Introduction to Kali Linux

M.M. Tamim Sharif

DFIR Analyst, CTF Player, Vice President MIST Cyber Security Club

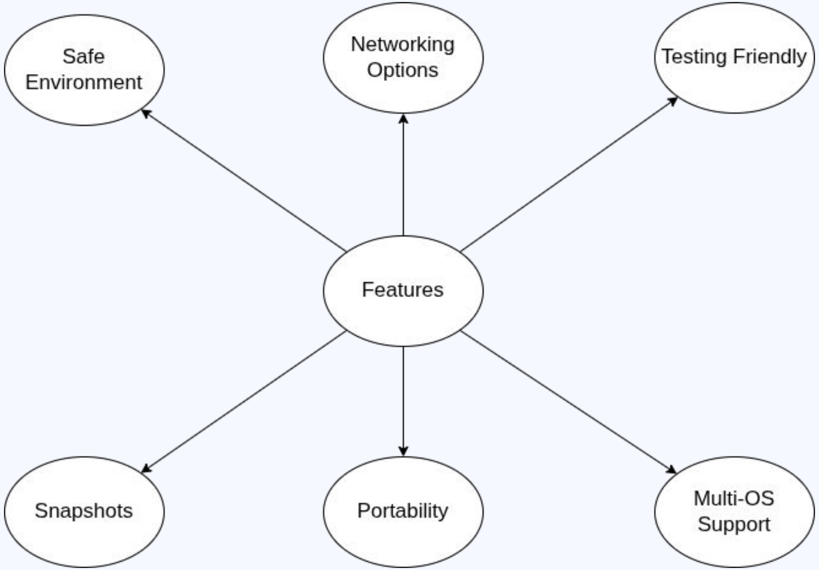
Achievement: 4th Runner-up, WTISD National Hackathon 2025
1st Runner-up , National MiniCTF (solo) 17th in HacktheBox Sharlocks (Globally)
Team Name: MIST_Shaheed_Yamin_Forever
Whatsapp: +8801788594010
Mail: tamimsharif2181@gmail.com

Table of contents

01

VirtualBox Setup for Kali Linux

Why Use VirtualBox for Kali Linux?



Scan Me

Kali Linux - A toolbox for Hacker

Why Kali??..

1.Penetration Testing OS

2.600+ Security Tools

3.Open Source

4.LUKS Encryption

5.Custom ISO

6.VirtualBox / VMware

7.ARM Devices

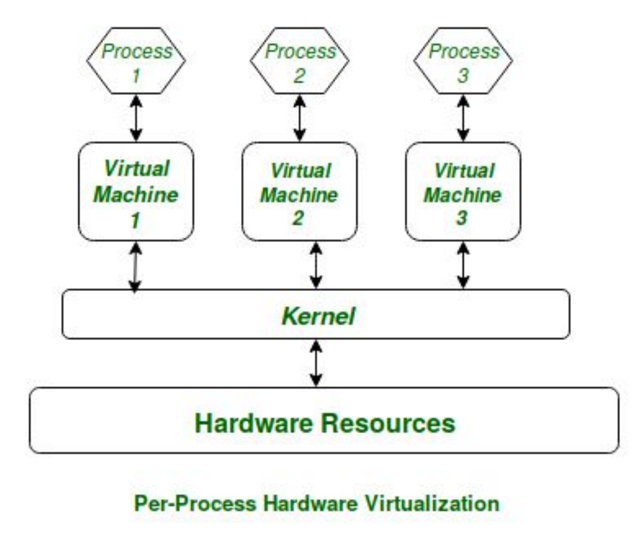
8.Kali Undercover Mode

9.Win-KeX (WSL)

10.Kali NetHunter

References: https://www.geeksforgeeks.org/linux-unix/features-of-kali-linux/

Linux Kernel



Per-Process Hardware Virtualization

Main Features:

1. Virtualization of resources
2. Middleman between H/D & S/W

Subsystem of Linux Kernel:

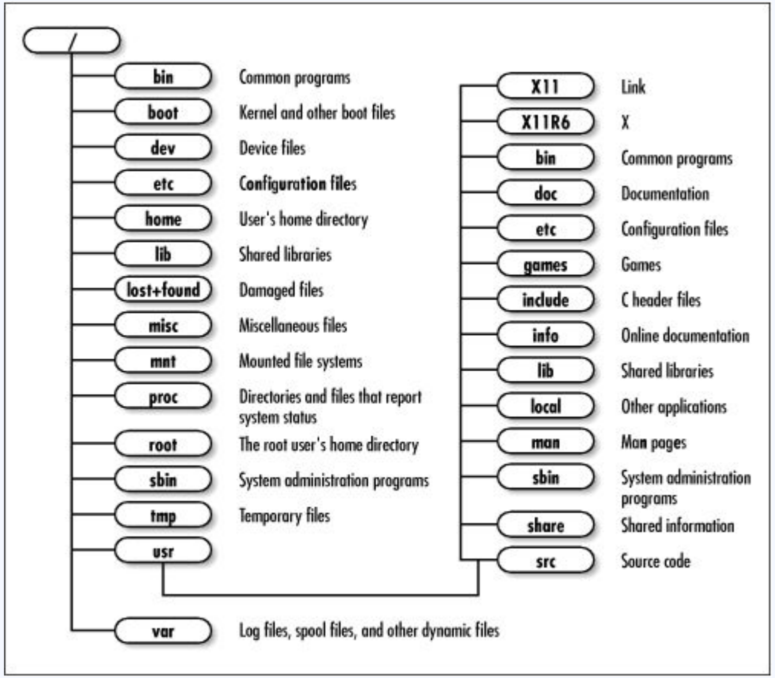
1. Process Scheduler
2. Memory Management Unit (MMU)
3. Virtual File System (VFS)
4. Networking Unit
5. Inter-Process Communication (IPC)

References: https://www.geeksforgeeks.org/linux-unix/the-linux-kernel/

The Linux Filesystem

Linux does not use Windows-style drive letters.Instead, all files, folders, and devices are children of the root directory, represented by the forward slash (/) character.The top-level directories are described as follows.

/bin/: basic programs
/etc/: configuration files
/home/: user's personal files
/lib/: basic libraries
/root/: administrator's (root's) personal files
/tmp/: temporary files (this directory is often emptied at boot)
/usr/: applications (this directory is further subdivided into bin, sbin, lib)
/var/: variable data handled by services. This includes log files, caches.
/proc/ and /sys/ are specific to the Linux kernel, They are used by the kernel for exporting data to user space



Command for Linux

pwd :: The current directory
cd :: Change directory
ls :: List directory
ls -la
cat, more, less, head, and tail :: used to print the content of a given file to the screen
echo :: print argument
man :: user manuals page
touch :: create an empty file
rm :: delete or remove the file
mkdir :: make directory
rm -rf [folder/file name] to delete
mv :: To move a file to a different directory
cp :: To copy a file or rename
which :: returns the full path to the file
locate :: to find the path
grep :: [ex ls -la /usr/bin | grep zip]
Piping Operator :: |
whoami

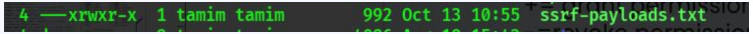
Important:

Information about **user accounts** are stored in the **/etc/passwd** file
the **fingerprints of the passwords** are stored in a different file, called **/etc/shadow**

tail -f /var/log/apache2/acceess.log is used to analysis updated log od apache web server

File Permission and Linux Application

r=read
w=write
x=executable
+= grant permission
-=revoke permission



```
4 ——xrwxr-x  1 tamim tamim        992 Oct 13 10:55  ssrf-payloads.txt
```

***sudo apt update :: ****To update the list of available packages in APT database*

***sudo apt upgrade :: ****upgrade the installed packages and core system to the latest versions*

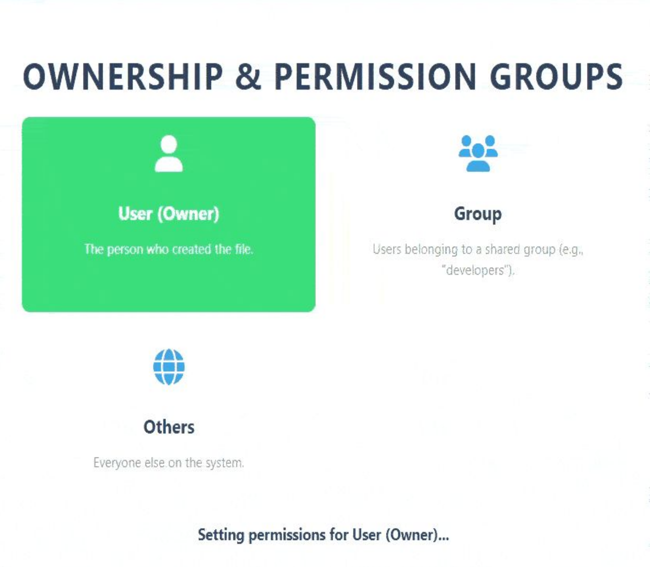
***apt-cache search [tools name] :: ****Displays much of the information stored in the internal cached package database*

***sudo apt show [tools name] :: ****to show description*

***sudo apt install [tools name] :: ****to install tools*

***sudo apt remove --purge [tools name] :: ****to remove tools*

sudo dpkg -i [filename.deb] ::



OWNERSHIP & PERMISSION GROUPS

User (Owner)
The person who created the file.

Group
Users belonging to a shared group (e.g., "developers").

Others
Everyone else on the system.

Setting permissions for User (Owner)...

References: https://www.geeksforgeeks.org/linux-unix/set-file-permissions-linux/

Linux Shell & Bash Scripting

# What a is Shell ?

A shell is a program that interprets user commands and passes them to the operating system kernel for execution

There are a few important shells on Linux:

sh: The Bourne SHell :: the foundation for almost all other shell environments
Bash: Also known as Bourne-Again SHell
ksh: Korn SHell :: ksh handles the loop syntax better than Bash
zsh: Z SHell ::

Shebang: #!/bin/bash **Output: ./out.sh**

Dollar Sign($): value of variables, parameters, or the output of command

.sh-> bash extension

References: https://www.w3schools.com/bash/bash_script.php

Codes: https://github.com/Tamimsharif83/NSU-Cybersec/blob/bash/bashScript/bash_script_snippets.md

Array & Loop

Basic for loop

```
for variable in list
do
  command
done
```

Range loop

```
for i in {1..5}
do
  echo "Run $i"
Done
```

Declare array

```
array=(item1 item2 item3)
```

Access array element

```
echo ${array[0]}
```

All elements

```
echo ${array[@]}
```

Array length

```
echo ${#array[@]}
```

Codes: https://github.com/Tamimsharif83/NSU-Cybersec/blob/bash/bashScript/bash_script_snippets.md

Practice Lab:

TryHackMe:

1. https://tryhackme.com/room/linuxfundamentalspart1
2. https://tryhackme.com/room/bashscripting

THANK YOU