CSCI369 – ETHICAL HACKING ASSIGNMENT

Q4. README

1. run sudo apt-get install -y python3-gnupg on the Ubuntu terminal
2. run sudo apt-get install -y python3-gpg on the Ubuntu terminal
3. run sudo apt install python3-pip on the Ubuntu terminal
4. run sudo pip3 install pycryptodome on the Ubuntu terminal
5. cd to the directory where the ransom.py & pub key are stored at.
6. run sudo python3 ransom.py

TERMINAL OUTPUT

```
sallyeo@sallyeo-VirtualBox:~$ sudo python3 ransomware.py
Enter the 128-bit symmetric key:
symmetric key generated

important.txt was encrypted and saved to encrypted_message.asc

key.txt is successfully deleted

important.txt is successfully deleted

Your file important.txt is encrypted. To decrypt it, you need to pay me $1,000
and send encrypted_key.asc to me
sallyeo@sallyeo-VirtualBox:~$
```

Shows the encrypted key and message.

```
sallyeo@sallyeo-VirtualBox:/$ cd /
sallyeo@sallyeo-VirtualBox:/$ ls
bin    encrypted_key.asc      lib     lost+found  proc  snap      tmp
boot   encrypted_message.asc  lib32   media       root  srv       usr
cdrom  etc                    lib64   mnt         run   swapfile  var
dev    home                   libx32  opt         sbin  sys
sallyeo@sallyeo-VirtualBox:/$ cat encrypted_key.asc
-----BEGIN PGP MESSAGE-----

hQGMA9ln7PZw8SvjAQv+IKSt95PW5/yU+PV1M2DzHZMkvwZMKZI14bV1td04BpRM
dUcpNb/sqsqXF4JQZyrKMMj2n1pnqojpa59OY/fec5q+fLOCFU1ZFcii3dVrm97K
WilbDLz0QU25vncQ64VR6O/8dQnV4PNcDp4zUv6NdI/gW4oBTLD/0cID5U84ytkR
XQLc3ynz34w1nzqdvEaccegiGE18e0fOf9UkbcAfuf/CqY4z+1vYkXgsc4McMOkF
pWfIwzWyR7PHo/wNeasIjc4zDPkEfSwZ2JbJJEcSNwIYC69BYIH/6kdWbUMj8xwF
vuiRbt6JkUjx/3rzIN0s9mL+kcscGSARaNGgxqUO3tJYZB/XGemnKnHwBZtpSppH
k7rA6hM18pLClnazJJFQXXMsorN+9O06uTLI6hYm3N2zfSIKMNIsDlJAWj8a9wmo
nC96FmjlHIfAQLuRre58912JEZ2eOoOk4tFSetOppnv1hsAe6U+eVPvsvzk9ZWKl
PfXANTcfoYJA8BILnXE70ksBhaqtYIA5+1d8v59oAKhXw5b1sI8QTvo05DRPZeFz
uNEiRBzVfRkPtSB24mwJbGErDyZHNYCTJOjrQJhV2Xtr1pTfiOAn7pR4vr8=
=iLQO
-----END PGP MESSAGE-----
sallyeo@sallyeo-VirtualBox:/$ cat encrypted_message.asc
QefnMOeDzfAKBIh2UQx7LTJve8v4s26SIbDdsTNrW4g=sallyeo@sallyeo-VirtualBox:/$
```

Behind the scenes for troubleshooting purposes:

Q4-1 The attacker enters the symmetric key.

```
sallyeo@sallyeo-VirtualBox:~$ sudo python3 ransom.py
Enter the 128-bit symmetric key:
symmetric key generated
```

Q4-2 The attacker encrypts the important.txt

```
Encrypted text(bytes): b'A\xe7\xe70\xe7\x83\xcd\xf0\n\x04\x88vQ\x0c{-2o{\xcb\xf
8\xb3n\x92!\xb0\xdd\xb13k[\x88'
Encrypted text(ascii): QefnMOeDzfAKBIh2UQx7LTJve8v4s26SIbDdsTNrW4g=
important.txt was encrypted and saved to encrypted_message.asc
```

The attacker importing his public key to encrypt the key.txt

```
Importing public key...


[{'fingerprint': 'F36D2264BDC7CE86AA6CEA14311505FD2D44ED75',
  'ok': '1',
  'text': 'Not actually changed\nEntirely new key\n'}]

Listing keys...
Public keys:
[{'algo': '1',
  'cap': 'scESC',
  'compliance': '23',
  'curve': '',
  'date': '1660043636',
  'dummy': '',
  'expires': '1723115636',
  'fingerprint': 'F36D2264BDC7CE86AA6CEA14311505FD2D44ED75',
  'flag': '',
  'hash': '',
  'issuer': '',
  'keygrip': 'DD7F3D02828E3F86C1335399AF60B51AC4D63E5F',
  'keyid': '311505FD2D44ED75',
  'length': '3072',
  'origin': '0',
  'ownertrust': '-',
  'sig': '',
  'sigs': [],
  'subkey_info': {'D967ECF670F12BE3': {'algo': '1',
                                       'cap': 'e',
                                       'compliance': '23',
                                       'curve': '',
                                       'date': '1660043636',
                                       'dummy': '',
                                       'expires': '1723115636',
                                       'flag': '',
                                       'hash': '',
                                       'issuer': '',
                                       'keygrip': 'unavailable',
                                       'keyid': 'D967ECF670F12BE3',
                                       'length': '3072',
                                       'origin': 'unavailable',
                                       'ownertrust': '',
                                       'sig': '',
                                       'token': '',
                                       'trust': '-',
                                       'type': 'sub',
                                       'uid': '',
                                       'updated': ''}},
  'subkeys': [['D967ECF670F12BE3',
               'e',
               '00E99B412D507065527C8C7AD967ECF670F12BE3',
               '8D86FD8A6DF7E03D58B6D7BC608479981F1CBB18']],
  'token': '',
  'trust': '-',
  'type': 'pub',
  'uids': ['sally <sally@uow.edu.au>'],
  'updated': ''}]
Private keys:
[]
```

Q4-3 Successfully encrypt the key.txt

```
Encrypting status...
True


encryption ok


gpg: WARNING: unsafe ownership on homedir '/home/sallyeo'
[GNUPG:] KEY_CONSIDERED F36D2264BDC7CE86AA6CEA14311505FD2D44ED75 0
[GNUPG:] KEY_CONSIDERED F36D2264BDC7CE86AA6CEA14311505FD2D44ED75 0
gpg: checking the trustdb
[GNUPG:] KEY_CONSIDERED F36D2264BDC7CE86AA6CEA14311505FD2D44ED75 0
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2024-08-08
[GNUPG:] ENCRYPTION_COMPLIANCE_MODE 23
[GNUPG:] BEGIN_ENCRYPTION 2 9
[GNUPG:] END_ENCRYPTION
```

Q4-4 & Q4-5 Delete key.txt and important.txt

Q4-6 Display warning message.

```
Current working dir: /home/sallyeo
key.txt is successfully deleted

Current working dir: /
important.txt is successfully deleted

Your file important.txt is encrypted. To decrypt it, you need to pay me $1,000 and send encrypted_key.asc to me
```