EX NO: 6a   **STUDY OF KALI LINUX DISTRIBUTION**

Rollno: 241901058

AIM:
    To study about Kali Linux: an advanced penetrating testing and security auditing Linux distribution.

DESCRIPTION:
    Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools aimed at various information security tasks, such as Penetration Testing, 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. Features are listed below-
        • **More than 600 penetration testing tools**
        • **Free and Open Source Software**
        • **Open source Git tree:** 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:** It adheres to the Filesystem 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 support for wireless interfaces. Kali Linux supports many wireless devices.
        • **Custom kernel, patched for injection:** As penetration testers, the development team often needs to do wireless assessments and Kali Linux 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.

• **GPG signed packages and repositories:** Every package in Kali Linux is signed by each individual developer who built and committed it, and the repositories subsequently sign the packages as well.

• **Multi-language support:** It has multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.

• **Completely customizable:** It can be customized to the requirements of the users.

• **ARMEL and ARMHF support:** It is suitable for ARM-based single-board systems like the Raspberry Pi and BeagleBone Black**.**

SECURITY TOOLS:

Kali Linux includes many well known security tools and are listed below-
• Nmap
• Aircrack-ng
• Kismet
• Wireshark
• Metasploit Framework
• Burp suite
• John the Ripper
• Social Engineering Toolkit
• Airodump-ng

Aircrack-ng Suite:

It is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security:

• **Monitoring:** Packet capture and export of data to text files for further processing by third party tools.

• **Attacking:** Replay attacks, deauthentication, fake access points and others via packet injection**.**

• **Testing:** Checking WiFi cards and driver capabilities (capture and injection).

• **Cracking:** WEP and WPA PSK (WPA 1 and 2).

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

RESULT: Thus the study of Kali Linux for penetration testing and auditing has been done successfully