1. Whois
whois is a query tool used to retrieve information about domain names, IP addresses, and their registrants.

2. Dig
dig (Domain Information Groper) is a network tool for querying DNS name servers and retrieving information about DNS records.

3. Traceroute
traceroute is a network diagnostic tool used to track the path packets take from your computer to a destination over the network

4. Nslookup
nslookup is a command-line tool used to query DNS to obtain domain name or IP address mapping, or for any other specific DNS record

1. Install Necessary Packages:
sudo apt install openssl

2. Convert Image to Raw Format:

If your image is in a format like JPEG or PNG, you'll need to convert it to a raw format like PPM or BMP. You can use tools like ImageMagick for this:

convert your_image.jpg your_image.ppm

3. Generate Encryption Key:
Create a random encryption key:

openssl rand -base64 32 > encryption_key.txt

4. Encrypt the Image:
Use OpenSSL's enc command to encrypt the image:

openssl enc -aes-256-cbc -salt -in your_image.ppm -out encrypted_image.enc < encryption_key.txt

5. Decrypt the Image:
To decrypt the image, use the same command but replace -in with -d (decrypt mode) and provide the encrypted image and key:

openssl enc -d -aes-256-cbc -salt -in encrypted_image.enc -out decrypted_image.ppm

6. Convert Back to Original Format (Optional):

If you need the decrypted image in its original format, convert it back using ImageMagick:

convert decrypted_image.ppm decrypted_image.jpg

----------Theory----------::

openssl: The command-line tool for working with cryptography.
enc: This tells OpenSSL to use the encryption/decryption functionality.
-aes-256-cbc: Specifies the AES encryption algorithm in 256-bit key length, using the Cipher Block Chaining (CBC) mode.
-salt: Adds a cryptographic salt to the encryption for additional security, making it more resistant to brute-force attacks.
-in image.png: Specifies the input file (your image) that you want to encrypt.
-out image.enc: Specifies the output file for the encrypted data (the resulting encrypted image).
-d: Tells OpenSSL to perform decryption.

7)what is wireshark
wireshark is an open-source network sniffing sotware which is designed to track network packets and through use of different filter opyions available in software
It allows users to inspect the network traffic at a very granular leve
troubleshoot network issues
analyze netowks packets

8)Nmap
Nmap (Network Mapper) is a free, open-source network scanning tool that allows you to scan networks, discover hosts, and identify open ports, services, and vulnerabilities.

commands
1)nmap -sn 192.168.1.1

The nmap -sn command is used for host discovery, also known as a ping scan.
This command checks whether the target is up or down without scanning any ports.

2)nmap -sT 192.168.1.1(TCP Connect Scan)
It performs a full TCP handshake with the target

Nmap sends a SYN packet to the target port.
If the port is open, the target responds with a SYN-ACK.
If the port is closed, the target responds with a RST packet, and the connection is not established.

3)nmap -sS 192.168.1.1
This option specifies a SYN scan (also known as a "stealth scan"). It sends a SYN packet to each target port and waits for a response to determine the port status.

4)nmap -sV 192.168.1.1
The command nmap -sV 192.168.1.1 is used to perform a service version detection scan on the target host.
This command helps identify what services are running on open ports and determines their version numbers.

5)nmap google.com
allowing you to discover open ports and services running on their servers

6)nmap -f google.com
This option enables fragmentation of the packets being sent. Nmap will split the packets into smaller fragments when scanning the target.

7)nmap 192.168.1.0/24
This is the most common method to scan all hosts in a subnet.

8)nmap -sU 192.168.1.1
To scan for open UDP ports, you can use the following command:

9)nmap -p 22,80,443 192.168.1.1
This typically refers to scanning TCP ports, and you can specify which ports to scan:

Q)HMAC
HMAC (Hash-based Message Authentication Code) is a secure method for verifying the integrity and authenticity of messages by
combining a cryptographic hash function with a secret key

Q)Hashing in kmap
Hashing is a process of transforming input data (such as a string, file, or any arbitrary data) into a fixed-size string of characters,
which is typically a sequence of numbers and letters. This output is known as a hash value or hash code

1. Generate a Private Key:
Command : openssl genpkey -algorithm RSA -out private_key.pem -aes256

2. Extract the Public Key:
Next, extract the public key from the private key:
Command : openssl rsa -pubout -in private_key.pem -out public_key.pem

3. Create or Obtain the Plaintext File:
Create or obtain the message you want to sign. For this example, create a file named plaintext.txt:
Command : touch plaintext.txt

4)Sign the Message Using the Private Key :
openssl dgst -sha256 -sign private_key.pem -out signature.bin plaintext.txt

5. Encrypt the Message Using the Public Key
Encrypt the plaintxt.txt file using the public key:
Command : openssl rsautl -encrypt -inkey public_key.pem -pubin -in plaintext.txt -out encrypted.bin

6. Decrypt the Message Using the Private Key
Decrypt the encrypted.bin file using the private key. This decrypts the encrypted.bin file using the private key and saves the decrypted content in decrypted.txt.
Command : openssl rsautl -decrypt -inkey private_key.pem -in encrypted.bin -out decrypted.txt

7. Verify the Signature Using the Public Key
Finally, verify that the signature matches the original plaintxt.txt file: Verified OK
Command : openssl rsa -pubout -in private_key.pem -out public_key.pem

Command : openssl dgst -sha256 -verify public_key.pem -signature signature.bin plaintxt.txt