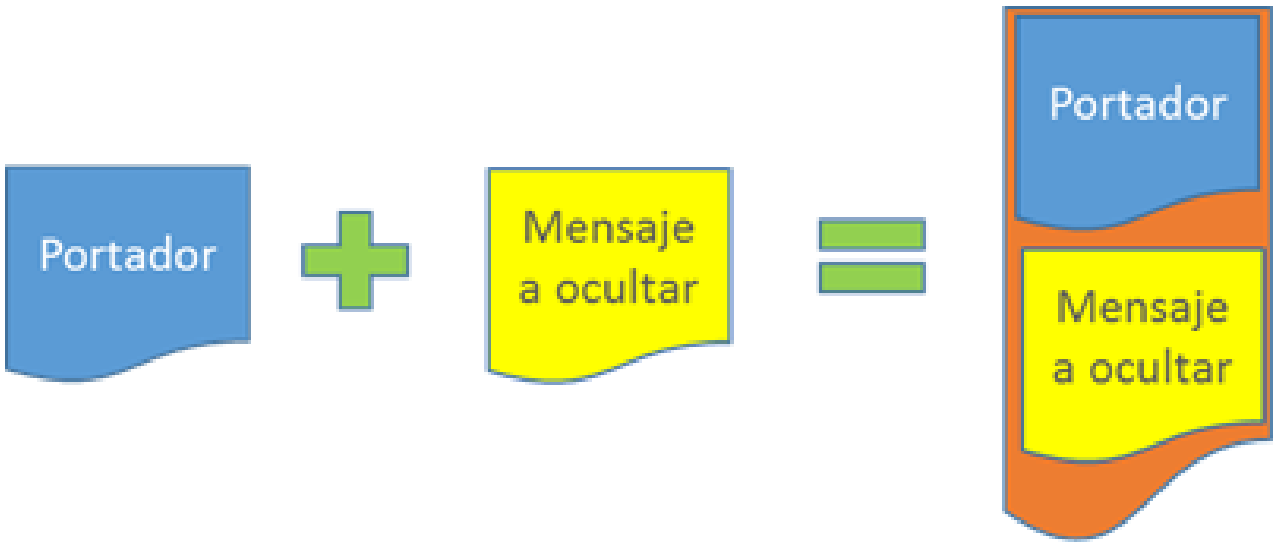
CONCEPTOS SEGURIDAD

1.- ESTEGANOGRAFIA

- **la esteganografía busca ocultar la existencia propia del mensaje**.

- **La combinación entre esteganografía y criptografía** podría ser la mezcla perfecta para el envío seguro de un mensaje secreto entre el emisor y el receptor del mismo.



Desde MSDOS

- 1) Tener una fotografía donde queramos esconder el mensaje, texto, contraseña, etc.
- 2) Crear un fichero .TXT y escribir en él, el texto etc que queremos esconder.
- 3) Abrimos el CMD.
- 4) Ejecutamos el comando copy /?, que nos muestra todas las opciones.
- 5) Ejecutamos **copy /b [ficherooriginal-foto.jpg]+[fichero.txt donde hemos escrito el texto a esconder] [nombredelfciherodesalida.jpg]**

    - copy /b file.jpg + mensaje.txt oculto.jpg

    - cat kitty.jpg datos.zip > imagen_secreto.jpg
    - type kitty.jpg datos.zip > imagen_secreto.jpg

Herramientas

- Stegsolve: Permite aplicar diversas técnicas de esteganografía a las imágenes.
- Zsteg: Es una herramienta de análisis para imágenes PNG/BMP .
- LSB-Steganography: Es un programa de Python que permite esteganografiar archivos en imágenes utilizando el bit menos significativo .
- StegSpy: Es una herramienta que comprueba esquemas esteganográficos clásicos.
- StegSnow: Es un programa que oculta mensajes en archivos de texto añadiendo tabulaciones y espacios al final de las líneas .
- Binwalk: Es una herramienta de análisis de firmware .
- Stego-Toolkit: Es un kit de herramientas de esteganografía .
- StegDetect: Realiza pruebas estadísticas para determinar si se utilizó una herramienta estego.
- StegoVeritas: Es otra herramienta de esteganografía .
- openstego

2.- Descifrar passwords: JohnRipper

- john --test

- A) BUSCAR FUERZA BRUTA
- john password.txt

- john --show password.txt

- B) BUSCAR POR DICCIONARIO
- CREAR password.lst

- john --wordlist=passwords.lst password.txt

- john --show password.txt

- EJEMPLO: **Rockyou.txt , Kaonashi.txt**

Descifrar : JohnRipper

- C) ZIP

- # ./zip2john /tmp/secret.zip > /tmp/secret.hash
- # cat /tmp/secret.hash

- OTROS ??

- office2john

3.- Metadatos

- EsiffTool
- Gestiona y permite ver metadatos….

- https://exiftool.org/

- FOCA
- https://cybersecuritycloud.telefonicatech.com/innovacion-labs/tecnologias-innovacion/foca

¿Qué es Encoding?

- **Encoding data, o codificar datos, es un proceso que consiste (simplemente) en cambiar el formato de los datos.**
- Encoding es un proceso reversible.
- Los datos pueden ser codificados (encoded) a un nuevo formato, y decodificados (decoded) a su formato original.
- Como es fácilmente reversible, encoding no debe usarse para proteger datos.
- Por el contrario, estos algoritmos suelen ser públicos, para que todos puedan codificar y decodificar fácilmente.

- **¿En qué casos se usa?**

- Generalmente para comunicar datos entre sistemas y aplicaciones, usando un formato más conveniente.

- Ejemplos de encoding: ASCII, URL Encoding, Base64.

¿Qué es Encryption?

- Encryption, o encriptación, es un proceso más seguro para proteger datos:
- De tal manera que sólo los **usuarios autorizados** (con una clave o contraseña) puedan desencriptar (decrypt) el resultado y acceder al contenido original.
- Debido a que codificar (encoding) es un término más general:
- Muchas veces se dice que encriptar consiste en una "codificación segura".
- Sin embargo, lo adecuado es ser precisos y distinguir encryption de encoding.
- **Tenemos 2 tipos de encriptación**: con clave simétrica, y con clave pública.
- Con clave simétrica, significa que la misma contraseña es usada para encriptar y desencriptar datos.
- Con clave de encriptación pública, una otra contraseña distinta es usada para desencriptar.
- **Ejemplos de encryption**: AES 256, Blowfish.
- AES significa Advanced Encryption Standard, y usa una clave simétrica.
- El nombre indica que se usa una clave de 256 bits.
- Es decir, hay 2 elevado a la 256 posibles claves que pueden ser usadas.

¿Qué es Hashing?

- Hashing es un proceso unidireccional, donde los datos se transforman a un string alfanumérico, con una longitud fija de caracteres.

- El string resultante se conoce como hash.
- Este hash no se puede revertir, ya que se trata de una operación en un solo sentido.
- Hashing se usa generalmente para verificar la integridad de los datos.
- Es importante resaltar que:

- Si 2 datos idénticos son hasheados, es decir, pasan a través de la misma función hash, el resultado será el mismo.
- Para entradas diferentes, los hashes resultantes serán diferentes y únicos.
- Un buen algoritmo de hashing causará que un cambio mínimo en la entrada, produzca una salida muy diferente.
- Ejemplos de función hash: SHA-512, MD5

Para generar un HASH existen diferentes algoritmos de cifrado entre los cuales tenemos:

- **Algoritmos asimétricos**
- Son aquellos que no poseen un algoritmo reverso para descifrar su contenido original
- **MD5**
- Longitud fija: 32 caracteres

Caracteres: 0 al 9, A a la Z mayúsculas y minúsculas

- **SHA**
- Longitud fija: 40 caracteres

Caracteres: 0 al 9, A a la Z mayúsculas y minúsculas

- **Algoritmos simétricos**
- Son aquellos que una vez cifrados poseen un algoritmo inverso que puede descifrar su contenido, por ejemplo:
- **BASE64**
- Longitud: variable
  Caracteres: 0 al 9 A a la Z solo mayúsculas
  Finaliza comúnmente en un igual “=” o doble igual “==”
- **BASE32**
- Longitud: variable
  Caracteres: 2 al 7 A a la Z solo mayúsculas, no se toma en cuenta el 0 porque podría confundirse con la O mayúscula, el 1 podría confundirse con la letra I y el 8 podría confundirse con la letra B
  Finaliza comúnmente con varios símbolos de igual “====”
- **CAESAR**
- Este es uno de los primeros algoritmos que aprenden los estudiantes en clases de criptografía, y consiste en tener 2 alfabetos y un número constante que nos indica cuantas posiciones se debe mover el alfabeto

Algoritmos

- Los caracteres iniciales del /etc/shadow identifican el algoritmo:

- 1 is Message Digest 5 (MD5)
- $2a$ is blowfish
- 5 is 256-bit Secure Hash Algorithm (SHA-256)
- 6 is 512-bit Secure Hash Algorithm (SHA-512)
- y (or 7) is yescrypt
- none of the above means DES

MD5

- MD5 (algoritmo de resumen de mensajes) es un protocolo criptográfico que se usa para autenticar mensajes y verificar el contenido y las firmas digitales. El MD5 se basa en una función hash que verifica que un archivo que ha enviado coincide con el que ha recibido la persona a la que se lo ha enviado. Anteriormente, MD5 se usaba para el cifrado de datos, pero ahora se utiliza principalmente para la autenticación.
- El algoritmo de hashing MD5 convierte los datos en una cadena de 32 caracteres. Por ejemplo, la palabra «frog» siempre genera este hash: 938c2cc0dcc05f2b68c4287040cfcf71. Del mismo modo, un archivo de 1,2 GB también genera un hash con el mismo número de caracteres. Cuando le envía ese archivo a alguien, el ordenador verifica su hash para asegurarse de que coincida con el que usted envió.
- Si cambia un solo bit en un archivo, independientemente de lo grande que sea el archivo, la información del hash cambiará completa e irreversiblemente. Nada, salvo una copia exacta, pasará la prueba MD5.

- Un hash MD5 tiene 16 bytes. Cada hash MD5 aparenta ser 32 números y letras, pero cada dígito está en hexadecimal y representa cuatro bits. Dado que un solo carácter representa ocho bits (para formar un byte), el recuento total de bits de un hash MD5 es de 128 bits. Dos caracteres hexadecimales forman un byte, por lo que 32 caracteres hexadecimales equivalen a 16 bytes.

- El MD5 tendrá siempre la misma longitud: un hash de 128 bits.

- La longitud del hash es 32

- Sólo se puede descifrar por diccionario

Certificado

- Un certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto.

El formato de certificados X.509 es el más común y extendido en la actualidad, , y contempla los siguientes campos:

-Versión.
-Número de serie.
-Identificador del algoritmo empleado para la firma digital.
-Nombre del certificador.
- etc ...

SEGURIDAD COMUNICACIÓNES INALAMBRICAS

Seguridad en Bluetooth

- La tecnología Bluetooth tiene un alcance de unos diez metros, por lo que se ha integrado en dispositivos de la vida cotidiana que forman parte de las redes personales (PAN) como teléfonos y relojes inteligentes.

- Los ciberatacantes que emplean estas comunicaciones suelen utilizar antes que amplían el campo de acción de la señal. Algunos de los ataques son los siguientes:

- **Bluejacking**. Consiste en el envío de spam al usuario por medio del intercambio con este de una vCard, de una nota o de un contacto.
- **Bluesnarfing**. Aprovecha las vulnerabilidades del protocolo para sustraer información del dispositivo atacado.
- **Bluebugging**. Utiliza técnicas de ingeniería social para que la victima acepte una conexión inicial para infectar el dispositivo con malware de control remoto. A partir de ahí el usuario dispondrá de acceso remoto al teléfono del usuario y podrá utilizar sus funciones.
- La adopción de algunas medidas de seguridad sencillas puede evitar los ataques. Por esta razón, deberían de formar parte de la conducta habitual de un usuario de dispositivos Bluetooh.

Seguridad en Bluetooth

- Algunas de ellas son:

- Activar bluetooh cuando sea necesario realizar algún tipo de comunicación a través de este medio y desactivarlo cuando se deje de utilizar.
- Cambiar el nombre del dispositivo para que no desvele datos personales y configurarlo para que permanezca oculto.
- No emparejar ni aceptar conexiones entrantes de dispositivos desconocidos, ya que la información podría estar infectada de software malicioso.
- Verificar periódicamente la lista de dispositivos de confianza para eliminar los que no se utilizan habitualmente.

Seguridad WIFI

- Las redes wifi utilizan una tecnología inalámbrica que realiza la conexión entre dispositivos situados en un área relativamente pequeña, como una habitación, una oficina, una casa o un edificio, a través de ondas electromagnéticas.

- Algunas de las medidas de seguridad basicas:

- **Personalizar la contraseña de acceso**: las contraseñas por defecto de algunos routers suelen ser muy vulnerables o se pueden averiguar rápidamente en Internet.
- **Cambiar el SSID**: el nombre de la red es el identificador con el que se etiqueta la red inalámbrica para que cada usuario pueda localizarla.
- **Revisar el cifrado**: la señal inalámbrica puede ser interceptada más fácilmente por una red cableada, por lo que es necesario utilizar estándares de cifrado como **WPA2**.
- **Desactivar el acceso por WPS**: el estándar WPS facilita la configuración de una red segura con WPA2 a sus usuarios.
- **Filtrar las MAC**: las direcciones MAC son establecidas por el fabricante y únicas apra cada dispositivo de la red.
- **Actualizar el firmware**: el fimware es el software que controla los circuitos de los dispositivos electrónicos.
- **Comprobar el historial de actividad**: la actividad del router puede desvelar información sobre posibles intrusiones, ya que muestra los datos de los equipos conectados, los horarios, la duración de la sesión, etc...
- **Utilizar software de auditoría**: en el mercado existen herramientas diseñadas para evaluar la seguridad de una red y detectar sus posibles vulnerabilidades. Una de las mas populares es Nmap.

WPA /

- Privacidad equivalente por cable (WEP)
- Acceso Wi-Fi protegido (WPA)
- Acceso Wi-Fi protegido 2 (WPA 2)
- Acceso Wi-Fi protegido 3 (WPA 3)

- El WEP (privacidad equivalente por cable) es el protocolo de seguridad de Wi-Fi más antiguo y común. Fue el componente de privacidad establecido en el IEEE 802.11, un conjunto de normas técnicas cuyo objetivo era proporcionar una red de área local inalámbrica (WLAN) con un nivel de seguridad comparable al de una red de área local (LAN) por cable.

- El WPA (acceso Wi-Fi protegido) es un protocolo de seguridad inalámbrica lanzado en 2003 para solucionar las crecientes vulnerabilidades de su predecesor, WEP. El protocolo Wi-Fi WPA es más seguro que el WEP, porque usa una clave de 256 bits para el cifrado, lo que supone una gran mejora respecto a las claves de 64 y 128 bits que usa el sistema WEP.

- El WPA también usa el Protocolo de integridad de clave temporal (TKIP), que genera de forma dinámica una nueva clave para cada paquete o unidad de datos. El TKIP es mucho más seguro que el sistema de clave fija que usa WEP.

- Aun así, el WPA no está exento de defectos. El TKIP, el componente principal de WPA, se diseñó para implementarse en los sistemas con WEP a través de actualizaciones de firmware. Esto hizo que el WPA siguiera basándose en elementos fácilmente explotables.

WPA2

- introdujo el sistema de cifrado avanzado (AES) para sustituir al sistema TKIP, más vulnerable.
- WPA2 requiere más potencia de procesamiento para proteger la red.
- Clave de 256 bits para el cifrado

NFC

- *Near Field Communication*
- El NFC establece conexiones empleando ondas de radio en la **frecuencia de 13,56MHz** y puede transferir datos a una velocidad aproximada de 420 kbit/s.