Name: Cristian Barreno

Encoding vs Hashing vs Encryption

Prerequisites

- Access to a Linux system
- Install GnuPG installed.
- Basic knowledge of navigating the Linux command line interface.

Task 1

Installation: Ensure that GnuPG is installed on your system. You can install it using the package manager of your Linux distribution. For example, on Ubuntu or Debian, you would use: sudo apt install gnupg

```
Last login: Thu Mar 21 00:27:15 2024 from 192.168.0.247

lyn@lynx:-$
lyn@lynx:-$
sudo apt-get install gnupg
[sudo] password for lynx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.2.27-3ubuntu2.1).
gnupg set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 61 not upgraded.
lynx@lynx:-$ ____
```

Task 2

Encrypting a File

gpg --symmetric malware.txt

```
S. |ynx@|ynx: ~

lynx@lynx: ~

lynx@lynx: ~

gpg: directory '/home/lynx/.gnupg' created

gpg: keybox '/home/lynx/.gnupg/pubring.kbx' created

lynx@lynx: ~$
```

This command is used to symmetrically encrypt a file. GPG will make you create a password, and then you will be set. On my screenshot below you can see that malware.txt.gpg was created.

Task 3

Attempt to view the encrypted file's contents using cat malware.txt.gpg.

I can see that the output is impossible to read, that means the content of the file is encrypted.

To decrypt the malware.txt.gpg file, run:

gpg --decrypt malware.txt.gpg > decrypted.malware.txt

```
T. lynx@lynx:~

lynx@lynx:-$ gpg --decrypt malware.txt.gpg > decrypted.malware.txt
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
lynx@lynx:-$
```

I can see that malware.txt.gpg was redirected to a new folder called decrypted.malware.txt

Verifying Decryption

```
cs_lyrw@lynx:~$

- ① ×
lyrw@lynx:~$ gpg --decrypt malware.txt.gpg > decrypted.malware.txt
gpg: AESZ56.CFB encrypted data
gpg: encrypted with 1 passphrase
lyrw@lynx:~$ cat decrypted.malware.txt
This is evil naughty malware
lynx@lynx:~$
```

I can see that the output matches the original content of malware.txt.