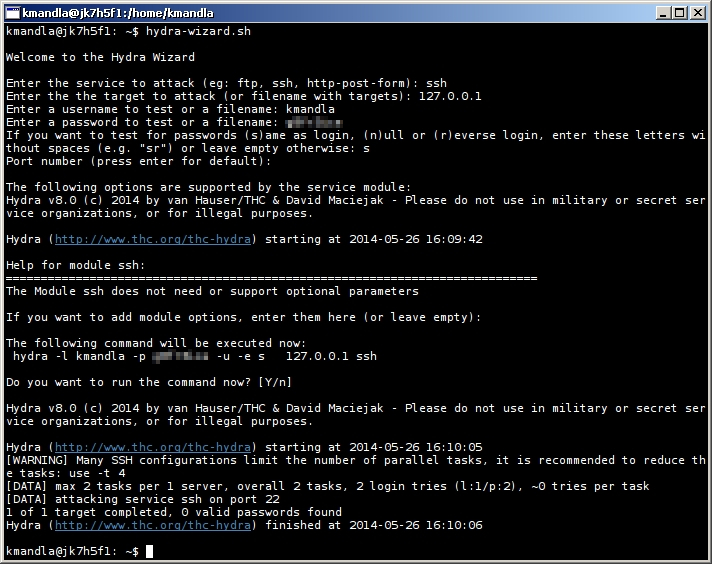
Network Mapper, also commonly known as Nmap, is an open-source network scanner that is used to recon/scan networks. Nmap uses raw IP packets in stealthy ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Many systems and network administrators also find it useful for tasks like:-

1. network inventory

2. managing service upgrade schedules

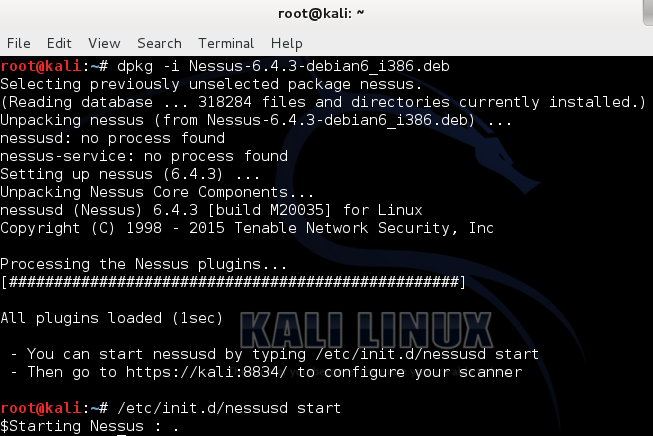
3. monitoring host or service uptime

**THC Hydra:**

****

When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, FTP, HTTP, HTTPs, SMB, several databases, and much more. it can be used to crack into web scanners, wireless networks, packet crafters, etc.

**Nessus :-**



Nessus is a remote scanning tool that you can use to check computers for security vulnerabilities. It does not actively block any vulnerabilities that your computers have but it will be able to sniff them out by quickly running 1200+ vulnerability checks and throwing alerts when any security patches need to be made.