**Faculty of Computer Science and Engineering**

|  |
| --- |
| **CSCI 301** |
| **Contemporary Topics in Security** |

**Ransomware Lab (This is a regular lab not the programming assignment)**

Date Posted : 30/05/2021

**You have Two weeks to submit the task**

**GROUP of TWO ASSIGNMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| Last Name | First Name | Student ID | Signature |
|  |  |  |  |
|  |  |  |  |

The programming assignment introduces students to a practical view of ransomware. This is a **group of two** assignment. **The members of the group must be part of the same lab** . Students will implement two flavours of ransomware attacks, using

**Learning outcomes:**

The learning objectives of this lab allow students to understand:

* Attack a vulnerable computer by Create a ransomware program
* To scan and select appropriate target files according to their type.
* Generate cryptographically secure random numbers
* Generate RSA based asymmetric key pairs, and AES\_CBC
* To develop a hybrid encryption scheme based on the RSA based asymmetric key pairs, and AES\_CBC based symmetric keys, applied for each targeted files.
* Develop recovery programs for the recovery of the different types of encryption keys, as well as programs for the recover of each of the encrypted files.

1. **Overview**

In this assignment, your task is to create a simple ransomware using Python script with the pycryptodome package.

**The requirements are as follows**:

1. You are an attacker who has already broken into a victim’s Linux/Unix machine on which Python 3.5 or above and pycryptodome package are installed;
2. You attacker will put your ransomware program, which is not necessary to be a single file, in the victim’s machine;
3. The victim has several text files in the **directory** (Mydirectory) where the ransomware is located.
4. Note that these text files have extension “.txt”.
5. The text files will be provided by the lab instructor.
6. **Your task**
7. **The attack:**

The ransomware should perform the following:

1. Throughout this task, whenever random number need be generated, you must use a cryptographically secure pseudo random number generator.
2. The ransomware will use the RSA algorithm to generate an asymmetric key pair: a public key and a ***private key, the latter is called ransomkey.bin***
3. For each \*.txt file discovered by the ransomware in Mydirectody, it will generate a distinct 128 bits random key for symmetric encryption using AES\_CBC. The file present in the directory that are not \*.txt files will not be modified.
4. Each of the \*.txt file will be encrypted with its corresponding symmetric key and stored as a \*.enc file in Mydirectory.
5. The symmetric keys are encrypted with the attacker’s public key and stored together with the corresponding files encrypted contents. The original \*.txt files must be removed. Make sure that they cannot be recovered.
6. Once the files are encrypted, the ransomware will display a message for asking ransom “Your text files are encrypted. To decrypt them, you need to pay me $5,000 and send ransomkey.bin in your folder to [me].” “[me]” should be your student email address
7. To decrypt contents, the attacker sells the private key to the victim
8. **The recovery**

You must also write two programs called respectively Key-recovery and file-recovery:

1. Key-recovery : is a program that will recover all the symmetric keys used for the encryption of the original \*.txt files. You will need to use the RSA algorithm to perform this operation. First, The key-recovery program should decrypt the encrypted key (ransomkey.bin), encode it to base64 and store it in ransomkey.txt
2. File-recovery: is a program that will recover all the original files by decrypting the encrypted files using AES\_CBC, along with the corresponding symmetric keys recovered in (a)
3. **Important Note:**
4. The keys used to encrypt files must not appear in the source code of the ransomware program and should not be stored in the plaintext format in the victim’s system.
5. AES\_CBC mode of encryption needs an initial vector (IV) (128 bit-long) for encryption and decryption. Your ransomware will generate this IV using cryptographically secure random number generators, and send it together with ransomkey.bin to the victim upon payments.
6. **You must document ALL your programs.**
7. **You must use pycryptodome for AES and public key encryption, and random number generation**
8. **When asked to provide the source and executable of a program. DO NOT dump the code into a word document. Our objective is to be able to compile (or interpret) and run your code.**
9. **Submission**
10. **Your assignment MUST satisfy all the above functional requirements**
11. **You must also Make a folder named** **ransomware-task-ID1-ID2 which includes**
12. The ransomware attack program**( fully documented)**
13. The ransomware Recovery programs for the key and the files**(fully documented)**
14. The private key file associated with the public key used in a ransomware program (named ransomprvkey.pem)
15. A short report that:
    1. Provides all necessary information to run your programs (e.g., the other python packages for your code) **( executable and source code**)
    2. And explain the execution of your program for each file that is encryped (**with screenshots**)
    3. And explain the execution of your program for each key that is encrypted or decrypted (**with screenshots**)
16. Compress the ransomware-task-ID1-ID2 folder using a zip program to create csci301-ransomware-task-ID1-ID2
17. Use Moodle to upload your zip file.

**Attaching code without any explanation will not receive credits.**

**Additional instructions will be provided by the Lab instructor.**

**There will be random code interviews conducted.**

1. **Input files**

The lab instructor will provide you with a set of files that you will download and store in the Mydirectory directory that you will create for this task.

1. **Marking Grid**

The following marking grid will be adopted.

|  |  |  |
| --- | --- | --- |
| Item | (including detailed description in the report) | **Marks**  The Description counts for 25%  The Software counts for 75% |
| **Ransomware attack** |  | **55** |
|  | **Search for the target files** | ***5*** |
|  | **RSA** | ***5*** |
|  | *Selection of a random Prime* |  |
|  | *Selection of a random public key* |  |
|  | *Generation of the private key* |  |
|  | **AES\_CBC** | ***10*** |
|  | *Selection of symmetric key for each target files* |  |
|  | **File Encryption** |  |
|  | *Encryption of each target file with a specific symmetric key, deletion of originals* | ***15*** |
|  | **Key Encryption and storage** |  |
|  | *Encryption of each symmetric key with the public key.* | ***20*** |
| **Recovery** |  | ***20*** |
|  | **Recovery of the symmetric keys** | ***10*** |
|  | **Recovery of each corresponding encrypted file** | ***10*** |
|  |  |  |
| **Report** |  | ***25*** |
|  | Description of Ransomware attack |  |
|  | Description of ransomware Recovery |  |
|  | **Executable, source or attack program** | ***10*** |
|  | **Executable, source or recovery program** | ***10*** |
|  | **Zipped folder** | ***5*** |