Universidad del Norte
Departamento de Ingeniería de Sistemas y Computación
Criptografía

EXAMEN FINAL

Fecha de entrega: 27 de noviembre de 2024, 6:30 a.m.

Ransomware

El objetivo de este examen es desarrollar un ransomware básico en el que se apliquen todos los conceptos vistos a lo largo del curso (con la excepción del protocolo Tor).

Para la operación de un ransomware se debe tener en cuenta los siguientes lineamientos:

1. El ransomware se instala sobre la máquina 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 utilizando un protocolo de intercambio de llaves.
   - En particular, se debe utilizar el protocolo AKE v.2.
     - Se debe generar un certificado digital para el atacante y para la víctima. Estos certificados deben tener (como mínimo) la identidad y la llave pública asociada.
       - Las llaves públicas deben ser generadas utilizando RSA con 2048 bits.
       - Los certificados pueden ser construidos como diccionarios con (mínimo) dos llaves: `id` para la identidad y `pk` para la llave pública.
     - El conjunto $\mathcal{K} \coloneqq \{0,1\}^{1024}$.
     - Utilice el esquema de firma digital `pkcs1_15` de `Crypto.Signature`. Recuerde aplicar el paradigma de hash luego firma con una función hash criptográfica de su elección.
     - Utilice el criptosistema `PKCS1_OAEP` de `Crypto.Cipher` para el cifrado y descifrado asimétrico.
     - Se debe utilizar RSA con 2048 bits para la generación del par de llaves de corto plazo.

3. Utilizando este secreto común, el ransomware genera una llave simétrica usando una KDF (Key Derivation Function) y usa esta llave para cifrar archivos almacenados en la máquina víctima.
   - Como KDF pueden utilizar una función hash criptográfica de su elección.

- Deben diseñar un método para cifrar los archivos utilizando el cifrador AES en modo CBC.

4. El ransomware notifica al usuario víctima sobre el ataque e indica cómo proceder para recuperar sus archivos (normalmente mediante un pago a una cuenta en bitcoin u otra criptomoneda).

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 recuperar sus archivos.

Para este proyecto deberán implementar un código prueba de concepto de los pasos 2, 3, 4 y 5 descritos previamente. Tengan en cuenta las siguientes recomendaciones:

- El código será una simulación de la operación de un ransomware, específicamente de los pasos 2, 3, 4 y 5.
- Dado que se espera una simulación, no es necesario realizar un código para conectar vía sockets el cliente (ransomware) y la máquina del atacante.
- Se sugiere realizar la implementación en un archivo de **Google Colab**.
- Se sugiere implementar un método que escaneé archivos dentro del disco de la máquina de Colab y luego proceda a cifrarlos.
- Se sugiere notificar (por medio de un mensaje en Colab) sobre qué archivos se han cifrado y cuánto se debe pagar para descifrarlos.
- Se sugiere escribir una función que reciba las rutas de los archivos cifrados y proceda a descifrarlos.

Si desean implementarlo en un escenario real están **bajo su propio riesgo**, ya que este tipo de malware conlleva una potencial perdida de información.

Adicionalmente, se debe proponer e implementar una estrategia para **verificar la integridad** de los archivos que fueron afectados por el ransomware.

Finalmente, respondan a las siguientes preguntas:

1. Asuman el rol del atacante. Imaginen que realizan una implementación funcional y real de su malware y lo convierten en un arma de ataque ¿Qué estrategias utilizarían para que la víctima lo instale en su máquina? Es decir, ¿Cómo implementarían el paso 1 descrito en la operación?

2. Asuman el rol del defensor. Describan políticas y prácticas para garantizar la confidencialidad, la integridad y la disponibilidad de recursos informáticos en una organización. En particular, estas políticas y prácticas deberían mitigar la ocurrencia de este tipo de ataques.

Para tener en cuenta:

- La solución (análisis) debe ser original.
- Puede utilizar Python, Java o el lenguaje de su elección para desarrollarlo.
    - Se recomienda utilizar Python, ya que en la explicación presentada se utiliza la librería **pycryptodome**.
- Todos los códigos deben estar documentados por los integrantes del equipo.
- Todo el código debe ser subido a un repositorio de **GitHub**.
- La sustentación del examen se realizará el día 27 de noviembre del 2024 en el horario de 08:30 a.m. a 12:30 p.m. en el laboratorio de ciencias de la computación (Bloque K, piso 6).
    - En este mismo horario también se sustentará el **proyecto** desarrollado a lo largo del semestre.
- **Todos** los integrantes del equipo deben estar presentes durante la sustentación del examen y del proyecto.