Cyber security internship

Elevate Labs

Task 2: Operating System Security Fundamentals (Linux & Windows)

Environment Setup

To perform security tasks safely and practically, **Kali Linux was installed in a VirtualBox Virtual Machine**. Virtualization provides an isolated lab environment that allows testing system security settings and configurations without affecting the main operating system.

Along with Kali Linux, the built-in security features of Windows such as **Windows Defender and Windows Firewall** were also explored to understand system protection mechanisms in Windows OS.

User Accounts & Access Control

Operating systems support multiple users and control access through authentication and access control policies. During this task, user management was explored to understand how security is maintained in both Linux and Windows.

Key points studied:

User account creation and management

Role of authentication and secure passwords

Restricting unauthorized access using access control rules

Importance of separate user accounts for security

File Permissions and Ownership (Linux Security)

Linux provides strong protection through a permission-based file security model. In this task, file access control was studied in Kali Linux to understand how each file and directory is protected.

Permissions are generally controlled for:

Owner

Group

Others

Main learnings include:

Read, write, and execute permissions

Permission-based restriction to prevent unauthorized access

Ownership control for managing responsibility over files and folders

This ensures that sensitive data is accessed only by authorized users.

Administrator vs Standard User Privileges

Privilege management plays a major role in operating system security.

Linux (Kali Linux)

Normal users have limited access

Administrative tasks require special privileges

Windows

Administrator accounts have full control over the system

Standard user accounts have restricted access

This task helped in understanding the **Principle of Least Privilege**, which reduces risk by limiting access rights to only what is required.

. Firewall Configuration

A firewall is a critical security control that filters network traffic based on defined rules. In this task, firewall security features were explored in both Linux and Windows.

Key understanding:

Firewall blocks unauthorized inbound and outbound connections

Helps protect against external attacks and scanning

Only necessary network access should be allowed

Firewall configuration is an essential step in OS hardening.

. Process and Service Monitoring

Every operating system runs many processes and services in the background. Some are essential, while others may be optional or vulnerable.

In this task, the following were studied:

Monitoring active processes

Identifying system services running in background

Understanding how suspicious processes can indicate malware or attacks

Regular process monitoring helps in identifying abnormal system activities early.

Disabling Unnecessary Services (Reducing Attack Surface)

Running unnecessary services increases the chances of exploitation. In this task, unnecessary or unused services were identified and disabled.

Benefits:

Reduces open entry points for attackers

Minimizes vulnerabilities

Improves system security and performance

Attack surface reduction is an important part of operating system security.

. OS Hardening Best Practices

Operating System Hardening means making the system stronger by applying security settings and best practices to prevent attacks.

Linux (Kali Linux) Hardening Practices

Keeping system updated and patched

Secure user access control

Applying strong permissions and access restrictions

Firewall protection

Disabling unused services and tools

Monitoring logs and system activity

Windows Hardening Practices

Enabling Windows Defender real-time protection

Enabling Windows Firewall

Applying system updates

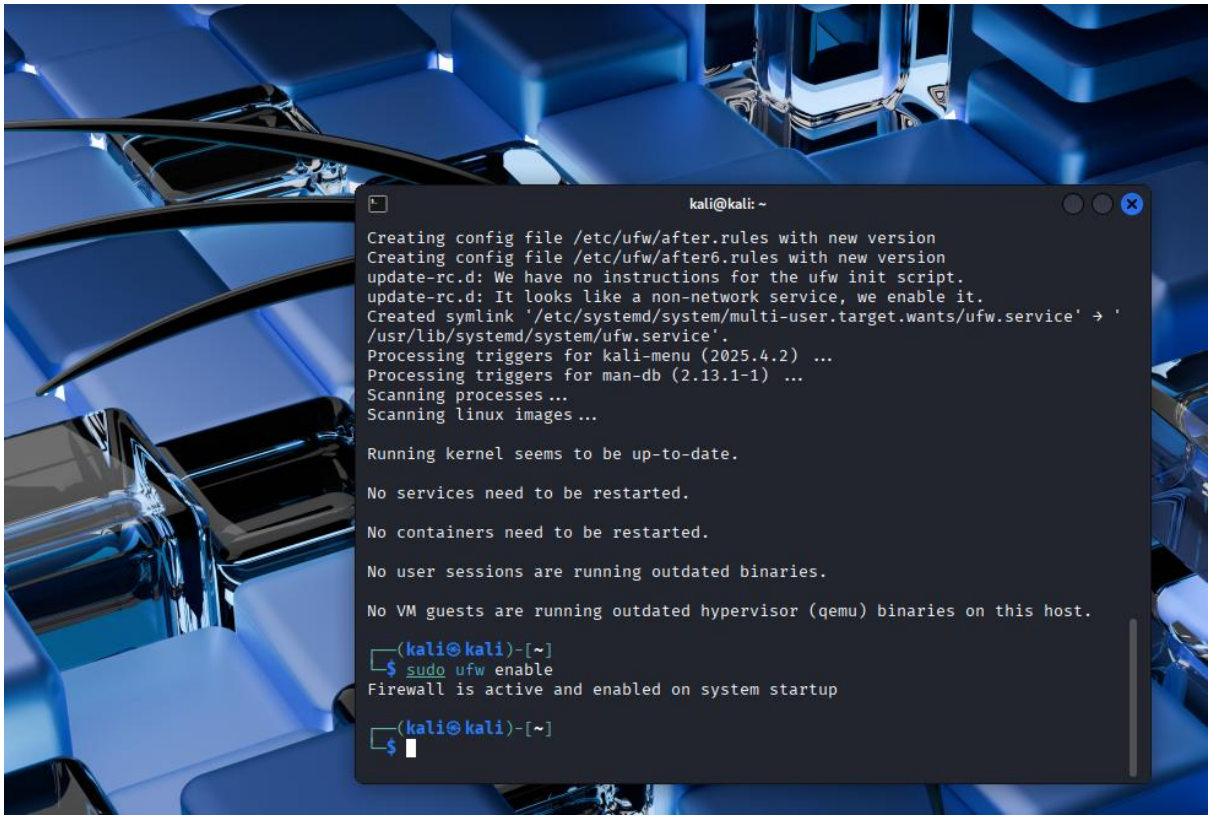
Restricting admin privileges and using standard accounts

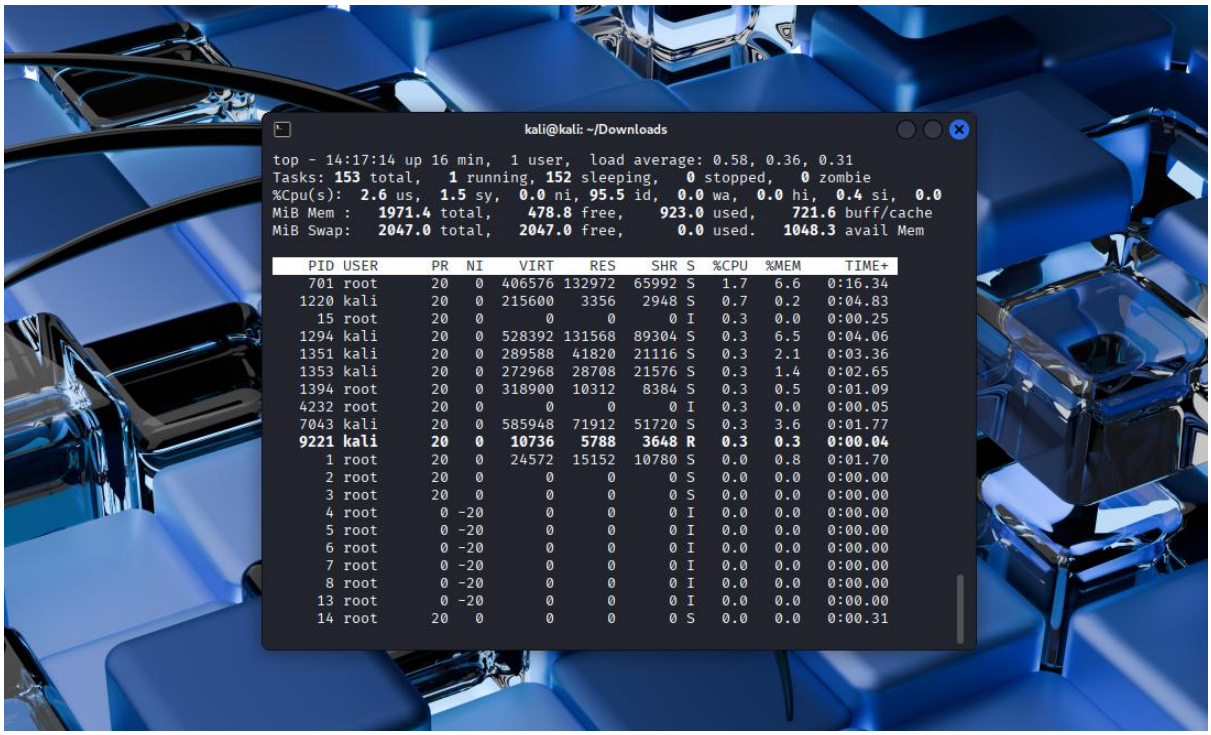
Disabling unnecessary startup programs

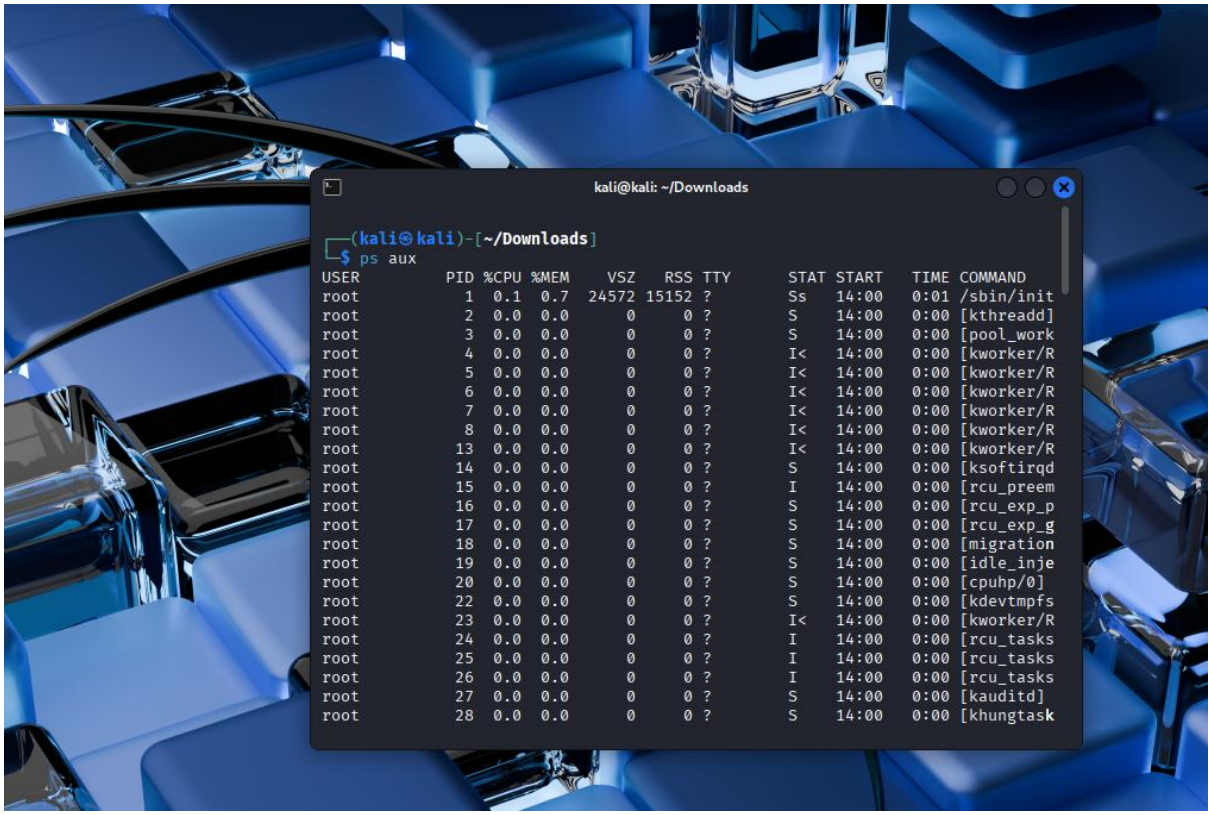
Enabling additional security protections

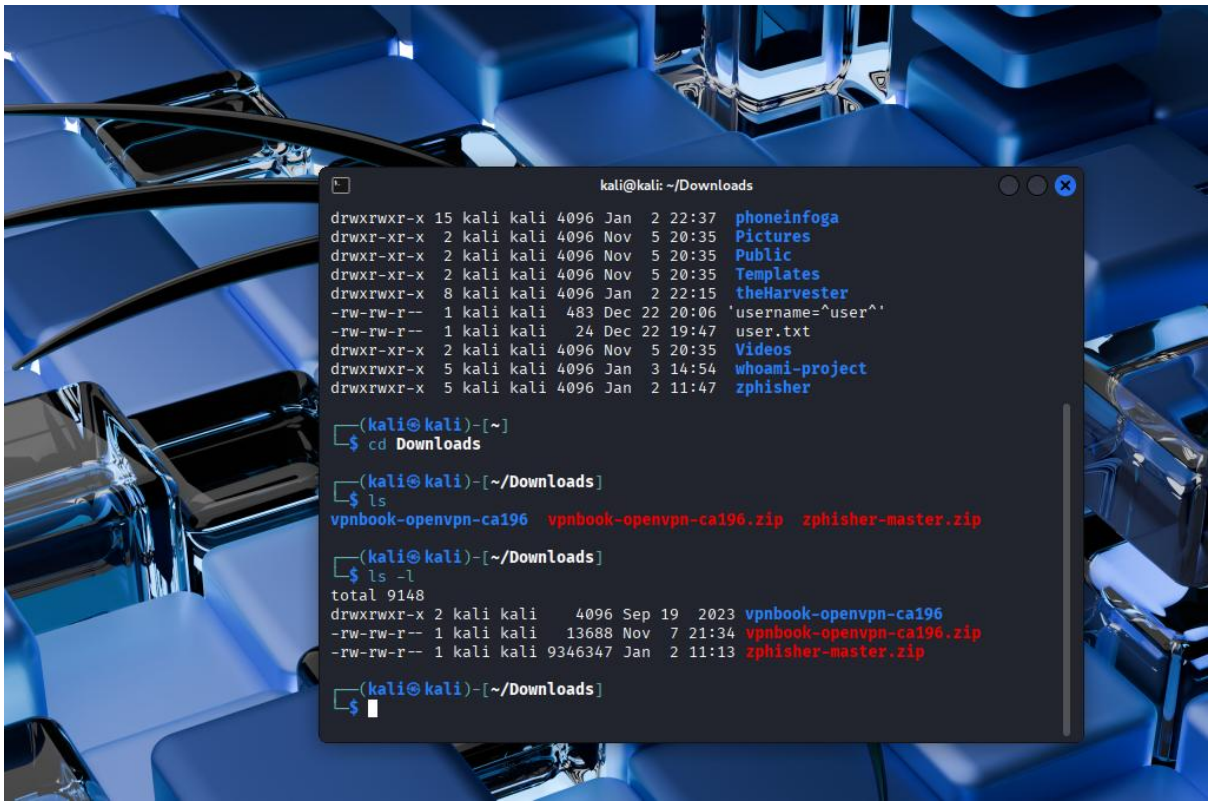
Conclusion

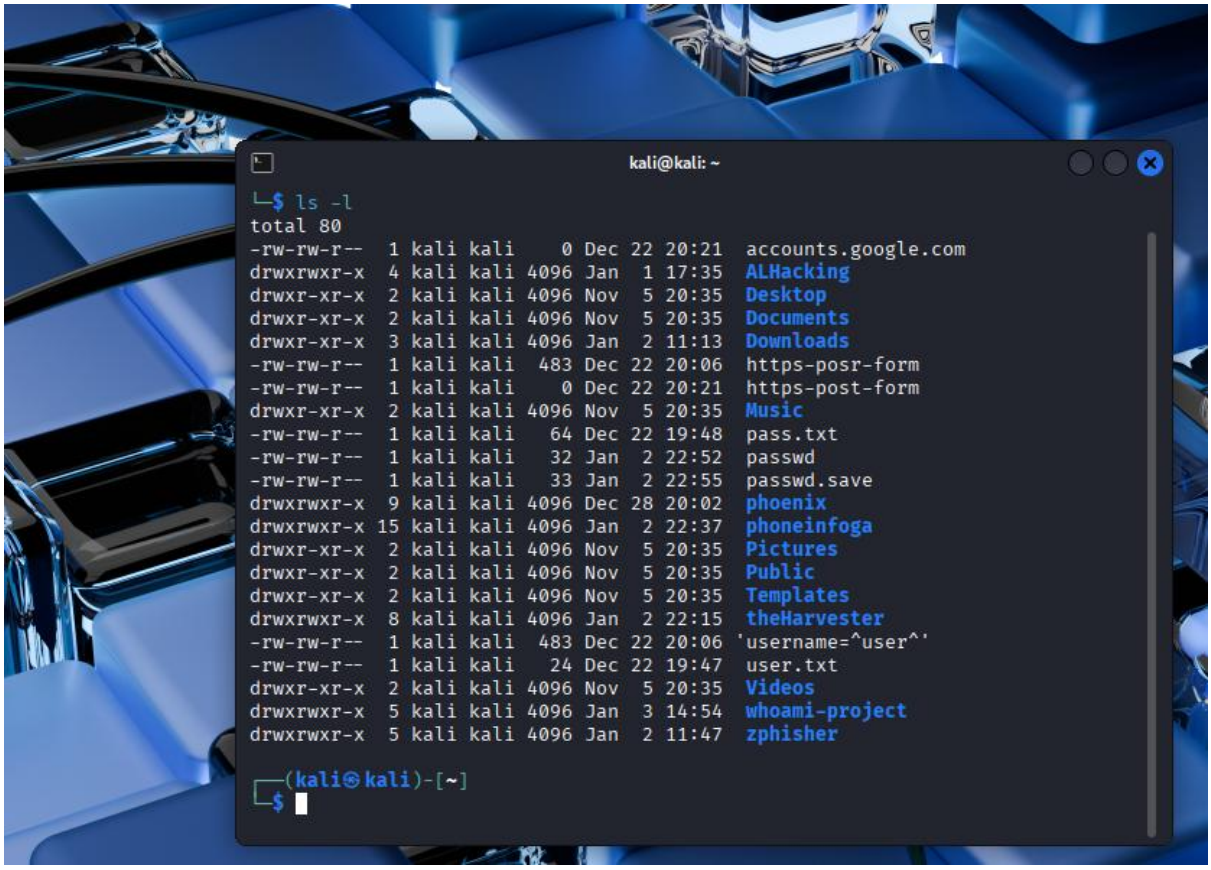
In this task, I learned the basics of operating system security by working practically with **Kali Linux in VirtualBox** and Windows security features like **Windows Defender** and **Firewall**. Through this activity, I gained a clear understanding of how operating systems control user access, manage file permissions, and handle administrator privileges. I also explored how firewall settings, process monitoring, and service management help in securing a system. Overall, this task helped me understand important OS hardening practices that reduce security risks, block unauthorized access, and protect systems from malware and cyberattacks.

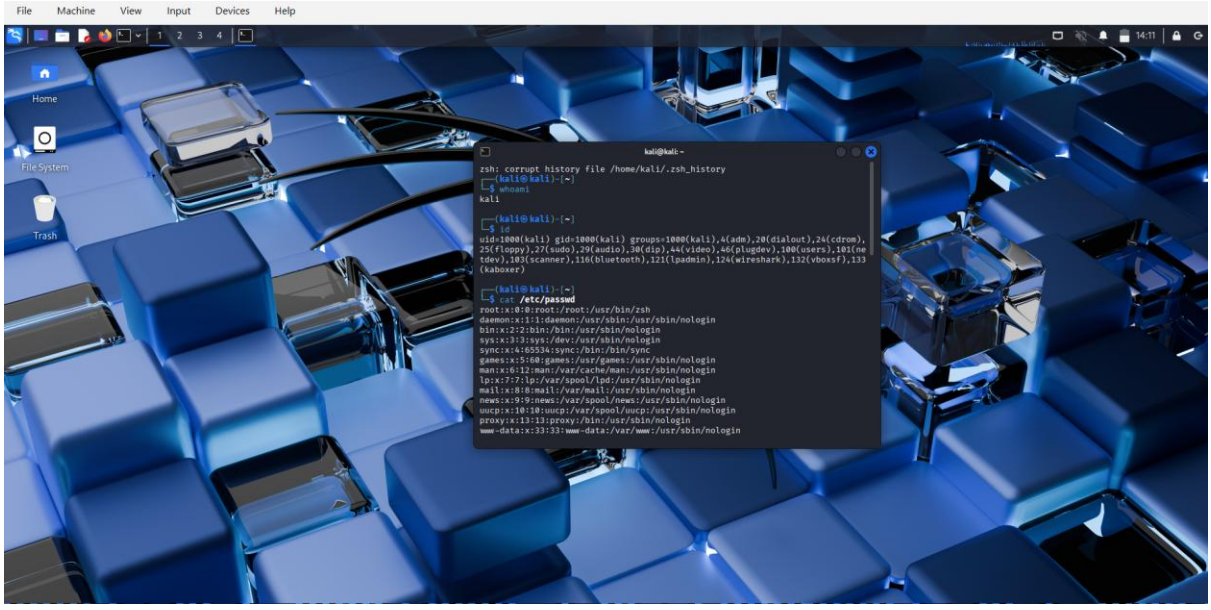

kali@kali: ~
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.4.2) ...
Processing triggers for man-db (2.13.1-1) ...
Scanning processes ...
Scanning linux images ...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(kali㉿kali)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup
(kali㉿kali)-[~]
$

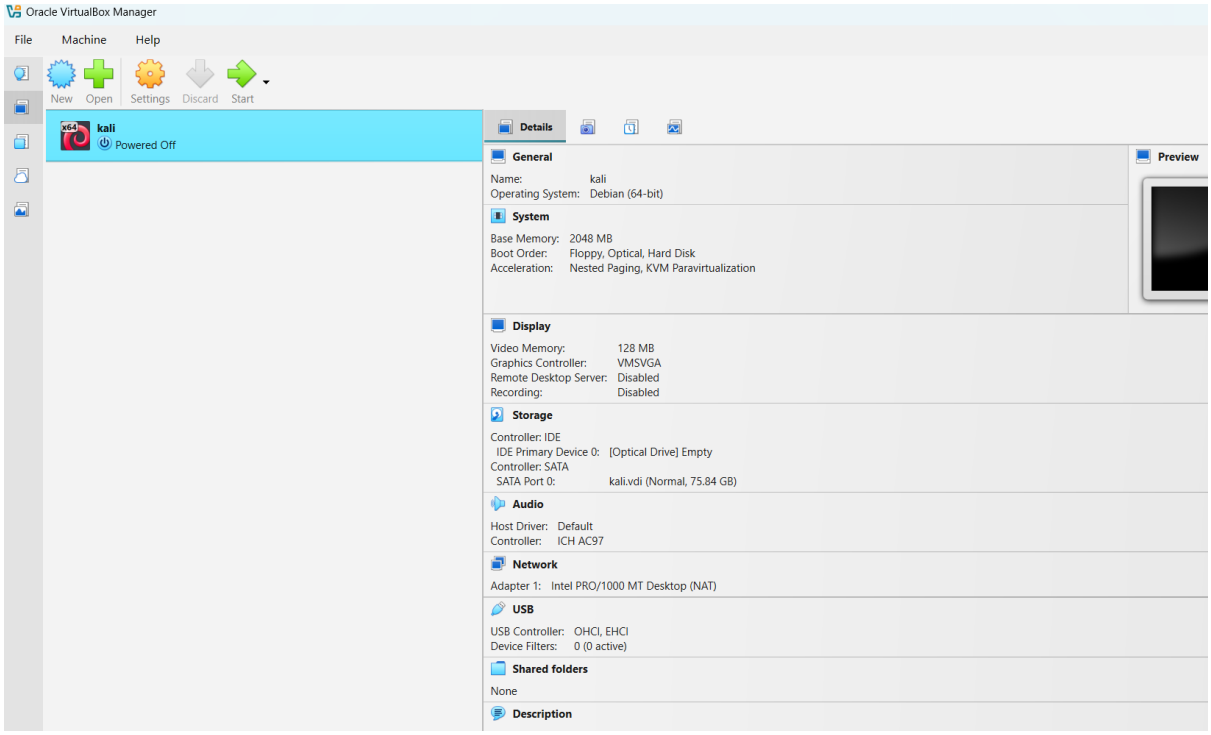

kali@kali: ~/Downloads
top - 14:17:14 up 16 min, 1 user, load average: 0.58, 0.36, 0.31
Tasks: 153 total, 1 running, 152 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2.6 us, 1.5 sy, 0.0 ni, 95.5 id, 0.0 wa, 0.0 hi, 0.4 si, 0.0
MiB Mem : 1971.4 total, 478.8 free, 923.0 used, 721.6 buff/cache
MiB Swap: 2047.0 total, 2047.0 free, 0.0 used. 1048.3 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+
701 root 20 0 406576 132972 65992 S 1.7 6.6 0:16.34
1220 kali 20 0 215600 3356 2948 S 0.7 0.2 0:04.83
15 root 20 0 0 0 0 I 0.3 0.0 0:00.25
1294 kali 20 0 528392 131568 89304 S 0.3 6.5 0:04.06
1351 kali 20 0 289588 41820 21116 S 0.3 2.1 0:03.36
1353 kali 20 0 272968 28708 21576 S 0.3 1.4 0:02.65
1394 root 20 0 318900 10312 8384 S 0.3 0.5 0:01.09
4232 root 20 0 0 0 0 I 0.3 0.0 0:00.05
7043 kali 20 0 585948 71912 51720 S 0.3 3.6 0:01.77
9221 kali 20 0 10736 5788 3648 R 0.3 0.3 0:00.04
1 root 20 0 24572 15152 10780 S 0.0 0.8 0:01.70
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00
3 root 20 0 0 0 0 S 0.0 0.0 0:00.00
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
7 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
13 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
14 root 20 0 0 0 0 S 0.0 0.0 0:00.31


kali@kali: ~/Downloads
┌──(kali㉿kali)-[~/Downloads]
└─$ ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.1 0.7 24572 15152 ? Ss 14:00 0:01 /sbin/init
root 2 0.0 0.0 0 0 ? S 14:00 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 14:00 0:00 [pool_work
root 4 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 5 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 6 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 7 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 8 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 13 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 14 0.0 0.0 0 0 ? S 14:00 0:00 [ksoftirqd
root 15 0.0 0.0 0 0 ? I 14:00 0:00 [rcu_preem
root 16 0.0 0.0 0 0 ? S 14:00 0:00 [rcu_exp_p
root 17 0.0 0.0 0 0 ? S 14:00 0:00 [rcu_exp_g
root 18 0.0 0.0 0 0 ? S 14:00 0:00 [migration
root 19 0.0 0.0 0 0 ? S 14:00 0:00 [idle_inje
root 20 0.0 0.0 0 0 ? S 14:00 0:00 [cpuhp/0]
root 22 0.0 0.0 0 0 ? S 14:00 0:00 [kdevtmpfs
root 23 0.0 0.0 0 0 ? I< 14:00 0:00 [kworker/R
root 24 0.0 0.0 0 0 ? I 14:00 0:00 [rcu_tasks
root 25 0.0 0.0 0 0 ? I 14:00 0:00 [rcu_tasks
root 26 0.0 0.0 0 0 ? I 14:00 0:00 [rcu_tasks
root 27 0.0 0.0 0 0 ? S 14:00 0:00 [kauditd]
root 28 0.0 0.0 0 0 ? S 14:00 0:00 [khungtask


kali@kali: ~/Downloads
drwxrwxr-x 15 kali kali 4096 Jan 2 22:37 phoneinfoga
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Pictures
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Public
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Templates
drwxrwxr-x 8 kali kali 4096 Jan 2 22:15 theHarvester
-rw-rw-r-- 1 kali kali 483 Dec 22 20:06 'username=^user^'
-rw-rw-r-- 1 kali kali 24 Dec 22 19:47 user.txt
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Videos
drwxrwxr-x 5 kali kali 4096 Jan 3 14:54 whoami-project
drwxrwxr-x 5 kali kali 4096 Jan 2 11:47 zphisher
┌──(kali㉿kali)-[~]
└─$ cd Downloads
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
vpnbook-openvpn-ca196 vpnbook-openvpn-ca196.zip zphisher-master.zip
┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 9148
drwxrwxr-x 2 kali kali 4096 Sep 19 2023 vpnbook-openvpn-ca196
-rw-rw-r-- 1 kali kali 13688 Nov 7 21:34 vpnbook-openvpn-ca196.zip
-rw-rw-r-- 1 kali kali 9346347 Jan 2 11:13 zphisher-master.zip
┌──(kali㉿kali)-[~/Downloads]
└─$


kali@kali: ~
└─$ ls -l
total 80
-rw-rw-r-- 1 kali kali   0 Dec 22 20:21 accounts.google.com
drwxrwxr-x 4 kali kali 4096 Jan 1 17:35 ALHacking
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Desktop
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Documents
drwxr-xr-x 3 kali kali 4096 Jan 2 11:13 Downloads
-rw-rw-r-- 1 kali kali 483 Dec 22 20:06 https-posr-form
-rw-rw-r-- 1 kali kali   0 Dec 22 20:21 https-post-form
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Music
-rw-rw-r-- 1 kali kali   64 Dec 22 19:48 pass.txt
-rw-rw-r-- 1 kali kali   32 Jan 2 22:52 passwd
-rw-rw-r-- 1 kali kali   33 Jan 2 22:55 passwd.save
drwxrwxr-x 9 kali kali 4096 Dec 28 20:02 phoenix
drwxrwxr-x 15 kali kali 4096 Jan 2 22:37 phoneinfoga
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Pictures
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Public
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Templates
drwxrwxr-x 8 kali kali 4096 Jan 2 22:15 theHarvester
-rw-rw-r-- 1 kali kali 483 Dec 22 20:06 'username=^user^'
-rw-rw-r-- 1 kali kali   24 Dec 22 19:47 user.txt
drwxr-xr-x 2 kali kali 4096 Nov 5 20:35 Videos
drwxrwxr-x 5 kali kali 4096 Jan 3 14:54 whoami-project
drwxrwxr-x 5 kali kali 4096 Jan 2 11:47 zphisher
┌──(kali㉿kali)-[~]
└─$


File
Machine
View
Input
Devices
Help
Home
File System
Trash
kali@kali: ~
zsh: corrupt history file /home/kali/.zsh_history
└─$ whoami
kali
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),103(scanner),116(bluetooth),121(lpadmin),124(wireshark),132(vboxsf),133(kaboxer)
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin


Oracle VirtualBox Manager
File
Machine
Help
New
Open
Settings
Discard
Start
kali
Powered Off
Details
Preview
General
Name: kali
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali.vdi (Normal, 75.84 GB)
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description