Práctica 3. Protección de datos

Para realizar en grupos de 4 personas. La composición de los grupos debe ser diferente que en las prácticas 1 y 2.

Todos los ejercicios deben ser realizados por todos los integrantes del grupo, aunque en la memoria, bastará con que se incluyan las evidencias de uno de ellos.

NOTA: En la nomenclatura de los archivos, *GN* hace referencia a su grupo de prácticas (p.ej: 1.1.1)

1) Utilizando Cryptool 1, generen un par de claves RSA de 2048 bits.
   a) Documenten el proceso.
   b) ¿Qué números conforman la clave pública?
   c) Realicen pruebas de cifrado y descifrado sobre el archivo `secreto.txt` disponible en Moodle. Comenten los resultados obtenidos.

2) Utilizando Cryptool 1, generen una clave D&H con 1000 < p < 2000.
   a) ¿Qué utilidad puede tener la clave obtenida?
   b) ¿Qué problemas de seguridad pueden darse con este método? ¿Cuál sería la solución?

3) Instalen la herramienta QuickHash y prueben las opciones básicas.
   a) Si se modifican los atributos de un archivo (p.ej. sólo lectura), ¿varía el hash?
   b) Busquen, prueben y documenten herramientas o comandos para calcular hashes, que estén disponibles de forma nativa en sistemas recientes de Windows, Linux y Mac OS.
   c) Seleccionen una cadena de texto de 6 letras (sólo minúsculas y sin ñ) y calculen su hash md5.
   d) Seleccionen una cadena de texto de 16 letras (sólo minúsculas y sin ñ) y calculen su hash md5.
   e) Seleccionen una cadena de texto de 6 letras (con minúsculas, mayúsculas, letra ñ/Ñ y números) y calculen su hash md5.

4) Instalen la herramienta John the Ripper y prueben las opciones básicas.
   a) Utilicen JtR para crackear el hash calculado en el apartado c del ejercicio 3. Describan las características de la máquina en la que ejecuta JtR, el comando JtR utilizado y el número de hashes por segundo que puede probar. ¿Cuánto tarda en crakear el hash?
   b) Calculen cuanto tardaría en crackear los hashes de los apartados d y e en la misma máquina.

5) Instalen la herramienta hashcat y prueben las opciones básicas.
   a) En la misma máquina que el ejercicio 4, utilicen hashcat para crackear el hash calculado en el apartado c del ejercicio 3.
   b) Comenten las diferencias observadas entre ambas herramientas.

6) Utilizando 7-Zip generen un archivo comprimido protegido con contraseña, teniendo en cuenta lo siguiente:
   - El algoritmo de compresión debe ser .zip
   - La contraseña debe ser de 6 letras (sólo minúsculas y sin ñ)
   - El algoritmo de cifrado debe ser AES.
   - Tome como base el archivo `secreto.txt`.

   a) Documenten el proceso.
   b) Utilicen JtR para intentar obtener la contraseña. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados obtenidos.

7) En una máquina Linux de la que dispongan, revisen los archivos `/etc/passwd` y `/etc/shadow` y realicen lo siguiente:
   a) Indiquen cuál es el objetivo de esos archivos y expliquen el formato de los mismos (los campos que contienen y qué significa cada campo).
   b) Averigüen qué algoritmo de hash se está utilizando.
   c) ¿Cuál es el propósito del campo "*salt*"?
   d) Intenten calcular manualmente el hash de la contraseña de uno de los usuarios y comprueben si coincide con el que figura en el archivo.
   e) Utilicen JtR para intentar obtener la contraseña de algún usuario. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados obtenidos.

8) Descarguen el gestor de contraseñas KeepassXC (https://keepassxc.org/download). Antes de instalarlo, hagan lo siguiente:
   a) Verifiquen el archivo descargado con el hash sha-256 y la firma PGP que se facilitan en la web. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados.
   b) ¿Qué método de verificación es más seguro? ¿Cuál es la diferencia?
   c) Una vez verificado el archivo, instalen la herramienta y prueben las opciones básicas.
   d) Además de la usabilidad, ¿qué diferencia importante, en términos de seguridad, encuentran entre usar un gestor de contraseñas o un archivo de texto cifrado con AES, por ejemplo?

9) Seleccionen un sitio web que utilice https y cuyo certificado digital contenga una clave pública RSA.
   a) Descarguen el certificado y analícenlo con la herramienta OpenSSL.
   b) ¿Qué números conforman la clave pública? Indíquelos en hexadecimal y decimal.
   c) ¿Cuál es el tamaño de la clave en bits? En caso de que no lo indicase de manera explícita el certificado, ¿de qué forma se podría saber?
   d) ¿Cuál es el contenido del campo Common Name? ¿Por qué es importante este campo?

10) Utilizando OpenSSL:
   a) Indique el comando necesario para cifrar el archivo `secreto.txt` con el algoritmo AES con una clave de 256 bits.
   b) ¿Cómo es el tiempo, comparado con RSA?

11) Utilizando OpenSSL, genere una clave RSA de 2048 bits.
    a) Indique el comando utilizado y la clave pública obtenida.
    b) ¿Cuál es el número e de la clave pública?
    c) Indique el comando necesario para cifrar el archivo `secreto.txt` usando la clave pública generada.
    d) ¿Cómo es el tiempo, comparado con el obtenido en el ejercicio 1?

12) Sigan los pasos vistos en clase para obtener un certificado digital de la FNMT.
    a) Documenten el proceso.
    b) Exporten el certificado de clave pública (¡no incluyan la clave privada!) de cada uno en formato PKCS #7 y guárdenlo con la siguiente sintaxis:
    `P3_Ej12_`*`GN`*`_Apellidos,_Nombre.p7b`

    NOTA:
    - IMPORTANTE: Tengan en cuenta que este certificado permite autenticación y firma digital con validez legal. De modo que deben almacenarlo en un lugar seguro y nunca revelar la clave privada.

13) Generen un par de claves PGP asociadas a su cuenta de la UDC.
    a) Documenten los pasos seguidos.
    b) Exporten la clave pública en formato texto de cada uno y guárdenla con la siguiente sintaxis: `P3_Ej13_`*`GN`*`_Apellidos,_Nombre.asc.`

14) Instalen y configuren la herramienta Thunderbird y prueben a enviar correo seguro, usando GPG, con las claves generadas en el ejercicio anterior. Prueben, al menos, los siguientes casos:
    - Envíen un correo firmado al resto de integrantes de su grupo.
    - Envíen un correo cifrado al resto de integrantes de su grupo.
    - Envíen un correo firmado y cifrado al resto de integrantes de su grupo.

    a) Documenten los pasos seguidos y muestren capturas de pantalla para cada caso.

    NOTAS:
    - Deben conservar (cada miembro del grupo) al menos un correo de prueba de cada caso, para el momento de la defensa).
    - Los mensajes deben tener "asuntos" suficientemente descriptivos de la prueba realizada (P. ej: "PGP - Prueba de correo electrónico firmado con la clave 0x1234" en lugar de "Prueba 3" o "sin asunto")

15) Imaginen que no disponen de una herramienta de correo con soporte integrado para PGP y deben generar el contenido del correo directamente con GPG en línea de comandos. Suponiendo que el texto del cuerpo del mensaje está en un archivo "`cuerpo-correo.txt`", indiquen los comandos GPG adecuados para:
    a) Generar un correo firmado para el resto de integrantes de su grupo.
    b) Generar un correo cifrado para resto de integrantes de su grupo.
    c) Generar un correo firmado y cifrado para el resto de integrantes de su grupo.
    d) Verificar un correo firmado recibido
    e) Descifrar un correo cifrado recibido
    f) Verificar y eescifrar un correo cifrado recibido

    NOTA: asegúrense de estar usando GnuPGP versión 2.X o superior.

    CONSEJO: prueben a enviar los correos generados, desde una herramienta de correo sin soporte para PGP (p. ej.: Outlook Web) a otra con soporte (p. ej.: la utilizada en el ejercicio anterior), con el objetivo de comprobar que los mensajes son interpretados correctamente.

16) En el ejercicio anterior usaron comandos PGP orientados a generar contenido válido para ser enviado por correo electrónico, pero PGP también puede usarse para cifrar archivos. Suponga que quiere almacenar el archivo `secreto.txt` cifrado con clave pública.
    a) Indiquen el comando GPG apropiado.
    b) ¿En qué se diferencia del comando usado para cifrar un correo electrónico?
    c) ¿Y si quiere cifrarlo con cifrado simétrico?

17) Configuren una herramienta de correo electrónico de su elección, con soporte para S/MIME y prueben, al menos, los siguientes casos (IMPORTANTE: Tengan en cuenta que si utilizan un certificado de la FNMT la firma tiene validez legal, de modo que firmen únicamente mensajes de prueba y conserven en un lugar seguro sus certificados):
    - Envíen un correo firmado al resto de integrantes de su grupo.
    - Envíen un correo cifrado al resto de integrantes de su grupo.
    - Envíen un correo firmado y cifrado al resto de integrantes de su grupo.

    a) Documenten los pasos seguidos y muestren capturas de pantalla para cada caso.

    NOTAS:
    - Deben conservar (cada miembro del grupo) al menos un correo de prueba de cada caso, para el momento de la defensa).
    - Los mensajes deben tener "asuntos" suficientemente descriptivos de la prueba realizada (P. ej: "S/MIME - Prueba de correo electrónico firmado con la clave 0x1234" en lugar de "Prueba 3" o "sin asunto")

Modo y fecha de entrega

La práctica se entregará vía Moodle, no más tarde del **viernes 6 de mayo a las 13:30**. Sólo una entrega por grupo. Un único archivo `P3_GN.zip`, que debe contener:

- Memoria, en formato .pdf, explicando con claridad lo que se pide en cada uno de los apartados.
    - NO repita el enunciado. Indique simplemente el apartado (p.ej. 1. a), 1.b), etc.)
    - Se valorará positivamente el que la memoria está firmada digitalmente por todos los integrantes del grupo.
- Archivos indicados en el enunciado de la práctica, directamente sobre el directorio raíz, sin subcarpetas, respetando la nomenclatura indicada.

Defensa

Posteriormente a la entrega, será necesario hacer una defensa de la misma. En la defensa deben estar presentes todos los integrantes del grupo.