Assignment Number: 10

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 13/09/2023

**Aim:** Explore the GPG tool of Linux to implement email security.

**LO mapped:** LO6

**Theory:**

GPG is the OpenPGP part of the GNU Privacy Guard (GnuPG). It is a tool to provide digital encryption and signing services using the OpenPGP standard. gpg features complete key management and all the bells and whistles you would expect from a full OpenPGP implementation.

* Step 1: Generate private key and public key pairs for sender and receiver using command

(Repeat for sender and receiver)

* Step 2: Create a file containing sender’s public key which then can be sent to

other users.

(for sender)

* Step 3: Similarly create file containing sender’s private key.
* Step 4: You can create a fingerprint of key using the command.
* Step 5: Sender needs to add in his public key ring, the public key of receiver (for sender)
* Step 6: Listing public keys in keyring

*(From public key rings of specific users)*

* Step 7: Sander can sign the public key of receiver using command

When you sign the key, it means you verify that you trust the person is who they claim to be. This can help other people decide whether to trust that person too. If someone trusts you, and they see that you’ve signed this person’s key, they may be more likely to trust their identity too.

* Step 8: Encrypt the data to send. (Create a file beforehand to be encrypted)

(Only encrypt, .gpg file created)

OR

(Encrypt and sign, ascii file created)

OR

(Encrypt and sign, .gpg file created)

* Step 9: Decrypt the file

**Conclusion:** We implemented Installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.