Lab 1: Investigate Kali Linux

Objectives

In this lab, you will complete the following objectives:

- Familiarize yourself with the Kali Linux GUI.
- Familiarize yourself with the Kali Linux shell.
- Understand basic file and directory operations.
- Learn about file permissions and how to manipulate them.

Background / Scenario

Linux is an open-source operating system known for its speed, reliability, and efficiency. It can run on minimal hardware resources and is highly customizable. Unlike proprietary systems like Windows and Mac OS X, Linux is maintained by a community of developers, making it adaptable for various applications, from embedded devices to supercomputers.

Kali Linux is a specialized distribution designed for security auditing and penetration testing. It includes numerous tools for these tasks, but it is not intended for everyday use like gaming or general development. As a cybersecurity professional, it's crucial to be adept at navigating both the graphical user interface (GUI) and the command line in Kali Linux.

Required Resources

- Kali Linux virtual machine (VM) customized for Internship Training course.
- Internet access.

Instructions

Part 1: Familiarize Yourself with the Kali Linux GUI

Step 1: Start the VM and learn about the Kali GUI

1. **Log In**: Start your Kali VM and log in with the username `kali` and the password `kali`. You should see the Kali desktop.

2. **Explore the Desktop**:
    - The desktop contains icons like the trash, file explorer, and application links.
    - The top panel includes running application icons and allows you to switch between different desktops, each of which can have unique configurations.
3. **Customize the Panel**:
    - Right-click the panel, select `Panel`, then `+ Add New Items...` to explore options for adding frequently used items.
    - Access `Panel Preferences...` to adjust the appearance and functionality of the panel. Experiment with the settings and then close the windows.
4. **Access Settings**: The top-right corner displays settings and system information, including network status and power options.

Step 2: Navigate the Applications Menu

1. **Open the Applications Menu**: Click the first icon on the left side of the panel to access the Applications menu, similar to the Start menu in Windows.
2. **Explore Applications**: Browse through the categories, examining the various tools available in Kali Linux, particularly those related to security.
3. **Open a Terminal**: Close any application windows and click the square black-and-white icon in the panel to open a terminal for the next part of the lab.

Part 2: Familiarize Yourself with the Kali Linux Shell

The shell (or terminal) is a powerful interface for interacting with the Linux operating system.

Step 1: Command Documentation

1. **Learn About the Man Page**:
    - In the terminal, type:

      ```
      man man
      ```
    - This command displays documentation about the `man` command. Use `q` to exit the man page.
    - **Question**: Name a few sections included in a man page?
2. **Basic Commands**: The following table lists some basic Linux commands and their functions:

Command	Description
mv	Moves or renames files and directories.
chmod	Modifies file permissions.
chown	Changes the ownership of a file.
dd	Copies data from an input to an output.
pwd	Displays the name of the current directory.
ps	Lists the processes currently running in the system.
su	Simulates a login as another user or to become a superuser.
sudo	Runs a command as a superuser or another named user.
grep	Searches for specific strings of characters within a file.
ifconfig	Displays or configures network card information (deprecated; use `ip address`).
apt-get	Installs, configures, and removes packages on Debian-based systems.
iwconfig	Displays or configures wireless network card information.
shutdown	Shuts down the computer or performs related tasks.
passwd	Changes the password for the current user.
cat	Lists the contents of a file.

Step 2: Create and Change Directories

In this step, you will use the `cd`, `mkdir`, and `ls` commands.

1. **Print the Current Working Directory**:

   ```
   pwd
   ```

   Question: What is the current directory?

2. **Navigate to the `/home/kali` Directory**:

   ```
   cd /home/kali
   ```

3. **List Files in the Current Directory**:

   ```
   ls -l
   ```

4. **Create a New Directory**:

   ```
   mkdir Test
   ```

5. **Verify the Directory Creation**:

   ```
   ls
   ```

6. **Remove the Directory**:

```
rmdir Test
```

7. **Verify the Directory Removal**:

```
ls
```

Part 3: Copying and Moving Files

1. **Copy a File**: To copy a file, use the `cp` command. For example, to copy `gvm_admin_passwd.txt` to `backup_gvm_passwd.txt`:

```
cp gvm_admin_passwd.txt backup_gvm_passwd.txt
```

2. **Verify the Copy**:

```
ls
```

3. **Move a File**: To move `gvm_admin_passwd.txt` to the Documents directory:

```
mv gvm_admin_passwd.txt Documents/
```

4. **Verify the Move**:

```
ls Documents/
```

Part 4: Deleting Files

1. **Delete a File**: To delete `backup_gvm_passwd.txt`:

```
rm backup_gvm_passwd.txt
```

2. **Verify Deletion**:

```
ls
```

Part 5: Viewing File Content

1. **View File Contents**: To view the contents of a file:

```
cat gvm_admin_passwd.txt
```

2. **Paginated Viewing**: If the file is long, use `less` for paginated viewing:

```
less gvm_admin_passwd.txt
```

Conclusion

Navigating the Kali Linux file system is essential for effective system management. By mastering basic commands such as `cd`, `ls`, `mkdir`, `cp`, `mv`, `rm`, and `cat`, you can efficiently manage files and directories in your environment. Understanding the GUI and the shell will enhance your ability to perform tasks in Kali Linux.

Lab 2: Installing Packages and Applications

Objectives

In this lab, you will:

- Use the Advanced Package Tool (APT) to manage packages in Kali Linux.
- Install, upgrade, and remove applications using command-line tools.
- Search for packages and manage repositories.

Background / Scenario

Kali Linux, built on Debian, utilizes the APT package management system, which simplifies the process of installing, upgrading, and managing software packages. Understanding how to use APT is essential for maintaining a functional and secure environment, particularly in cybersecurity roles.

Required Resources

- Kali Linux virtual machine (VM).
- Internet access.

Instructions

Part 1: Updating Package Lists

1. **Open a Terminal**:
    - Log into your Kali Linux VM.
    - Open a terminal by clicking on the terminal icon in the taskbar.
2. **Update the Package List**:
    - Run the following command to update the list of available packages and their versions:

```
sudo apt update
```

    - **Explanation**:

        - The `sudo` command allows you to run programs with the security privileges of another user (typically the superuser).
        - `apt` is the command-line tool for managing packages.
        - `update` fetches the latest package information from the repositories configured on your system. This ensures you have the most current information about the software available for installation.
    - **Example Output**:
    - `Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]`
    - `...`
    - `Reading package lists... Done`

Part 2: Installing Packages

1. **Install `curl`**:
    - Use APT to install `curl`, a command-line tool for transferring data with URLs:

```
sudo apt install curl
```

    - **Explanation**:
        - `install` tells APT to fetch the specified package and any required dependencies from the repository and install them.
        - `curl` is a useful tool for testing endpoints and downloading files.
    - **Example Output**:
    - `The following NEW packages will be installed:`
    - `  curl`
    - `...`
    - `Do you want to continue? [Y/n] Y`
2. **Verify the Installation**:
    - Check the version of `curl` to confirm the installation was successful:

```
curl --version
```

    - **Explanation**: This command displays the installed version of `curl`. If installed correctly, it will show version information.
    - **Example Output**:
    - `curl 7.68.0 (x86_64-pc-linux-gnu) libcurl/7.68.0 OpenSSL/1.1.1d`

Part 3: Upgrading Packages

1. **Upgrade All Installed Packages**:
    - Run the following command to upgrade all currently installed packages to their latest versions:

```
sudo apt upgrade
```

   - **Explanation**: This command checks for updates to all installed packages and upgrades them to the latest versions available in the repository.
   - **Example Output**:
   - `The following packages will be upgraded:`
   - `  package1 package2 ...`
   - `...`
   - `Do you want to continue? [Y/n] Y`
2. **Review Upgrade Messages**:
   - Observe the output, which lists packages that were upgraded. It may prompt you to confirm the upgrades; simply press `Y` and then `Enter` to proceed.

Part 4: Removing Packages

1. **Remove `curl`**:
   - To uninstall `curl`, use the following command:

```
sudo apt remove curl
```

   - **Explanation**: The `remove` command removes the specified package from the system while leaving its configuration files intact. This is useful if you want to reinstall the package later without losing its settings.
   - **Example Output**:
   - `Removing curl (7.68.0-1) ...`
2. **Confirm Removal**:
   - Verify that `curl` is no longer installed by checking its version:

```
curl --version
```

   - **Explanation**: If `curl` was successfully removed, this command should return an error indicating that `curl` is not found.
   - **Example Output**:
   - `curl: command not found`

Part 5: Searching for Packages

1. **Search for Networking Packages**:
   - Use the APT search functionality to find packages related to networking:

```
apt search networking
```

- **Explanation**: This command searches the package database for any packages that have "networking" in their name or description, displaying a list of matching packages.
- **Example Output**:
- `Sorting... Done`
- `Full Text Search... Done`
- `networking-tools/focal 1.0 all`
- `  A collection of networking tools`
- `...`

2. **Review Results**:
   - Take note of some of the networking tools available for installation, such as `net-tools`, `nmap`, or `traceroute`.

Part 6: Managing Repositories

1. **Edit Repositories**:
   - Open the `sources.list` file to view and manage your APT repositories:

```
sudo nano /etc/apt/sources.list
```

   - **Explanation**: This file contains a list of repositories that APT uses to fetch packages. Using `nano` opens the file in a text editor.
2. **Modify Repository Entries**:
   - Check for any commented-out entries (lines starting with `#`). Uncomment (remove the `#`) any repositories you want to enable.
   - **Example**: Change `#deb http://kali.download/kali kali-rolling main non-free contrib` to `deb http://kali.download/kali kali-rolling main non-free contrib`.
   - **Explanation**: Enabling additional repositories allows you to access more packages that are not available in the default repositories.
3. **Save and Exit**:
   - After making your changes, press `Ctrl + O` to save and `Ctrl + X` to exit the editor.

Part 7: Final Review

1. **Update Package List Again**:
   - After modifying repositories, run:

```
sudo apt update
```

- **Explanation**: This command updates the package list again to include any new repositories you just enabled.

2. **Explore Installed Packages**:
   - Use the following command to list all installed packages:

```
dpkg --get-selections | grep -v deinstall
```

   - **Explanation**: This command lists all installed packages, filtering out any that have been marked for deinstallation.
   - **Example Output**:
   - `curl`
   - `vim`
   - `nmap`

Conclusion

In this lab, you have learned how to manage packages in Kali Linux using APT. You should now be comfortable installing, upgrading, and removing applications, as well as searching for and managing software repositories. Mastery of these skills is essential for effective system administration and cybersecurity tasks.

Lab 3: Networking Commands

Objectives

In this lab, you will:

- Learn how to use basic and advanced networking commands.
- Understand how to configure network interfaces and diagnose network issues.
- Use tools to monitor and analyze network traffic.

Background / Scenario

Networking is a fundamental aspect of cybersecurity and system administration. Familiarity with networking commands allows you to configure, manage, and troubleshoot network connections effectively. Kali Linux includes a range of powerful tools for networking, making it an essential skill for ethical hackers and security professionals.

Required Resources

- Kali Linux virtual machine (VM).
- Internet access.

Instructions

Part 1: Displaying Network Configuration

1. **Open a Terminal**:
    - Start your Kali Linux VM.
    - Open a terminal by clicking the terminal icon.
2. **Check Network Interfaces**:
    - Use the following command to display the current network interfaces and their configuration:

```
ip addr show
```

- **Explanation**: The `ip addr show` command provides detailed information about all network interfaces, including IP addresses, MAC addresses, and status.
- **Example Output**:
- `2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000`
- `    link/ether 08:00:27:12:34:56 brd ff:ff:ff:ff:ff:ff`
- `    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth0`
- `    valid_lft forever preferred_lft forever`

3. **List Routing Table**:
   - To view the routing table, run:

```
ip route show
```

   - **Explanation**: This command displays the routing table, which contains information on how packets are routed through the network.
   - **Example Output**:
   - `default via 192.168.1.1 dev eth0`
   - `192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.10`

Part 2: Testing Network Connectivity

1. **Ping a Host**:
   - Use the `ping` command to test connectivity to a remote host, such as Google:

```
ping -c 4 google.com
```

   - **Explanation**: The `-c 4` option sends 4 packets. The `ping` command checks if the host is reachable and measures the round-trip time for messages sent.
   - **Example Output**:
   - `PING google.com (172.217.5.110) 56(84) bytes of data.`
   - `64 bytes from lhr25s10-in-f14.1e100.net: icmp_seq=1 ttl=118 time=10.4 ms`
   - `...`
2. **Trace Route to a Host**:
   - Use the `traceroute` command to see the path packets take to a destination:

```
traceroute google.com
```

   - **Explanation**: `traceroute` shows the sequence of hops between your machine and the destination, helping diagnose where delays or failures occur.

- **Example Output**:
- `traceroute to google.com (172.217.5.110), 30 hops max, 60 byte packets`
- `1 router.local (192.168.1.1) 1.234 ms 1.012 ms 1.003 ms`
- `2 10.0.0.1 (10.0.0.1) 10.234 ms 10.012 ms 10.003 ms`
- `...`

Part 3: Configuring Network Interfaces

1. **View Current Interface Configuration**:
   - Use the following command to see the current settings for your network interfaces:

```
ifconfig
```

   - **Explanation**: The `ifconfig` command displays the configuration of all active network interfaces.
   - **Example Output**:
   - `eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500`
   - `inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255`
   - `...`
2. **Manually Configure an Interface**:
   - To assign a static IP address to an interface (for example, `eth0`), use:

```
sudo ip addr add 192.168.1.20/24 dev eth0
```

   - **Explanation**: This command assigns the IP address `192.168.1.20` with a subnet mask of `255.255.255.0` to the interface `eth0`.
3. **Bring the Interface Up**:
   - Activate the configured interface with:

```
sudo ip link set eth0 up
```

   - **Explanation**: This command enables the specified interface, making it active.

Part 4: Monitoring Network Traffic

1. **Install `tcpdump`**:
   - Use the following command to install `tcpdump`, a powerful packet analysis tool:

```
sudo apt install tcpdump
```

- **Explanation**: This command installs `tcpdump`, allowing you to capture and analyze network traffic.
- **Example Output**:
- `The following NEW packages will be installed:`
- `  tcpdump`
- `...`

2. **Capture Network Traffic**:
   - Use `tcpdump` to capture packets on `eth0`:

```
sudo tcpdump -i eth0 -c 10
```

   - **Explanation**: The `-i` option specifies the interface, and `-c 10` limits the capture to 10 packets.
   - **Example Output**:
   - `10:30:01.123456 IP 192.168.1.10 > 192.168.1.1: ICMP echo request, id 1234, seq 1, length 64`
   - `10:30:01.123457 IP 192.168.1.1 > 192.168.1.10: ICMP echo reply, id 1234, seq 1, length 64`
   - `...`
3. **Analyze Network Traffic**:
   - To see live traffic, run:

```
sudo tcpdump -i eth0
```

   - **Explanation**: This command captures and displays all traffic on `eth0` in real-time. Use `Ctrl + C` to stop the capture.

Part 5: Final Review

1. **Check Network Status**:
   - Use the following command to see the status of all interfaces:

```
nmcli device status
```

   - **Explanation**: This command provides a summary of all network interfaces, showing their connection status.
   - **Example Output**:
   - `DEVICE  TYPE      STATE        CONNECTION`
   - `eth0    ethernet  connected    Wired connection 1`
   - `wlan0   wifi      disconnected  --`
2. **Check Firewall Status**:
   - Check if the firewall is active and what rules are in place:

```
sudo ufw status verbose
```

- **Explanation**: This command shows the status of the Uncomplicated Firewall (UFW) and its rules.
- **Example Output**:
- `Status: active`
- `To                         Action      From`
- `--                         ------      ----`
- `22/tcp                     ALLOW       Anywhere`

Conclusion

In this lab, you have learned essential networking commands and tools available in Kali Linux. Mastery of these commands allows you to effectively manage and troubleshoot network connections, which is crucial in cybersecurity roles.