Experiment 0: Kali Linux Introduction

Objective

To introduce students to the Kali Linux operating system, familiarize them with basic Linux commands, and explore commonly used pre-installed cybersecurity tools.

Step-by-Step Procedure

Step 1: Install Kali Linux using VirtualBox or VMWare

1. Download Kali Linux ISO from https://www.kali.org/get-kali/.
2. Download and install VirtualBox or VMWare Workstation Player.
3. Open the VM software and create a new virtual machine with Debian 64-bit as the OS.
4. Allocate 2 GB RAM and 20 GB hard disk space.
5. Mount the Kali Linux ISO in the virtual optical drive.
6. Boot and install Kali Linux using graphical install.
7. Complete installation by configuring language, time zone, username, and password.
8. Restart the VM and log into the Kali desktop.

Step 2: Learn Basic Linux Commands

Open the Terminal and try the following commands:

- pwd: Print working directory
- ls: List directory contents
- cd: Change directory
- mkdir test: Create directory
- touch file.txt: Create file
- nano file.txt: Edit file
- rm file.txt: Remove file
- man ls: Manual for ls
- ifconfig: View network config
- sudo apt update: Update packages
- sudo apt install nmap: Install tool

Step 3: Explore Pre-installed Cybersecurity Tools

Navigate through Applications → Kali Linux to explore categories:

- **Information Gathering: nmap, whois**
- **Vulnerability Analysis: nikto, wpscan**
- **Exploitation: Metasploit**
- **Password Attacks: John the Ripper, Hydra**
- **Wireless Attacks: aircrack-ng**
- **Sniffing: Wireshark**
- **Web App Testing: Burp Suite**
- **Forensics: Autopsy**

Launch using terminal commands or from the Applications menu.

Expected Outcome

- Understand Kali Linux environment.
- Learn to use basic terminal commands.
- Identify and explore cybersecurity tools available in Kali.

Observations

Command/Tool	Purpose/Observation

Viva Questions

1. What is Kali Linux and why is it used?
2. List any three categories of tools available in Kali Linux.
3. What does the 'cd' command do in Linux?
4. How do you install software using the terminal in Kali?
5. Name one tool used for vulnerability scanning in Kali.

----------END----------

1.What is Kali Linux?

Kali Linux is a free, open-source **Linux distribution** specifically designed for **penetration testing**, **digital forensics**, and **cybersecurity research**. It is maintained and developed by Offensive Security, a trusted provider of cybersecurity training and certifications.

Why is Kali Linux Used?

Kali Linux is widely used by:

- **Ethical hackers (White-hat hackers)**
- **Cybersecurity professionals**
- **Security researchers**
- **Penetration testers**
- **Forensics investigators**

Key Features:

Feature	Description
Pre-installed Tools	Comes with 600+ tools (e.g., Metasploit, Nmap, Wireshark, Burp Suite, Hydra).
Focus on Security Testing	Built purely for offensive security, pen testing, and red teaming.
Custom Kernel	Patched for injection attacks and wireless testing.
Live Boot Support	Can run from USB without installation.
Flexible Platform	Runs on desktops, Raspberry Pi, VMs, and even Android (via NetHunter).
Forensics Mode	Does not auto-mount drives to avoid altering evidence.

Real-World Use Cases:

1. **Penetration Testing**

   Simulating real-world attacks on systems to find vulnerabilities.

2. **Network Scanning**

   Identifying open ports, services, and hosts using tools like Nmap and Netdiscover.

3. **Password Cracking**

   Using tools like John the Ripper or Hydra to test password strength.

4. **Wireless Network Attacks**

   Cracking Wi-Fi passwords using aircrack-ng suite.

5. **Web Application Testing**

   Detecting vulnerabilities like SQL injection or XSS using Burp Suite, Nikto, etc.

6. **Digital Forensics**

   Recovering deleted files, analyzing memory dumps using Autopsy, Volatility.

Kali Linux vs Parrot OS

Feature	Kali Linux	Parrot OS
Developer	Offensive Security	Frozenbox & ParrotSec
Primary Focus	Offensive Security (Pen Testing, Exploitation)	Offensive Security + Privacy + Programming
Tools Included	600+ pre-installed tools	500+ tools (includes pentesting + privacy tools)
Forensics Mode	Yes (Live boot forensic mode)	Yes
Resource Usage	Slightly heavier	Lightweight and optimized
User Interface	XFCE (default), GNOME, KDE	MATE (default), KDE
Anonymity Tools	Minimal (can be added manually)	Built-in (Tor, AnonSurf, I2P)

Feature	Kali Linux	Parrot OS
Ideal For	Ethical Hackers, Red Teams	Hackers + Privacy Advocates + Developers
Update Frequency	Rolling Release, Stable	More frequent community updates
Software Repository	Debian-based, custom Kali repo	Debian-based + Parrot custom repos

When to Use Kali Linux:

- You are preparing for **OSCP** or advanced certifications.
- You need a **well-supported professional toolkit**.
- You prefer **tool specialization** over general-purpose functionality.
- You are working in a **penetration testing lab** environment.

When to Use Parrot OS:

- You need both **pentesting + privacy/anonymity tools** out-of-the-box.
- You have **low system resources** (RAM, CPU).
- You're a **developer** who wants security-focused features and programming tools.
- You want a **more visually modern desktop environment**.

Real-World Scenario:

Use Case	Recommended OS
Read Team Internal Assessment	**Kali Linux**
Privacy-focused OSINT	**Parrot OS**
Mobile Pen Testing (NetHunter)	**Kali Linux**
Lightweight Security Dev OS	**Parrot OS**

2. List all categories of tools available in Kali Linux.

1. Information Gathering

Tools for collecting data about targets.

Examples:

- **nmap, netdiscover, dnsenum, whois, theHarvester, recon-ng**

2. Vulnerability Analysis

Identify known vulnerabilities in systems, services, and applications.

Examples:

- **nikto, wpscan, OpenVAS, Yersinia**

3. Web Application Analysis

Tools focused on web application security testing.

Examples:

- **Burp Suite, OWASP ZAP, sqlmap, w3af**

4. Database Assessment

Assess security of SQL and NoSQL databases.

Examples:

- **sqlmap, jSQL, NoSQLMap**

5. Password Attacks

Brute-force or dictionary attacks against login credentials.

Examples:

- **Hydra, John the Ripper, Hashcat, Crunch**

6. Wireless Attacks

Test and exploit wireless networks.

Examples:

- **aircrack-ng, Wifite, Reaver, Fern WiFi Cracker**

7. Reverse Engineering

Decompile, debug, and analyze binary programs.

Examples:

- **Ghidra, radare2, apktool, edb-debugger**

8. Exploitation Tools

Exploit known vulnerabilities in systems.

Examples:

- **Metasploit Framework, Armitage, BeEF, RouterSploit**

9. Sniffing & Spoofing

Intercept and modify network traffic.

Examples:

- **Wireshark, Ettercap, Bettercap, mitmproxy**

10. Post Exploitation

Tools used after gaining access to a system.

Examples:

- **Empire, Metasploit post modules, PowerSploit**

11. Forensics

Analyze and recover evidence from compromised systems.

Examples:

- **Autopsy, Binwalk, Volatility, Foremost**

12. Reporting Tools

Generate professional reports of findings.

Examples:

- **Dradis, MagicTree, Faraday**

13. Social Engineering Tools

Simulate phishing and other social engineering attacks.

Examples:

- **Social Engineering Toolkit (SET), King Phisher**

14. Fuzzing Tools

Send malformed input to discover application crashes or bugs.

Examples:

- **wfuzz, zzuf, peach**

15. Stress Testing Tools

Check system strength under heavy load or attack simulation.

Examples:

- **THC-SSL-DOS, Slowloris, hping3**

16. Hardware Hacking Tools

Tools for embedded system security and hardware testing.

Examples:

- **O.MG, RFID tools, USBKill**

17. Cryptographic Tools

Encrypt, decrypt, crack hashes and analyze cryptographic flaws.

Examples:

- **Hashcat, GPG, ciphertest**

18. Miscellaneous Tools

Various utilities that don’t fall under a specific category.

Examples:

- **xdotool, chisel, proxychains, netcat**

3. What does the 'cd' command do in Linux?

The cd command stands for **"change directory"**. It is used in Linux and other Unix based operating systems to **navigate between folders/directories in the file system**.

```
cd [directory_path]
```

Common Examples:

Command	Meaning
cd /home/kali	Go to the /home/kali directory
cd ..	Go **up one level** (parent directory)
cd ~ or just cd	Go to the **home directory**
cd /	Go to the **root** directory
cd Documents	Move into the Documents subdirectory
cd ../Downloads	Go up one level, then into Downloads

Example:

```
pwd
/home/kali

cd Desktop
pwd
/home/kali/Desktop
```

This shows how cd moves you from your home directory into the Desktop folder.

4 How do you install software using the terminal in Kali?

In Kali Linux (which is based on **Debian**), software is typically installed using the **APT package manager** via the terminal.

Basic Command to Install Software:

sudo apt install <package_name>

- sudo: Runs the command with superuser (root) privileges.
- apt: Stands for Advanced Package Tool, used to manage packages.
- install: Tells apt to install the specified package.
- <package_name>: The name of the software you want to install.

Step-by-Step Example: Install nmap

sudo apt update

sudo apt install nmap

Explanation:

1. apt update — Updates the package list to ensure the latest versions are used.
2. apt install nmap — Installs the nmap network scanning tool.

Other Useful APT Commands

Command	Description
sudo apt update	Refreshes the list of available packages
sudo apt upgrade	Installs the latest versions of packages
sudo apt remove <package>	Uninstalls a package
sudo apt search <keyword>	Searches for a package
apt list --installed	Lists all installed packages

⚠ **Tips:**

- Always run sudo apt update before installing to avoid broken dependencies.
- Ensure you're connected to the internet.
- Some tools (like Burp Suite) are already pre-installed in Kali.

5. Name One Tool Used for Vulnerability Scanning in Kali Linux.

Answer: nikto

What is Nikto?

Nikto is an open-source web server vulnerability scanner. It performs comprehensive tests against web servers for multiple types of issues.

Key Features of Nikto:

- Scans for over **6700 potentially dangerous files/programs**
- Checks for **outdated versions of servers**
- Tests for **server misconfigurations**
- Identifies **default files**, **scripts**, and **insecure HTTP headers**

Example Usage:

```
nikto -h http://192.168.1.105
```

This command scans the web server running at IP 192.168.1.105 for vulnerabilities.

Example Lab Exercise: Vulnerability Scanning with Nikto and Comparison of Tools in Kali Linux

Objective:

- Perform vulnerability scanning on a local or test web server using **Nikto**.
- Compare **Nikto**, **wpscan**, and **OpenVAS** in terms of functionality and use-case.

Part 1: Using Nikto for Vulnerability Scanning

Step 1: Start a Target Web Server (DVWA or Metasploitable)

sudo service apache2 start

Or use a vulnerable machine like **Metasploitable2**.

Step 2: Run Nikto Scan

nikto -h http://127.0.0.1

Optional: Save results to a file:

nikto -h http://127.0.0.1 -o scan_results.txt

Step 3: Analyze the Output

- Look for outdated software.
- Insecure headers.
- Common files (admin.php, test, etc.).

Part 2: Comparison of Vulnerability Scanning Tools

Tool	Focus Area	Target	Strengths	Common Use Case
Nikto	Web server vulnerabilities	Apache, Nginx	Fast, simple, scans for known misconfigurations	Scanning local or hosted web servers
wpscan	WordPress-specific	WordPress sites	Detects vulnerable plugins/themes, brute-force users	Securing WordPress blogs and CMS setups
OpenVAS	Full network vuln. scan	Any IP/host	Deep network scans, detailed reports, CVE coverage	Enterprise-level vulnerability auditing

In short **Conclusion:**

- **Nikto** is ideal for quick and lightweight web server scanning.
- **wpscan** is specialized for **WordPress**.

OpenVAS offers deep, network-wide analysis for professional environments.