

**UJAR TECH SOLUTION**

Name: Rithik varma

Intern ID: UTS1103

TASK 1

Exploring the CIA Triad in Real-World Scenarios:

*Understand and practically identify the Confidentiality, Integrity, and Availability (CIA Triad) in real-world systems using examples, documentation, and system configurations.*

Practical Description

**Problem: -** Explore a Linux machine and describe how file permissions support CIA using 3 real-world systems (Gmail, Banking App, Hospital Record System).

Key Concepts of CIA Triad:

the term CIA refers to The cyber security fundamental which include the core concepts of securing Sensitive Data from Unauthorized or thread ACCESS.

The term CIA stands for Confidentiality Integrity AVAILABILITY.

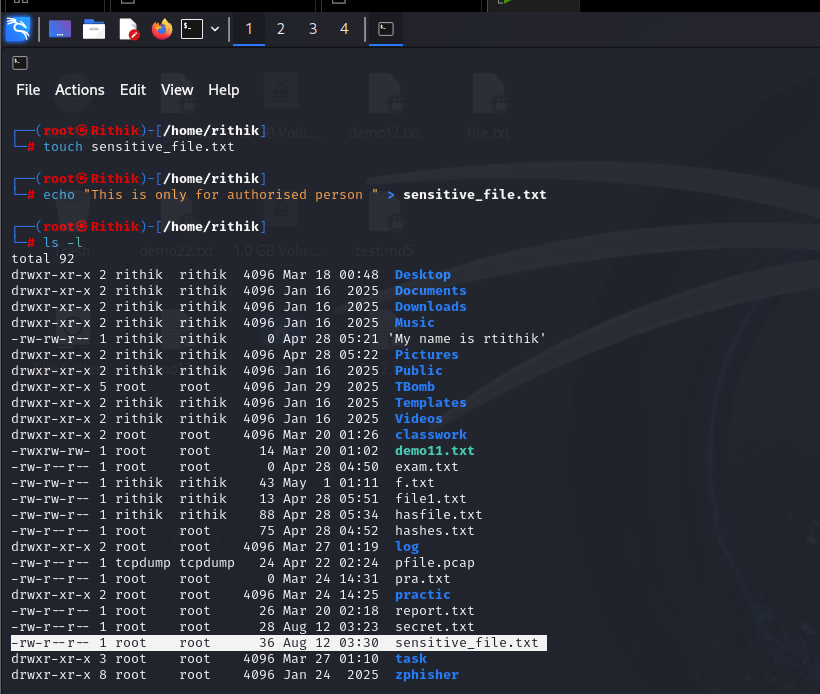
Definitions :

* Confidentiality : - It Ensure that the information is only accessible to the Authorized person and not exposed to Unauthorized/Attackers. This is achieved by enforcing strong passwords like adding (Biometrics, Two Factor authentication) , Restricting access control etc.
* INTEGRITY: - This make sure that the Data cannot be changed by the Attacker and the information is accurate and unaltered. it can be achieved by using hashing, digital signatures, backups, etc.
* AVAILABILITY: - It is responsible for Keeping Data and important documents ready when you need them. This can Achieved through redundancy, backups of data and important documents.

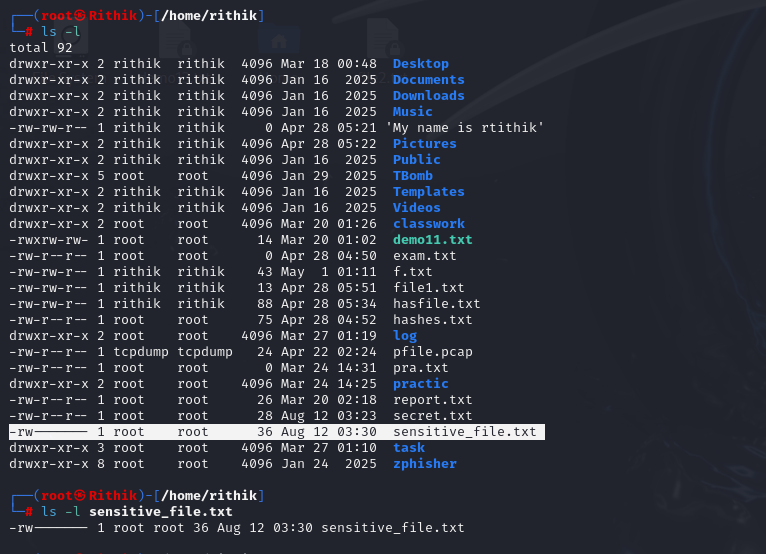
*The CIA triad provides a framework for organizations to assess their security posture, identify potential vulnerabilities, and implement appropriate controls to mitigate risks. While it's a widely accepted model, some argue that it may not fully encompass all aspects of modern security, especially with the rise of new technologies and evolving threats*.

Real-World Examples in Plain Language

| **Example** | **Confidentiality (Keep Secrets)** | **Integrity (Keep It Correct)** | **Availability (Keep It Ready)** |
| --- | --- | --- | --- |
| **Gmail** | Uses encryption so nobody can read your emails except you. | Google checks that your emails are not changed while stored. | Gmail runs on many servers, so it’s almost always online. |
| **Banking App** | Uses OTPs, biometrics, and encryption to keep your account safe. | Makes sure your transaction history isn’t changed without permission. | Has backup servers so you can use it even if one server fails. |
| **Hospital Records** | Only doctors or nurses with permission can see patient data. | Keeps a log of changes so no one can secretly change medical records. | Uses cloud storage and backups so records are available even during emergencies. |

Practical of CIA Using Kali Linux:******

Confidentiality practical:

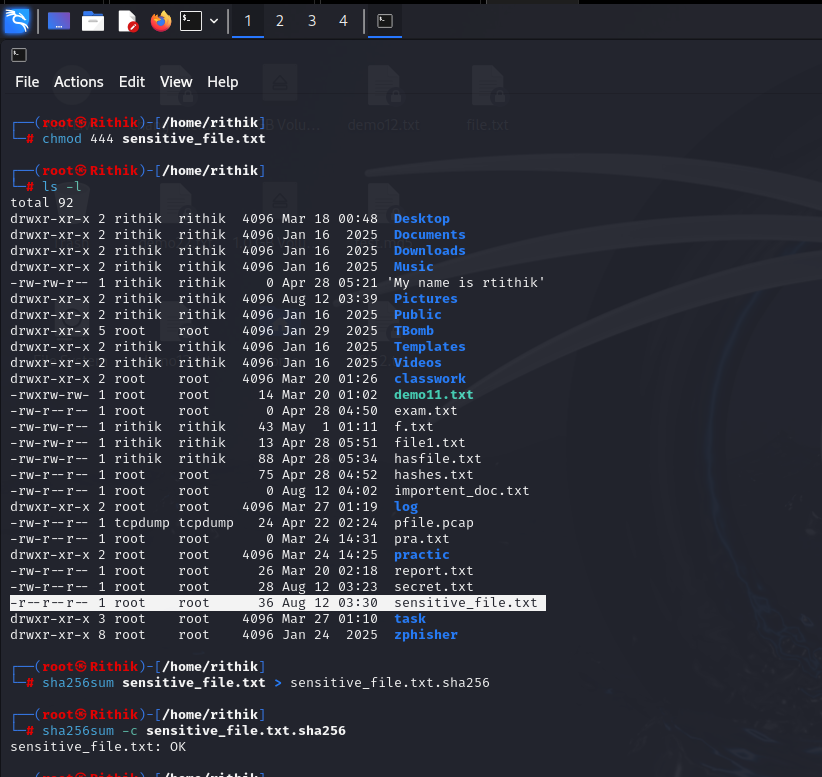
******

Here as you can see the permission is only given to owner (-rw-r--r-- to -rw-------) that means ***that only the owner can read and write to the file, thus protecting its confidentiality.***

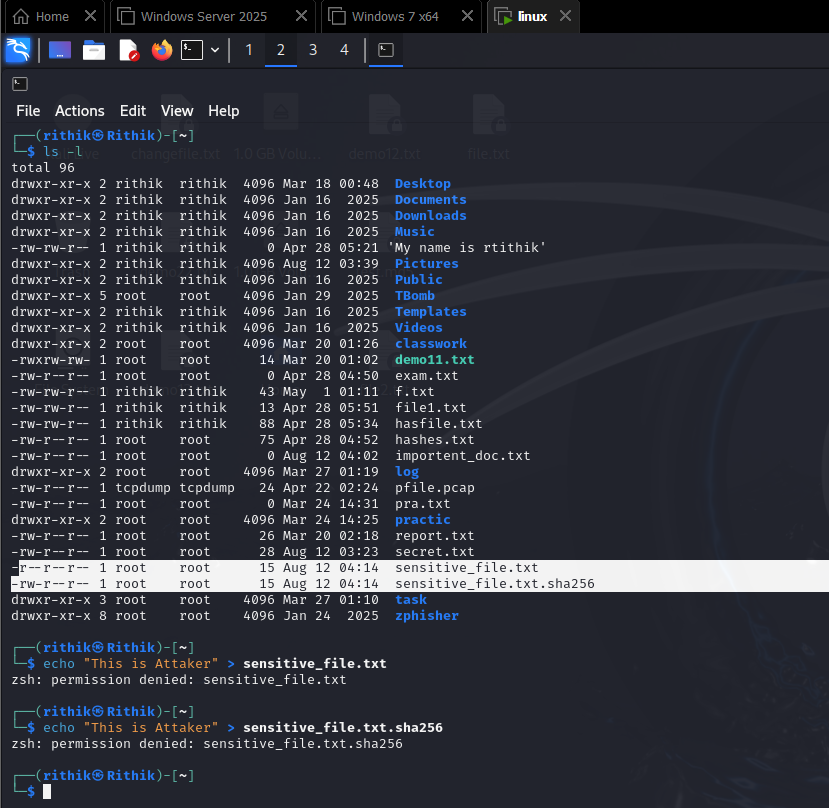
Integrity practical:

In Below image there is only read permission is given to all the authorized person (-r--r--r--).

***Hash is created using (sha256sum tool), so that no one can modify the data and it stay integrated.***

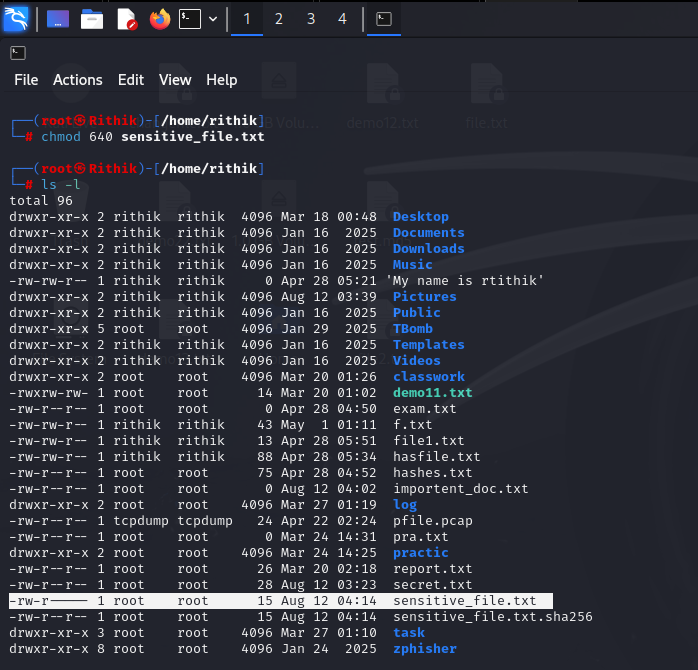
******

In Below image you can see the data is not getting manipulated by any un authorized person.

******

Availability practical:

The fallowing image contains (-rw-r------) this means that owner can read and writ both but the group can only read when it is needed.

******