

Practical 8

**1. Generate a GPG Key Pair**

Run this command to generate your key pair

gpg --full-generate-key

* Select key type: RSA and RSA (option 1).
* Key size: 4096 bits.
* Expiration: Choose a validity period (e.g., 1y for 1 year).
* Enter your name and email.
* Set a **strong passphrase** (remember this!).

2. Export Your Public Key (Optional, for Sharing)

Export your public key to share with others:

gpg --armor --export your-email@example.com > public.key

* This creates public.key (ASCII-armored).

3. Sign and Encrypt a File

**Method 1: Sign + Encrypt for Yourself (Self-Decryption)**

To **sign and encrypt a file so only YOU can decrypt it**:

gpg --sign --encrypt --recipient your-email@example.com file.txt

* Replace your-email@example.com with the email tied to your GPG key.
* This creates file.txt.gpg (binary) or file.txt.asc (ASCII-armored).

Create file

Navigate

Gpg –sign –encrypt –recipient email file.txt

Gpg –decrypt file.txt.gpg > newfile.txt

Q3

**Using Nmap (Command Line)**

1. **Basic Scan (Ping and Port Discovery):**

bash

CopyEdit

nmap 192.168.1.100

* + Scans the top 1000 TCP ports.
  + Shows which ports are open and what services may be running.

1. **Aggressive Scan (More Detail):**

bash

CopyEdit

nmap -A 192.168.1.100

* + Enables OS detection, version detection, script scanning, and traceroute.
  + Good for a full picture of the target system.

1. **Service and Version Detection:**

bash

CopyEdit

nmap -sV 192.168.1.100

* + Identifies service versions on open ports.

1. **Operating System Detection:**

bash

CopyEdit

nmap -O 192.168.1.100

1. **Scan All 65535 Ports:**

bash

CopyEdit

nmap -p- 192.168.1.100

1. **Save Results to File:**

bash

CopyEdit

nmap -A -oN scan\_results.txt 192.168.1.100

**🖼️ Using Zenmap (Graphical Interface)**

1. **Open Zenmap.**
2. In the **Target** field, enter the IP address or hostname of the remote machine.
3. In the **Profile** dropdown, choose one of the predefined scan types, such as:
   * **Intense scan**
   * **Intense scan plus UDP**
   * **Ping scan**
   * Or create a **custom scan**.
4. Click **Scan**.
5. Explore the **Ports/Hosts**, **Topology**, **Host Details**, and **Scans** tabs for details.
6. You can save the scan report via **File > Save Scan**.