Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 11
WACHTWOORDEN

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Informatie over de “Gebruiksvoorwaarden”

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Inhoudsopgave

Auteurs

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

Translation by Raoul Teeuwen

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

11.0 Introductie

Een van de belangrijkste karakters in de film The Matrix Reloaded is de Keymaker. De Keymaker wordt beschermd door de Matrix en gezocht door Neo, omdat hij de sleutels maakt en beheert tot de diverse onderdelen van de Matrix. De Matrix is een computer gegenereerde wereld;
de sleutels die de Keymaker maakt zijn wachtwoorden. In de film heeft hij algemene wachtwoorden, achterdeur-wachtwoorden en hoofdsleutels – wachtwoorden waarmee je overal binnen komt.
Wachtwoorden zijn sleutels die bepalen of je ergens toegang toe hebt. Ze laten je binnen en houden anderen buiten. Je kunt er informatie mee beschermen (wachtwoorden op documenten); toegangscontrole mee uitvoeren (wachtwoorden op webpagina's)
en authenticatie mee regelen (je laat ermee zien dat je bent wie je zegt te zijn).

11.1 Soorten wachtwoorden

Er zijn drie 'hoofd-'soorten wachtwoorden.

11.1.1 Reeks van tekens

In de simpelste vorm zijn wachtwoorden een combinatie van tekens: letters, cijfers en andere karakters zoals je die aantreft op een toetsenbord. Toegang tot een toetsenbord is voldoende om zulke wachtwoorden te gebruiken. Dit soort wachtwoorden varieren van heel simpele codes van 3 tekens om een garage of deur te openen tot de meer complexe combinatie van tekens om zeer vertrouwelijke informatie te beschermen.

11.1.2 Reeks van tekens met een bezit

Het volgende niveau van wachtwoord-bescherming is dat naast een reeks van tekens (kennis) ook 'iets' fysieks in bezit moet zijn. Een voorbeeld hiervan is een geldautomaat: je hebt moet zowel een bank-kaart hebben als de bijbehorende pincode weten. Dit wordt gezien als een betere vorm van beveiliging omdat, als je 1 van de 2 niet hebt, je geen toegang krijgt.

11.1.3 Biometrische wachtwoorden

Het derde niveau in wachtwoordbescherming is het biometrische wachtwoord. Dit is het gebruik van niet te kopieeren biologische kenmerken zoals vingerafdrukken of gezichtskenmerken. Een voorbeeld is de iris-scanner, waarbij de retina – dat is de achterwand van de binnenkant van je oog – gefotografeerd wordt. De retina bevat en uniek bloedvatenpatroon die makkelijk te zien is en je kunt vergelijken met een eerder vastgelegd patroon. Biometrische wachtwoorden zijn de meest geavanceerde vorm van toegangscontrole die worden gezien als meest veilig, maar in de praktijk is een wachtwoord gebaseerd op je vinger of oog niet veiliger dan een sterk wachtwoord dat je onthoudt, er van uitgaande dat de software dat je wachtwoord afhandelt goed werkt.

11.2 Geschiedenis van wachtwoorden

Een weetje uit de wachtwoorden-geschiedenis:
In oudere versies van MS Excel en Word werden wachtwoorden als platte tekst (plain text) opgeslagen in de header van de documenten. Bekeek je de header, dan kon je de wachtwoorden zo zien. Dit geldt voor alle versies ouder dan Office 2000.
Windows sloeg wachtwoorden ooit op in platte tekst in een verborgen bestand. Was je je wachtwoord vergeten? Je verwijderde gewoon het verborgen bestand en het wachtwoord was gewist (gedeactivieerd).
In de begintijd gebruikte Microsoft en Adobe een wachtwoordsysteem waarbij een bestand beschermd was als je het met de bijbehorende applicatie opende: opende je het bestand met een andere applicatie, bijvoorbeeld Notepad/Kladblok, dan werd er niet om een wachtwoord gevraagd.
Microsoft Access 2.0 databases konden worden geopend als tekstbestand door ze simpelweg te hernoemen en een ".txt"-extensie te geven. Je kon dan alle informatie in de database zien.
Adobe PDF files van versie 4.0 en ouder kon je gewoon printen en vaak inzien als je ze opende met Linux PDF lezers of het programma Ghostview voor Windows.
Draadloze netwerken hebben een beveiligingsprobleem omdat de beveiligingssleutel te raden is als je genoeg beveiligde pakketten hebt verzameld. Met de computers die mensen tegenwoordig in huis hebben is die sleutel bijna direct te kraken.
Bluetooth beveiliging wordt beschouwd als heel veilig zodra het is ingesteld. Het probleem is dat bluetooth
een unieke, vers gemaakte, sleutel uitwisselt tussen de apparaten die moeten communiceren, maar dat dat wachtwoord als platte tekst wordt uitgewisseld: als dat wachtwoord wordt onderschept is dus alle volgende communicatie binnen die sessie eenvoudig te ontsleutelen.

Oefening:
Download een PDF bestand van het Internet en probeer het te openen met verschillende programma's. Kun je chocola maken van wat je ziet?

11.3 Een sterk wachtwoord samenstellen

De beste wachtwoorden:
✓ vind je niet in een woordenboek
✓ bevat cijfers, letters en speciale tekens ($#% etc)
✓ bevat gewone letters en hoofdletters
✓ hoe langer hoe beter
Met een wachtwoord van 2 tekens, 26 letters in het alfabet, plus 10 cijfers (speciale tekens even buiten beschouwing gelaten),
hebben we 236 combinaties (687,000,000 mogelijkheden). Verleng je het wachtwoord naar 8 tekens, dan zijn er 836 combinaties (324,000,000,000,000,000,000,000,000,000 mogelijkheden).
Er zijn verschillende wachtwoord-generatoren te vinden op het internet, maar die genereren wachtwoorden die niet makkelijk te onthouden zijn.
Je kunt beter een ogenschijnlijk willekeurige reeks tekens gebruiken die je makkelijk kunt onthouden.
Twee voorbeelden:
- dwend7g! (de wolf en de 7 geitjes!)
- PJEY2k1h (Paul, Jan, Emma, Yvonne, 2 katten, 1 hond – de samenstelling van je gezin/huishouden)

Oefeningen:

1. Bedenk een sterk wachtwoord, **dat je kunt onthouden** wat goed scoort op de volgende webpagina: http://www.securitystats.com/tools/password.php
2. Bekijk de webpagina's van 3 banken en bepaal welk wachtwoordsysteem ze gebruiken om een rekeninghouder toegang te geven tot zijn/haar gegevens. Geven de banken ook adviezen zodat gebruikers sterke wachtwoord bedenken?

11.4 Wachtwoord versleuteling

Normaalgesproken praten mensen niet over versleuteling van wachtwoorden, omdat het een onzinnige discussie lijkt – wachtwoorden zijn per definitie versleuteld. Alhoewel dit over het algemeen waar is, is versleuteling niet een simpel ja of nee. De effectiviteit van versleuteling, meestal omschreven als 'hoe *sterk* is de versleuteling', varieert van heel zwak tot uiterst robust.
Op het zwakste nivo zijn er wachtwoorden die heel simpel versleuteld zijn. Dat levert een wachtwoord dat niet makkelijk leesbaar is, maar als je de sleutel weet kunnen we hem makkelijk vertalen met behulp van een computer, pen en papier of een simpel decodeer-speeltje. Een voorbeeld is de *ROT13* versleuteling. ROT13 vervangt elke letter in een tekst met de letter die 13 posities verderop in het alfabet zit. Dus 'ABC' wordt dan 'NOP'.
Zelfs als er algoritmes worden gebruikt die je meer als versleuteling kunt beschouwen, blijft de versleuteling zwak als de sleutel zelf zwak is. Zo is ROT13 een uiterst zwak systeem. ROT13 kan sterker worden gemaakt door een andere sleutel te gebruiken. Je kunt ROT10 gebruiken, waarbij elke letter wordt vervangen door de letter 10 posities verderop in het alfabet, of ROT-2 waarbij je de letters vervangt door de letter 2 posities *eerder* in het alfabet. Het kan nog sterker door een variabel verschil te gebruiken, zoals ROTpi,
waarbij de 1ste letter 3 plaatsen verschuift; de tweede, 1 positie; de derde, 4 posities; de vierde, 1
positie; en zo verder, gebruik maken van het getal pi (3.14159265...).

Onthoud dat een goed versleutelings systeem waardeloos is als je een zwak wachtwoord gebruikt, net zoals een sterk wachtwoord weinig zin heeft als de zaak slecht versleuteld is.
Oefeningen:
1. Hieronder tref je een lijst fruit die versleuteld is met het ROT13 systeem. Probeer de lijst te ontcijferen:
a) nccry
b) fvannfnccry
c) yvzbra
d) jngrezrybra
e) gbznng
2. Zoek een website waarmee je de ROT13-gecodeerde woorden automatisch kunt decoderen.
3. Er zijn veel verschillende systemen die versleutelingssystemen (encryptiesystemen) worden genoemd, maar de meeste daarvan zijn vrij eenvoudige codeer-methodes. Echte versleuteling maakt gebruik van een wachtwoord, een zogenaamde *sleutel*,
om te coderen en decoderen. Bepaald van de volgende systemen of het gaat om echte versleutelingsmethodes of om simpele codes?
a) Twofish
b) MIME
c) RSA

d) CAST
e) AES
f) BASE64
g) IDEA
h) TripleDES
i) ROT13
j) TLS

11.5 Wachtwoorden kraken (wachtwoord achterhalen)

Wachtwoorden kraken voor illegale doeleinden is verboden. Maar als het om je eigen wachtwoord gaat, gaat het om jouw informatie. Als je iets beveiligt met een wachtwoord en daarna je wachtwoord vergeet, heb je een probleem. Dan moet je weten hoe je een wachtwoord kun achterhalen.
Wachtwoord kraken bestaat uit een aantal basis technieken
"Om je heen kijken": wachtwoorden staan soms geplakt op de onderkant van wachtwoorden, onder muismatten etc.
Brute force: gewoon wachtwoorden uitproberen tot je de goede vindt
Geautomatiseerde woordenboek aanvallen: deze programma's werken een woordenlijst af.
Er zijn tientallen programma's te vinden op internet die je helpen de wachtwoorden op documenten te achterhalen. Maar nieuwere programma's beveiligen de informatie wel steeds beter en daardoor wordt het steeds lastiger om op deze manier de wachtwoorden te achterhalen.

Exercise:

Vind drie verschillende programma's waarmee je documenten kunt maken (tekst, spreadsheets,
gecomprimeerde bestanden) en die je vervolgens kunt beveiligen met wachtwoorden. Zoek vervolgens op internet hoe je de wachtwoorden op die bestanden kunt achterhalen.

11.6 Je beveiligen tegen wachtwoord hackers

Hier zijn wat suggesties om te zorgen dat je wachtwoorden niet worden gekraakt:
1. Gebruik sterke wachtwoorden die niet te kraken zijn via een woordenboek-aanval.
2. Noteer je wachtwoorden niet in de buurt van je computer.$
3. Stel in dat er maar 3 maal een verkeerd wachtwoord ingetikt mag worden voordat het account geheel op slot springt. De enige mogelijkheid om dan binnen te komen is het resetten van het wachtwoord (door de systeembeheerder).
(dit geldt niet voor documenten en wachtwoord-beveiligde zip-files – daar kun je dit niet op instellen.)
4. Wijzig regelmatig je wachtwoord.
5. Gebruik niet overal hetzelfde wachtwoord. Betekent dat dat je voor alles een uniek wachtwoord moet hebben? Absoluut niet. Gebruik een hoofdwachtwoord dat je gebruikt voor alle informatie die niet echt belangrijk voor je is (b.v. Het wachtwoord voor een site van een online spel, of van de online krant). Maar gebruik goede wachtwoorden voor dingen die echt beveiligd moeten zijn.

Oefening:
Bespreek met je groepje de adviezen zoals je die vindt op
http://www.securitystats.com/tools/password.php

Verder lezen

http://www.password-crackers.com/pwdcrackfaq.html
http://docs.rinet.ru/LomamVse/ch10/ch10.htm
http://www.ja.net/CERT/Belgers/UNIX-password - deadlink
http://www.crypticide.com/users/alecm/-security.html - deadlink
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