Hacker Highschool
SECURITY AWARENESS FOR TEENS

LECCIÓN 11
PASSWORDS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.

El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto.

El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a esponsorizarlo a través de la compra de una licencia, una donación o una esponsorización.

Índice

Contribuciones

Kim Truett, ISECOM

Chuck Truett, ISECOM

J. Agustín Zaballos, La Salle URL Barcelona

Pete Herzog, ISECOM

Jaume Abella, La Salle URL Barcelona - ISECOM

Marta Barceló, ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

11.1. Introducción

Uno de los principales personajes de la película MATRIX RELOADED es el "hacedor de llaves". El hacedor de llaves es un personaje críticamente importante, protegido por MATRIX y buscado incansablemente por Neo, porque es el encargado de fabricar y mantener las llaves que dan acceso a las diferentes zonas de MATRIX. MATRIX representa un mundo generado por ordenador y las llaves que dan acceso a las diferentes estancias son passwords o contraseñas. En la película se utilizan passwords de propósito general, passwords para las puertas traseras o back doors y passwords maestros que dan acceso a cualquier parte.

Los passwords son las llaves con las que se controla el acceso, manteniendo a los indeseables lejos de ti. En definitiva, los passwords controlan el acceso a la información (por ejemplo con los passwords en los documentos), restringen el acceso a los recursos (por ejemplo con los passwords en las páginas web) o implementan la autenticación (demostrando que tú eres quien dices ser).

11.2. Tipos de Passwords

Existen principalmente tres tipos de passwords. Los que necesitan algo que sé, los que implican algo que tengo y los que añaden algo que soy.

11.2.1. Cadenas de caracteres

En el nivel más básico, las contraseñas son cadenas de caracteres, números y símbolos. Tener acceso a un teclado proporciona un método para introducir este tipo de passwords. Las contraseñas pueden ir de las más sencillas, como los tres números para acceder a ciertas plazas de garaje, hasta las más complicadas combinaciones de caracteres, números y símbolos que se recomienda emplear para proteger la información más sensible.

11.2.2. Cadenas de caracteres más un token

En el siguiente nivel, los passwords requieren una cadena de caracteres, números y símbolos más un token o ficha de algún tipo. Un ejemplo típico es el de los cajeros automáticos. Para acceder a éstos se necesita una tarjeta y un número personal identificativo o PIN. Se consideran más robustos ya que si pierdes o olvidas alguno de los dos requerimientos tu acceso será denegado.

11.2.3. Passwords biométricos

El tercer nivel de complejidad son los passwords biométricos. Consisten en utilizar alguna característica física no reproducible, como las huellas digitales o el aspecto de la cara, para permitir el acceso. Un ejemplo es el escáner de retina en el cual el interior del ojo se fotografía para la posterior identificación del sujeto. La retina contiene un patrón único de distribución de vasos sanguíneos fácilmente apreciable y que se puede utilizar para la identificación del individuo. Los passwords biométricos son los que se consideran más sofisticados y más seguros de todos los passwords. Sin embargo, un password que se pueda transportar en el dedo o en el ojo no tiene porqué ser más seguro que uno transportado en la cabeza si el software está bien configurado.

11.3. Historia de las Contraseñas

En las versiones más antiguas de MS Excel y Word, se guardaban las contraseñas en forma de texto llano o nativo (sin ningún tipo de cifrado) en la cabecera de los documentos protegidos. Si se conseguía acceder a la cabecera del documento se podía leer la contraseña. Esto es válido para todas las versiones anteriores a Office 2000.

El sistema operativo Windows llegó a guardar las contraseñas con un formato de texto llano en un archivo oculto. En el caso de olvidar el password se podía anular simplemente borrando el archivo oculto con lo que desaparecía el password.

Pronto, Microsoft y Adobe empezaron a usar passwords, pero sólo para denotar que los documentos necesitaban de una passwords para ser abiertos, no para leer la información. Esto significaba que si el documento se abría con otra aplicación, como por ejemplo el bloc de notas (notebook) el password no era necesario y la información podía ser leída sin problemas.

Microsoft Access 2.0 podía ser abierto como un fichero de texto fácilmente, simplemente renombrando el fichero con extensión ".txt". Haciendo esto se podía leer perfectamente la información contenida en la base de datos.

Los ficheros Adobe PDF 4.0 y anteriores se podían imprimir y, muchas veces, visualizar también usando lectores PDF de Linux o el Ghostview para Windows.

Las redes inalámbricas (wireless networks) tienen un problema con la encriptación, ya que la clave de encriptación se puede calcular una vez se ha capturado un elevado volumen de la información que se transmite por el aire. Actualmente, con la capacidad de cálculo que tienen los ordenadores, cada vez se tarda menos en "crackear" los passwords.

La seguridad de los sistemas Bluetooth se considera muy fiable, una vez el sistema está configurado. El problema es que bluetooth transmite un único password entre los dispositivos para establecer la conexión y éste se envía como texto llano. Si esa contraseña es interceptada, toda transmisión futura durante esa sesión puede descifrarse fácilmente.

11.3.1. Ejercicio 1

Descárgate de Internet un fichero PDF e intenta abrirlo con otro programa que no sea el Acrobat Reader. Puedes leer correctamente la información que contiene dicho documento?

11.4. Construcción de passwords robustos

Un password robusto es aquél que:

- No puede encontrarse en un diccionario
- Contiene números, letras y símbolos
- Contiene letras mayúsculas y minúsculas
- Cuanto más largo, más robusto es

Con un password de 2 letras y 26 letras en el alfabeto, contando además con 10 números (ignorando los símbolos), hay 236 posibles combinaciones (687,000,000 posibilidades). Si aumentamos la longitud del password a 8 caracteres, ya disponemos de 836 combinaciones (324,000,000,000,000,000,000,000,000,000 posibilidades).

Hay muchos generadores de passwords robustos disponibles en Internet, pero éstos generarán un password que es casi imposible de recordar.

Intente emplear, en cambio, una cadena aparentemente aleatoria de letras o números que usted pueda recordar fácilmente.

Por ejemplo:

Ys=#1pt! (Yo soy el numero uno para ti)

ArJuAg1p (Ariadna, Juan Agustín y 1 perro – miembros de la familia)

LxRzDg24 (Alex Ruiz Diego – consonantes del nombre completo y la edad)

11.4.1. Ejercicio 1

Crea un password robusto **que puedas recordar** que obtenga una buena puntuación en la siguiente página web: http://www.securitystats.com/tools/password.php

11.4.2. Ejercicio 2

Busca en Internet 3 páginas web de bancos o cajas de ahorro y averigua el tipo de password con el que se accede a la información restringida y si recomiendan algún tipo de password o PIN (longitud, alfanumérico, DNI,…).

11.5. Cifrado de los passwords

El cifrado o encriptación de los passwords es un tópico no muy usual. Aunque es importante distinguir si hablamos de passwords encriptados o no encriptados, lo que realmente marca la diferencia es el método de encriptación que se utiliza. Esto es debido a que muchas veces, lo que nos parece un fichero encriptado es, simplemente, un fichero "codificado". Esto hace que para nosotros el fichero no sea leíble directamente, pero si que lo podríamos entender o traducir fácilmente usando un ordenador.

Además, incluso un fichero encriptado podría haber sido generado mediante una clave débil (fácil de adivinar) o un esquema de encriptación poco robusto.

Por estas razones es importante que, en el caso de encriptar cualquier tipo de información, seas consciente de que estas usando un esquema de encriptación confiable el cual ha sido probado y verificado a fondo. Por otro lado, debes asegurarte de que tu password es también un password robusto. Un buen sistema de encriptación no sirve de nada sin un buen password. Y viceversa.

11.5.1. Ejercicio 1

Hemos encriptado una serie de nombres de frutos usando un método de encriptación muy básico llamado "ROT13". Busca por Internet en que consiste este método y trata de descifrar las palabras:

a) gbzngr

b) anenawn

c) cvñn

d) cren

e) znamnan

11.5.2. Ejercicio 2

Busca algun sitio web donde puedas descifrar automáticamente estas palabras.

11.5.3. Ejercicio 3

Existen muchos sistemas de encriptación, pero realmente, muchos de ellos son simplemente sistemas de codificación. Sabes cual es la diferencia? La mayoría de nosotros seguramente no sabrá responder a esta pregunta. Realmente, la diferencia está en que los sistemas de codificación no necesitan un password para ser decodificados.

De los siguientes sistemas de encriptación, identifica cuales son realmente tipos de encriptación y cuales son esquemas de codificación.

a) Twofish

b) MIME

c) RSA

d) CAST

e) AES

f) BASE64

g) IDEA

h) TripleDES

i) ROT13

j) TLS

11.6. Password Cracking (password Recovery)

El Password Cracking o el descifrado de contraseñas para propósitos ilegales es, evidentemente, ilegal. Pero si es su propio password el que quiere descifrar, entonces estamos hablando de su información. Si de lo que se trata es de que un individuo está utilizando un password para proteger algo, y entonces se olvida de éste, se necesita una recuperación de contraseña o password recovery.

El descubrimiento de passwords consiste en seguir unas técnicas básicas:

Echar una mirada alrededor: los passwords se guardan a menudo debajo de los teclados, bajo las alfombrillas del ratón o se cuelgan en las hojas "*post-it*" personales.

La fuerza bruta: simplemente se prueban passwords de forma secuencial hasta que uno funciona.

Los ataques de diccionario automatizados: estos programas cruzan una serie de palabras pertenecientes a un diccionario hasta que una de éstas funcione como una contraseña válida.

Hay muchos programas disponibles en Internet que nos pueden ayudar con la recuperación de passwords introducidos en diferentes tipos de documentos. Sin embargo, cuanto más nueva es la versión del programa más fiable éste se vuelve y, por consiguiente, más difícil es obtener los passwords descifrados que usan, o encontrar un programa que nos ayude en la recuperación del password.

11.6.1. Ejercicio

Averigua tres tipos de programas que se suelan emplear en desarrollar documentos de todo tipo (de texto, hojas de cálculo, compresores de archivos) y que permitan la utilización de passwords para proteger el acceso a los contenidos. A continuación busca algún programa o método en Internet que facilite la recuperación de passwords de este tipo de archivos.

11.7. Protección contra el descifrado de passwords

Estas son algunas recomendaciones para evitar el descifrado de tus passwords:

1. Utiliza contraseñas robustas que no puedan extraerse con un ataque de diccionario.

2. No anuncies el password cerca del ordenador.

3. Configura el sistema para que en el caso de que se produzcan tres intentos fallidos el sistema se quede bloqueado. La contraseña debería restablecerse entonces. Esto no se aplica a documentos protegidos con password o a los archivos .zip comprimidos ya que no suelen disponer de la opción de bloqueo.

4. Cambia las contraseñas regularmente.

5. Usa una variedad suficiente de contraseñas para diferentes ordenadores. ¿Significa esto que se necesita crear una única contraseña para cada cosa? No. Se puede mantener un password maestro para las cosas sin importancia (quizás para la cuenta que le exigieron que creara para TheSIMS.com o para su cuenta en el periódico local). Pero utiliza passwords robustos para lo que realmente necesite estar seguro.

11.7.1. Ejercicio

Analizad en grupos el resto de recomendaciones que se describen en el siguiente enlace:

http://www.securitystats.com/tools/password.php

Lecturas de ampliación en Internet

http://www.password-crackers.com/pwdcrackfaq.html

http://docs.rinet.ru/LomamVse/ch10/ch10.htm

http://www.ja.net/CERT/Belgers/UNIX-password

http://www.crypticide.com/users/alecm/-security.html

http://www.securitystats.com/tools/password.php

http://www.openwall.com/john/

http://www.atstake.com/products/lc/

http://geodsoft.com/howto/password/nt_password_hashes.htm