1. **Scenario: Imagine your web application is hosted in an on- premises server room. To protect it effectively, outline the different types of security controls you would implement under the following categories:**

1. Managerial Controls (Administrative)

These focus on the strategic planning and high-level management of risk within the organization. They are often defined by policies and legal requirements.

- **Security Policy and Training:** Establishing an official "Acceptable Use Policy" and conducting mandatory security awareness training for all staff.
- **Risk Assessment:** Regularly performing formal assessments to identify vulnerabilities in the server room infrastructure and web application.
- **Example:** A **Background Check** policy for all IT staff who have physical access to the server room.
- Managerial control is preventive

2. Operational Controls

These are the day-to-day procedures and "human-executed" security measures designed to ensure that policies are being followed correctly.

- **Change Management:** A formal process to review and approve any changes to the server or application code to prevent accidental security gaps.
- **Log Review:** An administrator manually reviews system access logs daily to look for unusual patterns or unauthorized access attempts.
- **Example: Incident Response Planning**, which is a **Corrective** control that outlines exactly what to do once a breach has been detected.
- Operational control is Detective

3. Technical Controls

These are security measures implemented through hardware or software to protect the digital assets of the web application.

- **Firewalls and WAFs:** A Web Application Firewall (WAF) filters incoming HTTP traffic to block SQL injection or Cross-Site Scripting (XSS) attacks.
- **Intrusion Detection Systems:** An IDS that monitors network traffic and alerts administrators when it recognizes signatures of a known cyberattack.
- **Example: Data Encryption** (at rest and in transit), which is a **Preventive** control that ensures data is unreadable if intercepted.
- Technical controls are preventive

4. Physical Controls

These protect the actual hardware and the server room environment from physical unauthorized access or environmental hazards.

- **Locked Server Racks:** Keeping the physical servers inside locked cages or racks within the room to prevent tampering.
- **CCTV Surveillance:** Video cameras positioned at the entrance and inside the server room to record who enters and what they do.
- **Example:** A **Fire Suppression System**, which is a **Corrective** control that activates to minimize damage if a physical fire starts in the server room.
- Physical control is Detective

2. **SECURITY PRINCIPLES-CIA TRIAD AND AAA**

The CIA Triad:

The CIA Triad represents the three essential pillars of any information security strategy.

- **Confidentiality:** Ensures that sensitive data is accessible only to authorized users.
    - Application: You would use **encryption** (like TLS for data in transit) to prevent unauthorized eyes from reading patient or financial records.
- **Integrity:** Guards against the **unauthorized modification** or destruction of data to ensure it remains accurate and trustworthy.
    - Example: You would implement **digital signatures** or **hashing** to verify that a medical prescription or bank transaction hasn't been altered after being sent.
- **Availability:** Guarantees that systems and data are **accessible to authorized users** whenever they are needed.
    - Example: You would use **redundant servers**, backup power, and **load balancers** to ensure the web application stays online during a hardware failure or a DDoS attack.

• The AAA Framework: Access Control Mechanism

While the CIA defines your goals, the AAA framework provides the technical "how-to" for managing user access to that system.

- **Authentication:** The process of **verifying who a user is**.
    - Example: This is usually achieved through "something you know" (password), "something you have" (security token), or "something you are" (fingerprint).
- **Authorization:** Occurs after authentication and determines **what a user is allowed to do**.
    - Example: A "Guest" may only be authorized to view the homepage, while an "Admin" is authorized to delete database records.
- **Accounting:** The process of **tracking and recording** what a user did while they were logged in.
    - Example: This creates an **audit trail** that logs the time, date, and specific commands issued by a user, which is vital for troubleshooting and security forensics.

3. **what is the difference between symmetric and asymmetric encryption?**

Symmetric vs. Asymmetric Encryption

Encryption is a fundamental approach to ensuring data confidentiality . The primary difference lies in the number of keys used and how they are managed.

1. Key Management

- **Symmetric Encryption:** Uses a **single, shared secret key** for both encryption and decryption. Both the sender and the receiver must possess the exact same key.
- **Asymmetric Encryption:** Uses a **mathematically linked key pair**: a **Public Key** (can be shared with anyone) and a **Private Key** (kept secret by the owner). Data encrypted with the public key can only be decrypted by the matching private key.

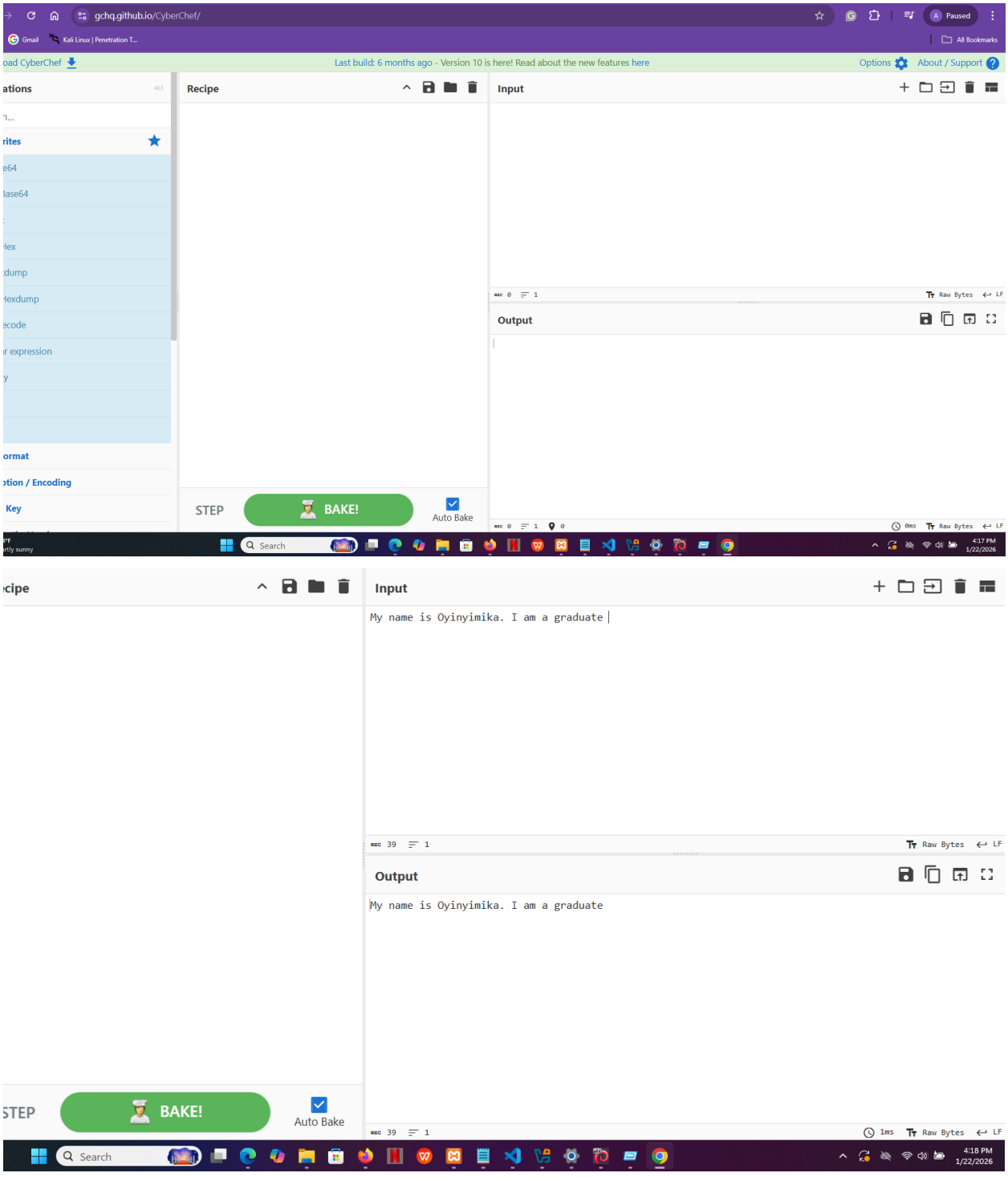
2. Examples of Algorithms

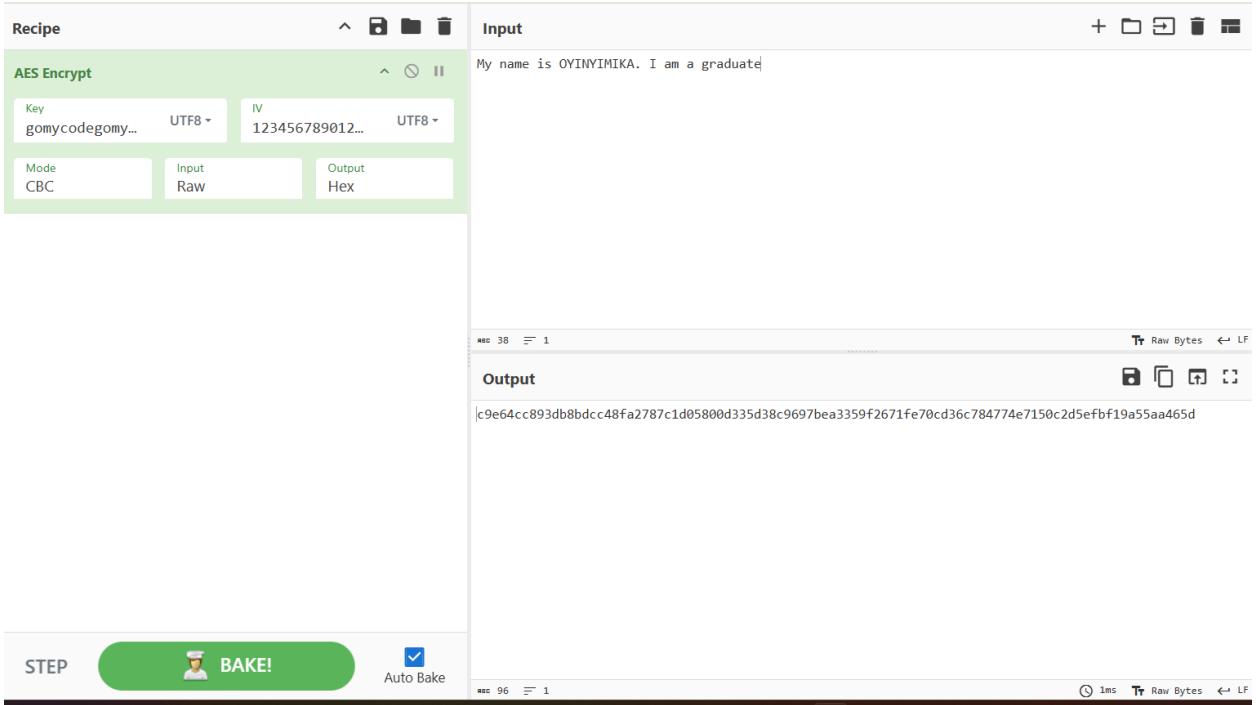
- **Symmetric Algorithms:**
    - **AES (Advanced Encryption Standard):** The current industry standard for securing data.
    - **DES (Data Encryption Standard):** An older, legacy algorithm now considered insecure for modern data.
- **Asymmetric Algorithms:**
    - **RSA (Rivest-Shamir-Adleman):** Widely used for secure data transmission and digital signatures.
    - **ECC (Elliptic Curve Cryptography):** Offers high security with smaller key sizes, making it efficient for mobile devices.

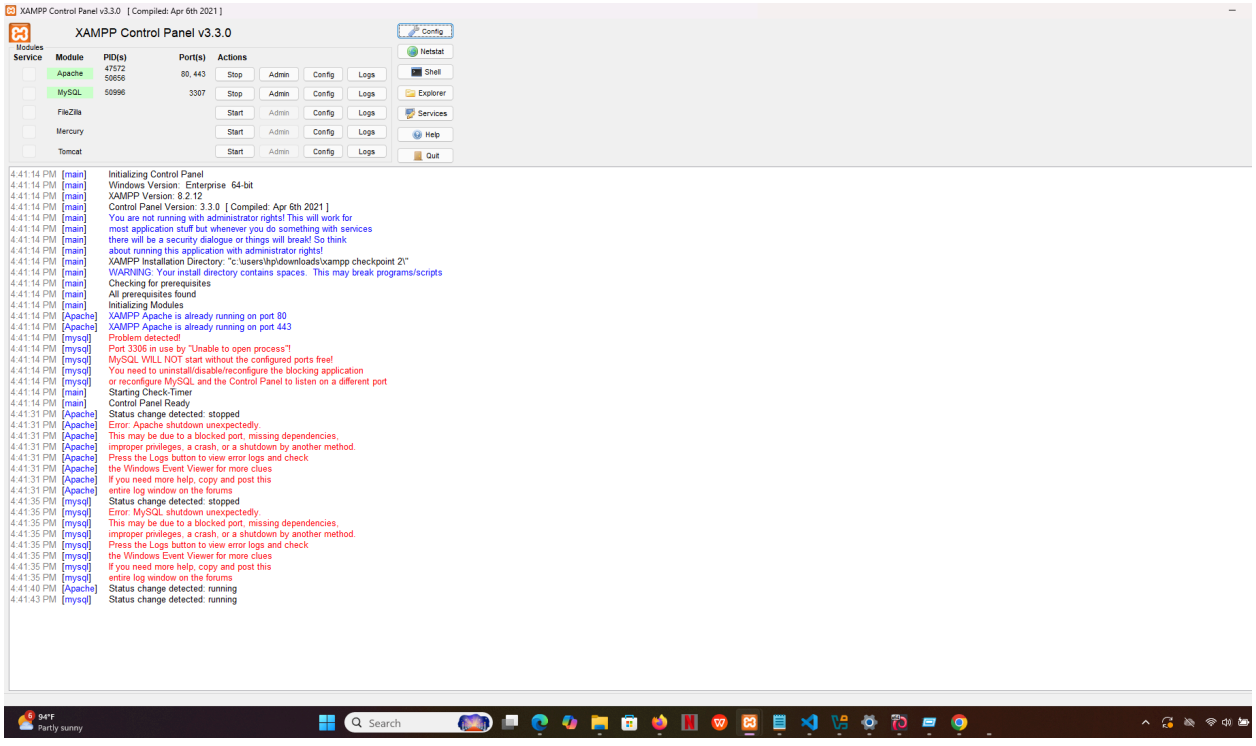
3. Typical Use Cases

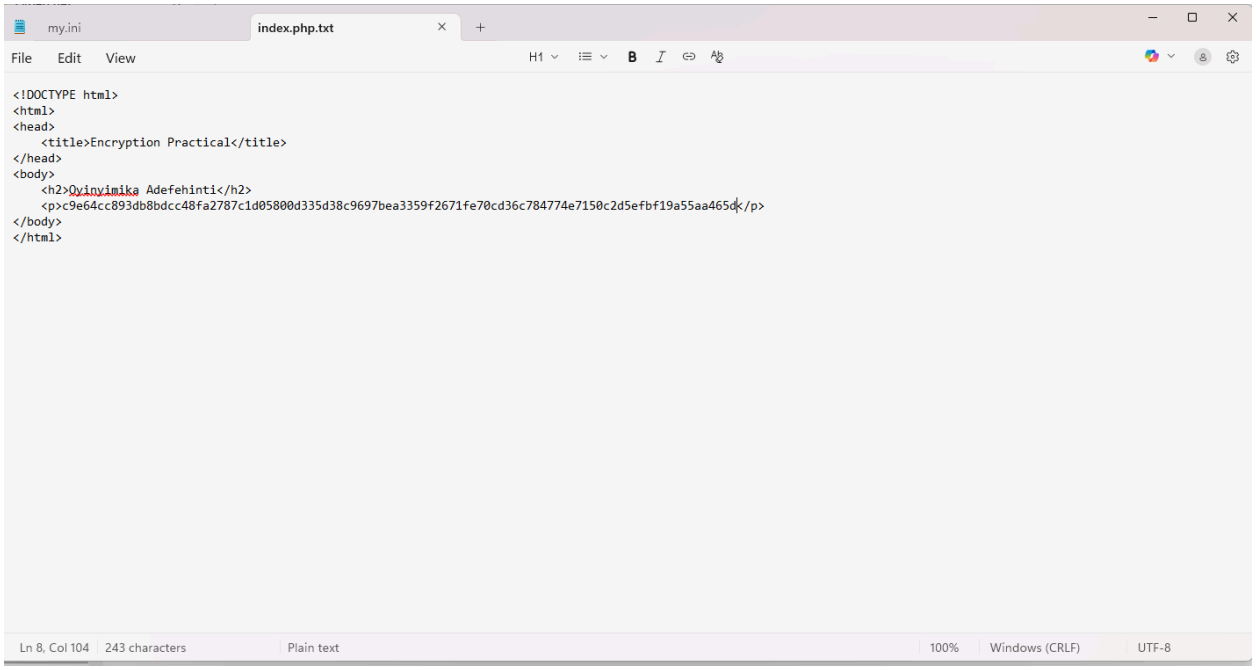
- **Symmetric Encryption:** Used for **bulk data encryption** and **Data at Rest** (such as encrypting a hard drive or a large database) because it is computationally fast.
- **Asymmetric Encryption:** Typically used for **Key Exchange** (securely sending a symmetric key over an insecure network) and **Digital Signatures** to verify the identity of a sender.

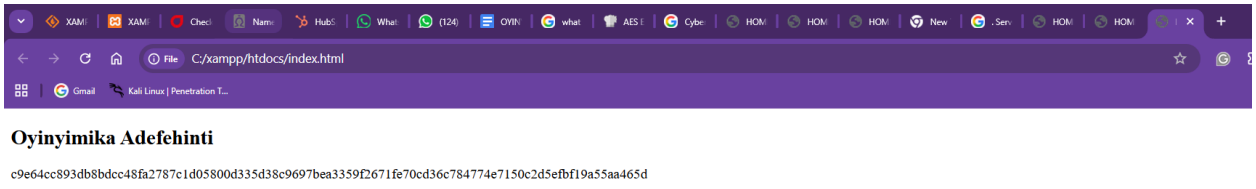
4.


gchq.github.io/CyberChef/
Recipe
Input
Output
STEP
BAKE!
Auto Bake
My name is Oyinyimika. I am a graduate
My name is Oyinyimika. I am a graduate


Recipe
AES Encrypt
Key
gomycodegomy...
UTF8
IV
123456789012...
UTF8
Mode
CBC
Input
Raw
Output
Hex
STEP
BAKE!
Auto Bake
Input
My name is OYINYIMIKA. I am a graduate
Raw Bytes
LF
Output
c9e64cc893db8bdcc48fa2787c1d05800d335d38c9697bea3359f2671fe70cd36c784774e7150c2d5efbf19a55aa465d
1ms
Raw Bytes
LF
Search
4:40 PM
1/22/2026


XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
47572
50656
80, 443
Stop
Admin
Config
Logs
MySQL
50996
3307
Stop
Admin
Config
Logs
FileZilla
Start
Admin
Config
Logs
Mercury
Start
Admin
Config
Logs
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
4:41:14 PM [main] Initializing Control Panel
4:41:14 PM [main] Windows Version: Enterprise 64-bit
4:41:14 PM [main] XAMPP Version: 8.2.12
4:41:14 PM [main] Control Panel Version: 3.3.0 [Compiled: Apr 6th 2021]
4:41:14 PM [main] You are not running with administrator rights! This will work for
4:41:14 PM [main] most application stuff but whenever you do something with services
4:41:14 PM [main] there will be a security dialogue or things will break! So think
4:41:14 PM [main] about running this application with administrator rights!
4:41:14 PM [main] XAMPP Installation Directory: "c:\users\hp\downloads\xampp checkpoint 2\"
4:41:14 PM [main] WARNING: Your install directory contains spaces. This may break programs/scripts
4:41:14 PM [main] Checking for prerequisites
4:41:14 PM [main] All prerequisites found
4:41:14 PM [main] Initializing Modules
4:41:14 PM [Apache] XAMPP Apache is already running on port 80
4:41:14 PM [Apache] XAMPP Apache is already running on port 443
4:41:14 PM [mysql] Problem detected!
4:41:14 PM [mysql] Port 3306 in use by "Unable to open process"!
4:41:14 PM [mysql] MySQL WILL NOT start without the configured ports free!
4:41:14 PM [mysql] You need to uninstall/disable/reconfigure the blocking application
4:41:14 PM [mysql] or reconfigure MySQL and the Control Panel to listen on a different port
4:41:14 PM [main] Starting Check-Timer
4:41:14 PM [main] Control Panel Ready
4:41:31 PM [Apache] Status change detected: stopped
4:41:31 PM [Apache] Error: Apache shutdown unexpectedly.
4:41:31 PM [Apache] This may be due to a blocked port, missing dependencies,
4:41:31 PM [Apache] improper privileges, a crash, or a shutdown by another method.
4:41:31 PM [Apache] Press the Logs button to view error logs and check
4:41:31 PM [Apache] the Windows Event Viewer for more clues
4:41:31 PM [Apache] If you need more help, copy and post this
4:41:31 PM [Apache] entire log window on the forums
4:41:35 PM [mysql] Status change detected: stopped
4:41:35 PM [mysql] Error: MySQL shutdown unexpectedly.
4:41:35 PM [mysql] This may be due to a blocked port, missing dependencies,
4:41:35 PM [mysql] improper privileges, a crash, or a shutdown by another method.
4:41:35 PM [mysql] Press the Logs button to view error logs and check
4:41:35 PM [mysql] the Windows Event Viewer for more clues
4:41:35 PM [mysql] If you need more help, copy and post this
4:41:35 PM [mysql] entire log window on the forums
4:41:40 PM [Apache] Status change detected: running
4:41:43 PM [mysql] Status change detected: running
94°F
Partly sunny
Search





5. **What is Steganography?**

Steganography is the practice of concealing a secret message, file, or image within another non-secret message, file, or image. The primary goal is obscurity: an observer should not even realize that a hidden message exists in the first place.

Steganography vs. Encryption

Encryption is the art of secret writing. Its primary objective is to hide the *meaning* of a message. When you encrypt data, you use mathematical algorithms and keys to scramble it into "ciphertext". To any unauthorized person, the result is clearly a secret message, but it appears as unreadable gibberish. In this way, encryption actually draws attention to the fact that a secret exists, but it relies on the strength of the algorithm to keep it safe.

Steganography, on the other hand, is the art of covered writing. Its primary objective is to hide the *existence* of the message itself. Instead of scrambling data, steganography embeds the secret information inside a seemingly harmless "carrier" or "cover" file, such as a digital photo of a landscape or an MP3 music file. To a casual observer, the carrier looks and behaves exactly like a normal file, leaving no suspicion that a secret communication is even taking place.

Examples

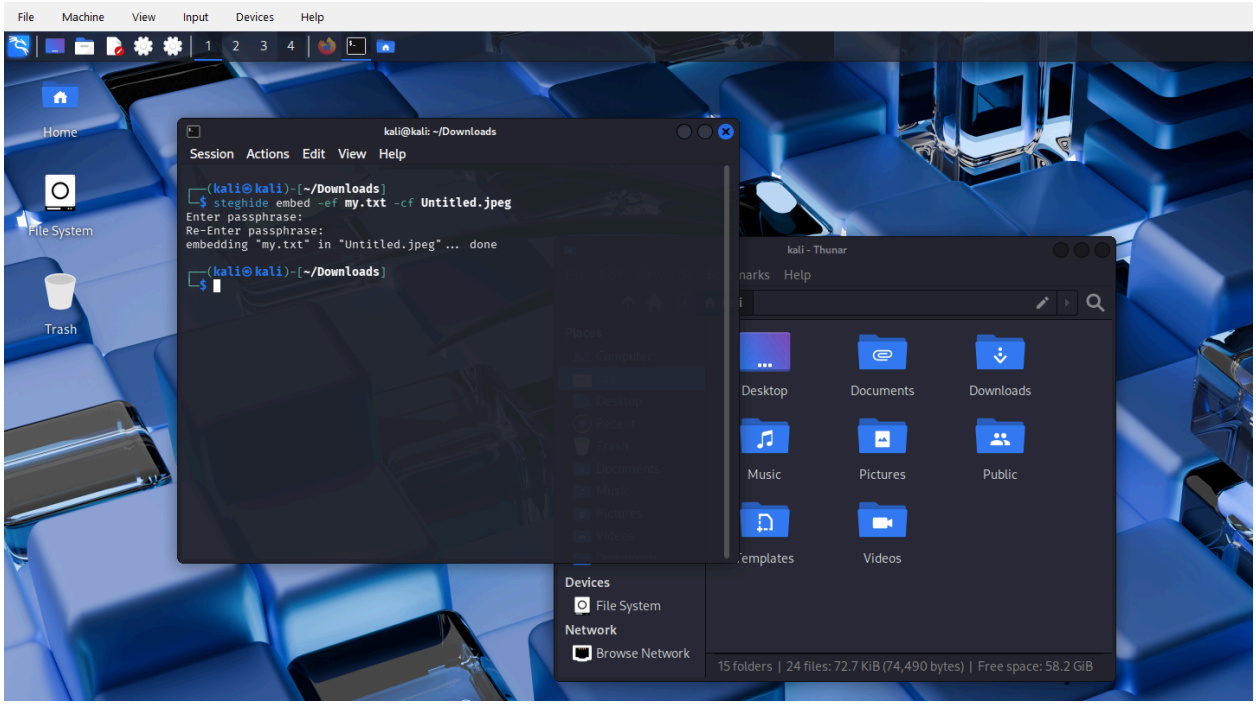
For Attackers

- **Malware Delivery:** An attacker might hide malicious code inside a seemingly harmless `.jpg` or `.png` file. When a user downloads the image, a small "dropper" script extracts the hidden code and infects the system.
- **Command & Control (C2):** Hackers can send instructions to infected computers by hiding commands in images posted on public social media forums, making the traffic look like normal web browsing.

For Defenders

- **Digital Watermarking:** Companies hide unique, invisible identifiers inside their digital assets (like movies or high-res photos). If the file is leaked or stolen, the "hidden" mark can be used to prove ownership or identify the source of the leak.
- **Data Leak Prevention (DLP):** Defenders can use steganographic "tags" on sensitive documents. If those documents are attached to an email, security software can detect the hidden tag and block the outgoing transmission.

6.


File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
kali@kali: ~/Downloads
Session Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ steghide embed -ef my.txt -cf Untitled.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "my.txt" in "Untitled.jpeg"... done
(kali㉿kali)-[~/Downloads]
$
kali - Thunar
narks Help
Desktop
Documents
Downloads
Music
Pictures
Public
Videos
Devices
File System
Network
Browse Network
15 folders | 24 files: 72.7 KiB (74,490 bytes) | Free space: 58.2 GiB

7.

index.php.txt | index.html.txt

File Edit View

```
<!DOCTYPE html>
<html lang="en">
<head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title>HOME | Oyinyimika</title>
</head>
<body>

    <p>Hello Oyinyimika adefehinti</p>
   <p>Encrypted message:c9e64cc893db8bdcc48fa2787c1d05800d335d38c9697bea3359f2671fe70cd36c784774e7150c2d5efbf19a55aa465d </p>

      <img src="oyin.jpg" alt="Description of image" width="500" height="500">
</body>
</html>
```

C:/xampp/htdocs/index.html

Gmail | Kali Linux | Penetration T...

Hello Oyinyimika adefehinti

Encrypted message:c9e64cc893db8bdcc48fa2787c1d05800d335d38c9697bea3359f2671fe70cd36c784774e7150c2d5efbf19a55aa465d

meet.google.com is sharing your screen. Stop sharing Hide

92°F Sunny

Search