Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 11
LE PASSWORD

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.

All works copyright ISECOM, 2004.

Informazioni sulla licenza d'uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo "non-commerciale" verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo "doposcuola".

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L'erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all'indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Contributors

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

Per la versione in lingua italiana:

Raoul Chiesa (ISECOM)

Doriano Azzena (centro CSAS del progetto Dschola IPSIA Castigliano - Asti)

Sophia Danesino (centro CSAS del progetto Dschola ITIS Peano – Torino)

Nadia Carpi (centro CSAS del progetto Dschola ITIS Peano – Torino)

Claudio Prono (@ Mediaservice.net Srl. Torino – ISECOM Authorized Training Partner)

11.0 Introduzione

Uno dei principali personaggi di "Matrix Reloaded" è il "mastro delle chiavi". Il Mastro delle chiavi ha importanza critica: è protetto da Matrix e cercato da Neo, perchè fabbrica e tiene le chiavi per i vari ambienti di Matrix. Matrix è un mondo generato da computer; le chiavi che produce sono password. Nel film ci sono password generiche, password per porte segrete e passepartout – password di qualunque genere.

Le password sono le chiavi che controllano l'accesso. Consentono l'accesso a voi e lo negano ad altri. Forniscono informazioni di controllo (password su documenti); controllano l'accesso (password su pagine web) e l'autenticazione (a patto che voi indichiate chi siete).

11.1 Tipi di Password

Esistono tre tipi principali di passwords.

11.1.1 Stringhe di Caratteri

Al livello più basso, le password sono stringhe di caratteri, numeri e simboli. L'accesso tramite tastiera consente l'inserimento di questi tre tipi di password. Queste passord variano tra la più semplice – quale i codici numerici utilizzati su qualche lucchetto – alle combinazioni di caratteri, numeri, simboli più complicati consigliate per la protezione di informazioni riservate.

11.1.2 Stringhe di Caratteri più un token

Il livello successivo è quello di richiedere una stringa di caratteri, numeri e simboli con un token di qualche tipo. Un esempio è ATM, che richiede una *carta* – il token – ed un numero di identificazione personale o PIN. Questo è considerato più sicuro, perchè in assenza di uno di questi, viene negato l'accesso.

11.1.3 Password Biometriche

Il terzo livello di password è quello di tipo biometrico. Questo utilizza caratteristiche biologiche non riproducibili, come le impronte digitali o caratteristiche del viso, per consentire l'accesso. Un esempio è la scansione della retina in cui la retina – che è la superficie interna del retro dell'occhio - viene fotografata. La retina contiene un intreccio unico di vasi sanguigni facilmente esaminabili che viene confrontato con un riferimento. Le password di tipo biometrico sono le più sofisticate e sono considerate ' più sicure', ma nella realtà una password che si 'porta' nel proprio dito o occhio non è più sicura di una password forte che si porta nella propria testa, a patto che il software che utilizza la password sia correttamente configurato.

11.2 Storia delle Password

Ecco alcune vulnerabilitànella storia delle password:

Nelle versioni più vecchie di MS Excel e Word, le password erano memorizzate in chiaro nelle informazioni di intestazione del documento. Esaminando l'intestazione era possibile leggere la password. Questo è vero per tutte le versioni precedenti a Office 2000.

Windows una volta memorizzava le password in chiaro in un file nascosto. Avevate perso la chiave? Era sufficiente cancellare il file nascosto e la password veniva cancellata.

Più recentemente, Microsoft e Adobe hanno utilizzato password per far sì che un file fosse protetto quando aperto con le loro applicazioni. Se aperto con altre applicazioni, quale il Notepad, la password non era necessaria.

Il database Microsoft Access 2.0 potrebbe essere aperto facilmente come file di testo semplicemente rinominando i file con estensione ".txt". In questo modo è possibile esaminare i dati presenti nel database.

I file Adobe PDF nelle versioni 4.0 e precedenti erano stampabili e spesso esaminabili utililizzando lettori PDF in ambiente Linux o Ghostview in ambiente Windows.

Le reti wireless hanno un problema con la crittografia poichè la chiave di crittografia può essere indovinata una volta collezionata una quantità di dati crittati sufficiente per trovarne la struttura. Con l'attuale potenza computazionale disponibile anche a casa, la chiave per trovare la password può essere ricavata quasi immediatamente.

La sicurezza di Bluetooth è considerata molto elevata, una volta installato. Il problema è che bluetooth trasmette una password unica, generata tra i dispositivi al momento di stabilire una connessione, e la ttrasmissione della password avviene in chiaro. Se viene intercettata, tutte le trasmissioni successive per quella sessione possono essere facilmente decodificate.

Esercizio

Effettuate il download di un file PDF da Internet e cercate di aprirlo con altri programmi. Come si mostra il contenuto?

11.3 Costruire una Password Forte

Le passwords migliori:

✓non possono essere trovate in un dizionario

✓contengono numeri, lettere e simboli strani in cima ai numeri

✓contengono lettere maiuscole e minuscole

✓più lunghe sono, più "forti" sono

Con una password di 2 lettere e 26 lettere nell'alfabeto, più 10 numeri (ignorando i simboli), ci sono 236 combinazioni possibili (687.000.000 possibilità). Aumentando la lunghezza della password a 8 caratteri ci sono 836 combinazioni (324.000.000.000.000.000.000.000.000.000.000 possibilità).

Ci sono molti generatori di password disponibili in internet, ma generano password che è quasi impossibile ricordare.

Cercate invece di usare una stringa di lettere o numeri apparentemente casuali che potete ricordare facilmente.

Ad esempio:

ricei3or! (Riccioli d'oro e i 3 orsetti)

GGPL2g1c (Giovanni, Giorgio, Paolo, Lucia, 2 gatti, 1 cane – i membri della vostra famiglia)

Esercizi

- Create una password forte **che voi siate in grado di ricordare** che abbia un punteggio alto nella seguente pagina web: http://www.securitystats.com/tools/password.php
- Esaminate le pagine Web di 3 diverse banche e scoprite che tipo di password è richiesta per consentire ad un titolare di conto di accedere a informazioni riservate. Queste banche forniscono raccomandazioni che spingano gli utenti a utilizzare password forti?

11.4 Crittografia delle Password

Le persone generalmente non discutono i meccanismi di crittografia delle password, perchè sembra che non ci siano opinioni da discutere - le password sono, per definizione, crittografate. Questo è generalmente vero, ma la crittografia non è una semplice scelta "si o no". La validità della crittografia, generalmente indicata come la sua *forza*, varia da debole a molto robusta.

Le password più deboli sono quelle che sono semplicemente state codificate. Questo produce una password che non è direttamente leggibile, ma, data la chiave, è possibile facilmente tradurla utilizzando un computer, carta e penna o un decodificatore di plastica trovato in una scatola di cereali. Un esempio di questo è il cifrario *ROT13*. ROT13 sostituisce ogni lettera in un testo con la lettera distante da essa 13 posizioni in ordine alfabetico. Ad esempio 'ABC' diventa 'NOP'.

Anche utilizzando algoritmi che possono essere più propriamente chiamati crittografici, la crittografia è debole, se la chiave utilizzata è debole. Utilizzando ROT13 come esempio, se si considera come chiave lo spostamento di 13, allora è una chiave estremamente debole. Si può utilizzare ROT10, sostituendo ogni lettera con quella di 10 posizioni avanti, o ROT-2, rche sostituisce ogni lettera con quella che la precede di 2 posizioni. Si può anche rafforzare la sicurezza variando il differenziale, come ROT∏, in cui la prima lettera viene spostata di 3 posizioni; la seconda di una, la terza di quattro, la quarta di una e così via; così utilizzando il numero ∏ (3.14159265...) si ottiene un differenziale che varia continuamente.

A fronte di queste possibili variazioni, quando si crittografa un qualunque tipo di informazione, si deve essere sicuri di utilizzare un metodo affidabile di crittografia e che la chiave – il vostro contributo all'operazione di crittografia – porti ad un risultato robusto.

Bisogna anche ricordare che un buon sistema di crittografia è inutile senza buone password, così come buone password sono inutili senza una buona crittografia.

Esercizi:

1.Il seguente elenco mostra una lista di frutti (in lingua inglese) codificati con il cifrario ROT13. Cercate di decodificarli:

a) nccyr

b) benatr

c) yrzba

d) jngrezryba

e) gbzngb

2. Trovate una pagina web che vi consenta di decodificare automaticamente le parole codificate con il cifrario ROT13.

3.Ci sono molti sistemi differenti che vengono chiamati crittografici, ma in realtà molti di essi sono unicamente metodi di codifica. Un vero meccanismo di crittografia richiede una password, chiamata *chiave* per poter effettuare l'operazione di cifratura e decifrazione. Dei seguenti meccanismi quali sono metodi di cifratura e qualli semplici codici?

a)Twofish

b)MIME

c)RSA

d)CAST

e)AES

f)BASE64

g)IDEA

h)TripleDES

i)ROT13

j)TLS

11.5 Password Cracking (Password Recovery)

Scoprire una password (*password cracking*) per scopi illegali è illegale. Ma se è la vostra password, allora l'informazione è di vostra proprietà. Una volta che proteggete con password qualcosa, e poi dimenticate la vostra password, siete bloccati. Di qui la necessità di recuperare la password (*password recovery*).

La scoperta di una password si basa su poche tecniche:

- "Guardarsi intorno": le passwords sono spesso scritte sul retro della tastiera, sotto i mouse o appuntate nell'agenda personale.
- Forza bruta: semplicemente si provano tutte le password fino a trovare quella giusta.
- Attacco automatico basato su dizionari: questi programmi utilizzano una serie di dizionari possibili fino a che una parola funziona da password.

Ci sono molti strumenti disponibili sul web che aiutano a recuperare una password su documenti. Tuttavia, le ultime versioni dei programmi stanno diventando sempre più sicure e quindi è sempre più difficile ottenere password utilizzando le precedenti tecniche o utilizzando software di recupero password.

Esercizio

Identificate tre diversi programmi che siano usati per sviluppare documenti (testo, fogli eletronici, archivi) e permettete l'uso di password per limitare l'accesso a questi documenti. Successivamente, utilizzando Internet, trovate le istruzioni su come recuperare le password perdute per questi files.

11.6 Protezione dal *Password Cracking*

Di seguito potete trovare alcuni suggerimenti su come evitare che le vostre password vengano scoperte.

1. Utilizzate passwords forti che non possano essere rilevate con un attacco a dizionari

2. Non segnate le vostre password vicino al vostro computer

3. Limitate a tre i tentativi di accesso errati consentiti, poi bloccate l'accesso. La password dovrà quindi essere impostata nuovamente (questo non si può applicare a documenti o file zip protetti da password poichè non hanno opzioni per bloccare l'inserimento della password)

4. Cambiate regolarmente le password.

5. Utilizzate password diverse per computer diversi. Questo significa che dovete creare una password univoca per ogni cosa? Assolutamente no. Mantenete una password principale per le cose di cui non vi importa molto (ad esempio l'account che vi è stato richiesto di creare per TheSIMS.com o per il vostro account sul giornale locale), ma utilizzate buone password per qualunque cosa debba realmente essere sicura.

Esercizio

Discutete con la classe le raccomandazioni che si trovano in

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

Letture di approfondimento

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

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

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