**Actividad II**

**Generalidades**

Esta actividad se puede desarrollar en parejas (grupo de dos).

**Objetivo.**

Desarrollar un ransomware básico usando las siguientes herramientas:

1. Procedimientos para cifrar/descifrar archivos en Python: Click [aquí](https://colab.research.google.com/drive/1Wt2-klTUY1ckajkHPwAsf5dpefM5Xtuf?usp=sharing)
2. Procedimientos para intercambiar una llave sesión entre dos partes en Python:

Click [aquí](https://colab.research.google.com/drive/1DwYgja8k8oye__in6t0CZQpvhJ_paYJJ?usp=sharing)

**Operación de un ransomware.**

Un ransomware es un tipo de programa malicioso cuyo objetivo es cifrar archivos en la maquina víctima para evitar el acceso a estos archivos. Su operación se describe a continuación:

1. El ransomware se instala sobre la maquina víctima con permisos adecuados.
2. El ransomware abrirá una conexión con una máquina operada por el atacante. A través de esta conexión, ambas partes compartirán un secreto común usando un protocolo criptográfico.
3. Usando este secreto común, el ransomware genera una llave simétrica y usa esta llave para cifrar archivos almacenados en la máquina víctima.
4. El ransomware notifica al usuario víctima sobre el ataque y como proceder para recuperar sus archivos (normalmente mediante un pago a una cuenta en bitcoin).
5. Una vez que el usuario víctima ha realizado el pago, el atacante, quien también posee el secreto común (intercambiado en el paso **1**), le enviará las instrucciones para generar la llave a partir del secreto común y así poder descifrar los archivos.

**Actividades**

1. Implemente un código prueba de concepto de los pasos 2, 3, 4, 5 descritos previamente. Tener en cuenta las siguientes recomendaciones:

* Implementación de paso 2: Usando sockets TCP y el esquema trapdoor RSA (codificado en **b**), implemente el siguiente protocolo.

|  |  |  |
| --- | --- | --- |
| Maquina Víctima |  | Maquina Atacante |
|  |  |  |
|  |  |  |
|  |  |  |

Una vez se ha compartido entre la maquina víctima y la maquina atacante, implemente un método similar a getKey(password) de **a**, para derivar una clave simétrica .

* Para el paso 3, se sugiere implementar un método que escanee archivos dentro el disco, y luego proceda a cifrarlos usando el método encrypt(key,filename) provisto en **a** y la llave simétrica . Recuerde borrar el archivo original después de haberlo cifrado (Es decir, sólo dejar el archivo cifrado en disco).
* Para el paso 4, se sugiere implementar una función que genere un archivo de texto que indique qué archivos se han cifrado y las instrucciones (incluye cuánto se debe pagar) para descifrarlos/recuperarlos.
* Para el paso 5, se sugiere escribir una función que reciba un vector con las rutas de los archivos cifrados y . Este método tendrá que derivar la llave simétrica a partir de y procederá a descifrar los archivos cifrados. Para esto, use el método decrypt(key,filename) provisto en **a** y la llave simétrica .

1. Además de la implementación prueba de concepto de su ransomware, responda las siguientes preguntas:

* Asuma el rol de atacante. Suponga que usted quiere convertir su ransomware en un arma de ataque
  + ¿Qué estrategias usaría para que la víctima lo instale en su máquina? Es decir, ¿cómo implementaría el paso 1 descrito en la operación?
  + Describa otra forma para implementar el paso 2 (intercambio de llaves) para evitar sospechas. Es decir, sin usar sockets, ¿cómo implementaría este paso? Sugerencia: Uso de canales escondidos con ICMP.
* Asuma el rol de defensor.
  + Describa políticas y prácticas para garantizar confidencialidad, integridad y disponibilidad de recursos informáticos en la organización. En particular, estas políticas y prácticas deberían mitigar la ocurrencia de este tipo de ataques.

**Entregables**

1. Códigos escritos en Python (versión 3.7.9 o superior) de su ransomware.
   * Código que se ejecuta en la máquina víctima.
   * Código que se ejecuta en la máquina del atacante.
2. Documento con sus respuestas a las preguntas propuestas.