Universidad Politécnica de Cartagena

Escuela Técnica Superior de Ingeniería de Telecomunicación

SEGURIDAD EN REDES

Práctica 3: Usos cotidianos de la criptografía (II):

Técnicas esteganográficas
Verificación de un hash
Generación de contraseñas seguras
Acceso a portales con certificado digital
Escaneo de puertos TCP/UDP

Autores: Josemaría Malgosa Sanahuja
María Dolores Cano Baños

SEGURIDAD EN REDES

Usos cotidianos de la criptografía PRÁCTICA 3 (segunda parte)

TÉCNICAS ESTEGANOGRÁFICAS

1. Describir sucintamente- pero con detalle- en qué consiste la Esteganografía

trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

2. Conectarse al portal de la asignatura y descargarse los ficheros monalisa_orig.jpg, miro_orig.jpg y blanco_orig.jpg. Crear un archivo de texto denominado supersecreto.txt que contenga la siguiente frase "*te juro por snoopy que este cuadro lo he pintado yo*". Utilizando el programa *steghide*, insertar en el archivo *monalisa_orig.jpg* el archivo *supersecreto.txt* (llamar a la imagen resultante *monalisa.jpg*)

```
alumno@localhost:~/pr3> steghide embed -cf monalisa_orig.jpg -ef supersecreto.tx
```

3. Abrir ambos ficheros con un programa para visionar imágenes (el navegador *firefox*, por ejemplo) ¿Se percibe a simple vista alguna diferencia entre las imágenes? ¿Y si se aplica la técnica esteganográfica sobre el archivo *miro_orig.jpg*? ¿Y con el archivo *blanco_orig.jpg*?

No se nota ninguna diferencia en ninguna foto

4. Eliminar el archivo *supersecreto.txt* y utilizando el programa *steghide*, recuperar dicho archivo a partir de la imagen *monalisa.jpg*

```
alumno@localhost:~/pr3> steghide extract -sf monalisa_mod.jpg
```

VERIFICACIÓN DE UN HASH

En la descarga de ficheros de Internet es habitual que se compruebe el hash asociado al fichero a descargar calculado previamente por el mismo portal de descarga con el calculado por usted mismo una vez finalizada la descarga. De esta manera, se tiene garantías de que durante la descarga, nada ni nadie ha alterado el contenido del archivo. Descargarse del portal de la asignatura el archivo Actas_Jitel_2009.pdf

5. Verificar que la suma de comprobación MD5 es 3836db5b5ce70c8b724ef9d20f9a31e1

```
alumno@localhost:~/pr3> md5sum Actas_Jitel_2009.pdf
3836db5b5ce70c8b724ef9d20f9a31e1  Actas_Jitel_2009.pdf
```

6. Verificar que la suma de comprobación SHA1 es 2af93f0b396d3993b547b083863f7dfb467673fc

```
alumno@localhost:~/pr3> sha1sum Actas_Jitel_2009.pdf
2af93f0b396d3993b547b083863f7dfb467673fc  Actas_Jitel_2009.pdf
```

GENERACIÓN DE CONTRASEÑAS SEGURAS

7. Describa el funcionamiento del comando *pwgen* e indique distintas formas de ejecutarlo atendiendo a las necesidades de seguridad de los siguientes escenarios:

   (a) Contraseñas de los equipos del hogar (ordenador, tablet, smart-phone, etc)
   (b) Contraseñas de servicios de internet (correo electrónico, facebook, twiter, etc.)
   (c) Contraseñas de los servidores en red

8. Describir un método para generar contraseñas seguras y simultáneamente fáciles de recordar

A través de una frase que podamos recordar, cogemos las iniciales de cada palabra y vamos convirtiendolas a numeros, caracteres...

ACCESO A PORTALES A TRAVÉS DE CERTIFICADOS DIGITALES

El certificado digital es el documento electrónico que identifica a los sujetos (personas o instituciones) en Internet mediante un mecanismo de clave asimétrica, como por ejemplo el RSA. Los certificados digitales son emitidos por una Autoridad Certificadora en la que todos confiamos (en España, la más conocida en la Fábrica Nacional de Moneda y Timbre, FNMT).

El certificado digital únicamente contiene la clave pública y debe publicitarse en Internet haciéndolo accesible a cualquier internauta (utilizando para ello repositorios especialmente diseñados para este propósito). Por el contrario, la clave privada asociada a dicho certificado debe

almacenarse en una zona segura, accesible sólo por el propio usuario.

El formato más extendido de certificados digitales es el X.509. Los campos más importantes de un certificado X.509 son: Versión, Número de serie, ID del algoritmo, Emisor, Validez (No antes de, No después de), Información de clave pública del sujeto (algoritmo de clave pública, clave pública del sujeto), Algoritmo usado para firmar el certificado y Firma digital del certificado por parte de la Autoridad Certificadora. Los certificados X.509 se identifican a través de la extensión *crt*. A su vez, un certificado puede estar codificado en binario (DER) o en formato texto (PEM).

Las Autoridades Certificadoras acostumbran a utilizar el formato PKCS12 (p12) para remitir a un usuario la información relacionada con su certificado digital. Básicamente, el formato p12 contiene un certificado X.509 y su correspondiente clave privada, todo ello empaquetado en un único archivo. La clave privada acostumbra a ir cifrada por un algoritmo simétrico (y el usuario no puede olvidar la clave; de lo contrario, el certificado no podrá utilizarse nunca). Aunque todos los navegadores reconocen el formato p12, el certificado X.509 sigue siendo necesario para poder publicitar tu identidad en Internet.

9. Si dispone de un certificado digital auténtico (por ejemplo, uno emitido por la FNMT), impórtelo dentro del navegador *firefox*. Acceda al portal de la DGT mediante su certificado digital y compruebe la cantidad de puntos que dispone su carnet de conducir. Acceda también al Aula Virtual de la UPCT mediante el certificado digital

   Para contestar a las siguientes preguntas si no dispone de un certificado digital, puede descargarse uno -emitido por el profesor de la asignatura- que está disponible en el repositorio de certificados del portal de la asignatura a través del enlace *certificado p12 del alumno desafortunado*

10. Utilizando *openssl*, extraer la clave privada del certificado p12 (llamarla *FNMTpriv.pem*)

```
alumno@localhost:~/pr3> openssl pkcs12 -in alm.p12 -out FNMTpriv.pem
```

11. Utilizando *openssl*, extraer el certificado X509 del certificado p12 (llamarlo *FNMT.crt*).. Utilizando *openssl*, visionar todos los campos del certificado

```
alumno@localhost:~/pr3> openssl pkcs12 -in alm.p12 -out FNMT.crt -nodes
```

12. Utilizando *openssl*, extraer la clave pública del certificado *FNMT.crt* (llamarla *FNMTpub.pem*).

```
alumno@localhost:~/pr3> openssl x509 -in FNMT.crt -out FNMTpum.pem
```

ESCANEO DE PUERTOS TCP/UDP ABIERTOS

13. *nmap* es un comando que permite descubrir los puertos y sus correspondientes servicios TCP/UDP que un ordenador remoto tiene abiertos (un atacante lo utilizaría para entrar en el ordenador a través de alguno de los puertos abiertos). Abrir una consola y ejecutar (y explicar el funcionamiento) de los siguientes comandos:

    nmap labit201.upct.es
    nmap -p 1-80 labit201.upct.es del puerto 1 al 80
    nmap -p 80 labit501.upct.es solo del puerto 80
    nmap -A labit201.upct.es

```
alumno@localhost:~/pr3> nmap labit201.upct.es
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-23 19:38 CET
Nmap scan report for labit201.upct.es (212.128.44.45)
Host is up (0.037s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
alumno@localhost:~/pr3> nmap -A labit201.upct.es
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-23 19:39 CET
Nmap scan report for labit201.upct.es (212.128.44.45)
Host is up (0.040s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.1 (protocol 2.0)
| ssh-hostkey:
|   1024 3d:7e:74:27:be:5a:25:82:57:f7:4e:7d:a5:20:a0:42 (DSA)
|   2048 80:cb:3c:e7:b5:c4:f0:96:7a:d3:98:46:ea:dc:8c:66 (RSA)
|_  256 6a:4d:85:83:8e:90:87:7a:18:e2:31:94:d5:fe:9b:91 (ECDSA)
80/tcp open  http    Apache httpd 2.2.29 ((Linux/SUSE))
|_http-favicon: Apache on Linux
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.29 (Linux/SUSE)
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.19 seconds
```