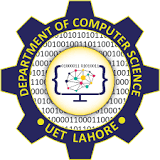
**LAB REPORTS**



**Session 2023-2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Dr. Faiza

**Course:**

Information Security

**Department of Computer Science**

**University of Engineering and Technology,**

**Lahore Pakistan**

Contents

[**TASK 1 ASSET CLASSIFICATION** 3](#_Toc188784360)

[**1.** **ASSET CLASSIFICATION:** 3](#_Toc188784361)

[ **Critical Assets:** 3](#_Toc188784362)

[ **Non-Critical Assets:** 3](#_Toc188784363)

[**2.** **SYSTEM SCAN:** 3](#_Toc188784364)

[ **File System Scan using ls-l command:** 3](#_Toc188784365)

[ **Disk usage Analysis using df –h command:** 4](#_Toc188784366)

[ **Network scan report using netstan command:** 5](#_Toc188784367)

[**3.** **CONCLUSION:** 6](#_Toc188784368)

# **TASK 1 ASSET CLASSIFICATION**

## **ASSET CLASSIFICATION:**

The assets obtained from the system scans can be categorized into following categories:

### **Critical Assets:**

These assets are essential for the functioning, security, and integrity of the system. Any failure or compromise of these assets could lead to significant operational or security risks.

Example: Operating system files, network interfaces and configurations, system libraries, user and permission settings, security and firewall rules etc.

### **Non-Critical Assets:**

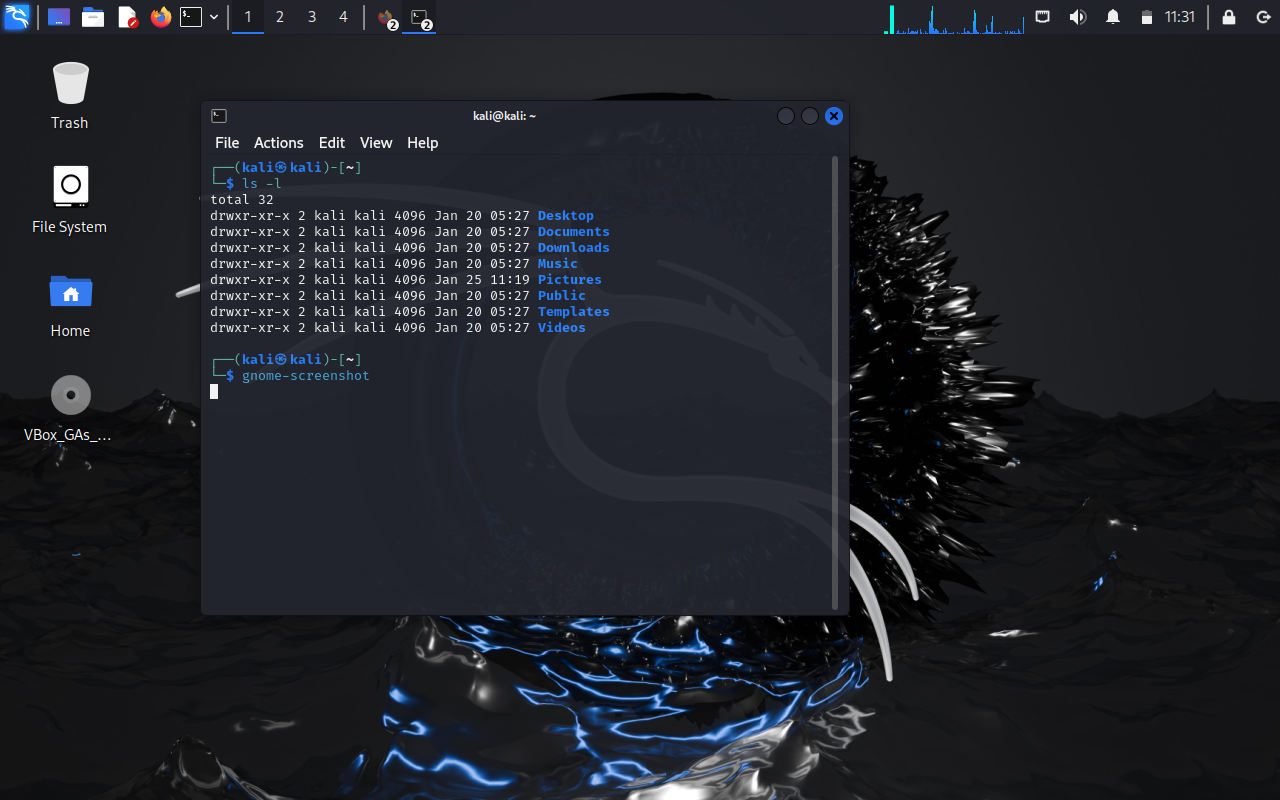
These assets contribute to operational efficiency but didn’t pose an immediate risk if modified or compromised.

Example: Temporary files & logs, user installed applications, background process, unused network interfaces, archived & backup files.

## **SYSTEM SCAN:**

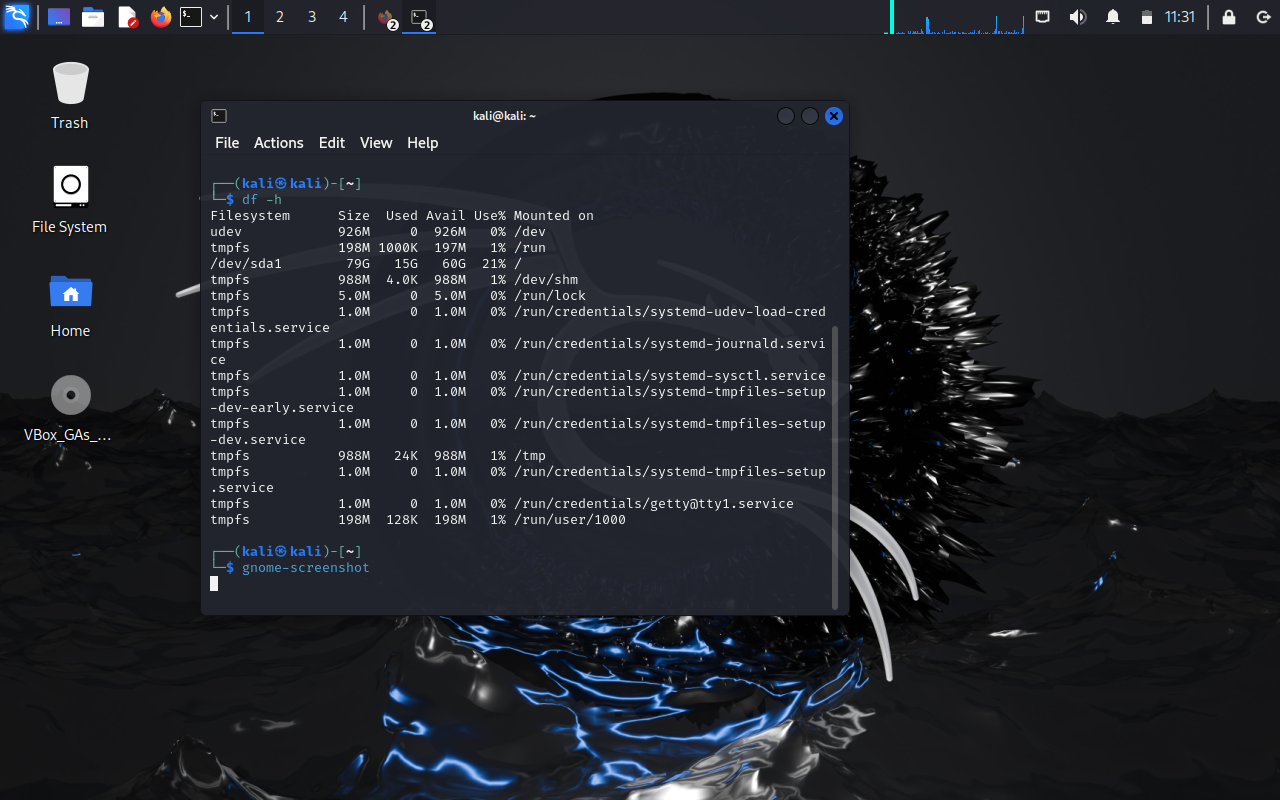
### **File System Scan using ls-l command:**

Identified some system directories and files, some critical operating system files and some non-essential user generated files.



### **Disk usage Analysis using df –h command:**

Identified some critical storage partitions and its utilization, highlighted some disk space related threats and also identifies some non-critical log files consuming space.



### **Network scan report using netstan command:**

It listed active network connections and listening ports. It also identified open ports crucial for services and detected some non-critical inactive interfaces.



# **CONCLUSION:**

This analysis provides an overview of the software assets and their classification based on system scans. By following the outlined recommendations, system stability, security, and efficiency can be improved significantly. Continuous monitoring and periodic audits are recommended to ensure ongoing system integrity.