

Wachtwoord kraken?

Zo doet u dat!

Een wachtwoord kraken klinkt illegaal, maar hoeft dat zeker niet te zijn. Zelfs met goed beheer raakt iedereen weleens een wachtwoord kwijt. Wij laten zien hoe u toch toegang krijgt in het geval dat u zich onverhoopt hebt buitengesloten!

Een inlogscherm heeft als doel uw identiteit te verifiëren. Daarbij geldt dat iedereen die uw wachtwoord kent, volgens de computer ook u is. Het omgekeerde geldt ook. Bent u het wachtwoord kwijt, dan bent u volgens de computer niet u en krijgt u geen toegang. Zoek dan uw toevlucht tot een andere methode, het kraken van het wachtwoord dus. Experts onderscheiden 'passive online attacks', 'active online attacks' en 'offline attacks'. Netwerkverkeer afvangen en filteren op authenticeringsinformatie is een voorbeeld van de eerste. Vaak zijn wachtwoorden wel op de computer versleuteld, maar niet als ze over het netwerk gaan. Dan zijn wachtwoorden die door de computer gebruikt worden, en onzichtbaar zijn voor de gebruiker, gewoon te achterhalen. Anders ligt dit bij een 'active online attack'. Ook daarbij wordt netwerkverkeer afvangen, maar nu het verkeer dat voor een andere computer is bestemd. Dit heeft dus al meer weg van crimineel hacken. Bij een 'offline attack', mischien wel de bekendste vorm van kraken, wordt de beoogde code apart gezet om dan in alle rust met een wachtwoordkraker te worden gesloopt. Dit kan via 'brute force', waarbij wordt geprobeerd de sleutel teken voor teken te vinden, maar het kan ook sneller middels bekende woorden en uitdrukkingen. Dit heet een 'dictionary attack'. Een variant hierop is het resetten van een wachtwoord, die dan niet wordt gekraakt, maar wordt vervangen.

WINDOWS-WACHTWOORDEN

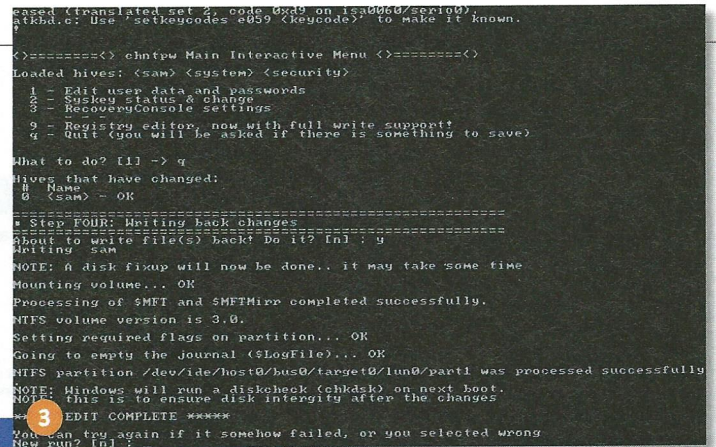
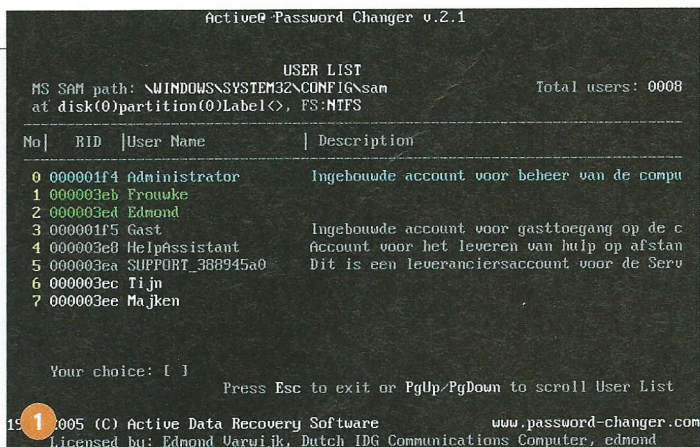
Tijdens de installatie richt Windows XP maximaal vijf gebruikersaccounts in. Deze hebben allemaal maximale rechten en zijn niet voorzien van een wachtwoord. Ook wordt een Administrator-account aangemaakt. XP Professional beveiligd dit tijdens de installatie met een wachtwoord, XP Home Edition niet. Gebruikersnamen en wachtwoorden bewaart Windows in de Security Access

L0phtCRACK

Een ander bekend programma om Windows-wachtwoorden te kraken is L0phtCrack. Dit programma maakt gebruik van brute force attacks en dictionary attacks. LC5, zoals het programma inmiddels heet, is eind 2004 overgenomen door Symantec, maker van alle Norton-producten. Symantec kon ons voor dit artikel geen LC5-versie ter beschikking stellen, en ook niet vertellen wat de toekomst van L0phtCrack is. Zie voor nadere informatie: www.atstake.com.

Manager (SAM). Dit is een deel van Windows Register, en is te vinden via \HKEY_LOCAL_MACHINE\SAM of op de harde schijf als SAM in de systeemap \Windows\System32\config. Gebruikersnamen en wachtwoorden die daarin staan, zijn niet leesbaar. Windows zet die informatie middels cryptografie om in een schijnbaar willekeurige reeks karakters. Dit is 'one-way hashing', wat wil zeggen dat het alleen mogelijk is uit een wachtwoord een sleutel te generen, maar niet omgekeerd. Bij het inloggen controleert Windows dus ook of de uitkomsten gelijk zijn en niet of het feitelijke wachtwoord klopt. Kunt u niet meer inloggen bij uw computer, dan is het veelal overbodig het wachtwoord te kraken en kunt u volstaan met een programma dat het wachtwoord vervangt of een blanco wachtwoord maakt. Omdat Windows de SAM-database volledig afschermt, kunt u alleen buiten het besturingssysteem om toegang verkrijgen tot het SAM-bestand. Windows moet daarvoor altijd worden afgesloten. Volgens Wes Miller, Product Manager van Internals Locksmith, een van de programma's die toegang kan verwerven, is directe toegang ook hét punt waar systeembeveiliging eindigt. 'Ongeacht het besturingssysteem, zodra een gebruiker di-

illustratie: SevensHeaven



recte toegang heeft tot de hardware, is alle bescherming verdwenen.'

TOEGANG KRIJGEN TOT WINDOWS

Iedereen die weleens is geweigerd bij het inloggen, bijvoorbeeld omdat de CapsLock-functie aanstond, weet hoe het voelt om geen toegang te krijgen tot zijn eigen computer. Echt fataal hoeft dit niet te zijn, gezien alle oplossingen die voorhanden zijn. Gebruikt u Windows XP Home Edition en hebt u nooit de moeite genomen het wachtwoord van de Administrator aan te passen, dan hebt u geluk. Dit wachtwoord is standaard leeg en een druk op Enter moet voldoende zijn om als Administrator in te loggen. Dit kan in Home Edition overigens alleen in Veilige Modus, waarvoor u tijdens het opstarten op F8 drukt. Andere versies van Windows maken het u niet zo makkelijk. In deze gevallen is het Administrator-account wel altijd voorzien van een wachtwoord. U ontkomt dan niet aan het inbreken in uw eigen computer. Active@ Password Changer is een DOS-programma dat Windows-wachtwoorden leegmaakt. Ook kan het een account weer inschakelen als dat is vergrendeld of een wachtwoord opgeven dat nooit zal verlopen. Het is maar een klein programma, maar de download omvat ook een bootdiskette en



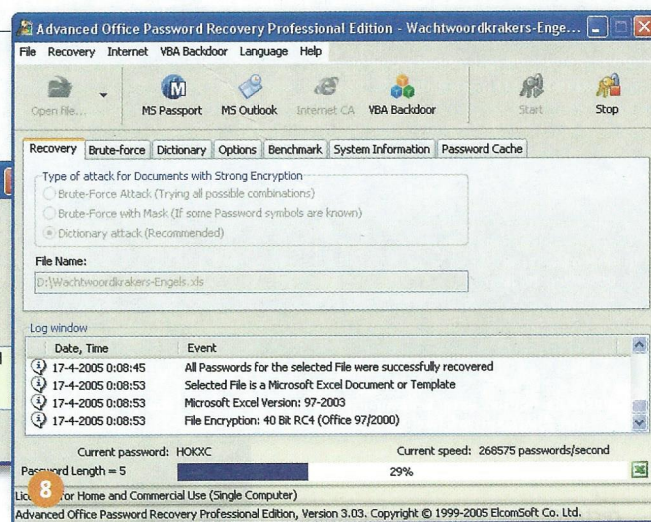
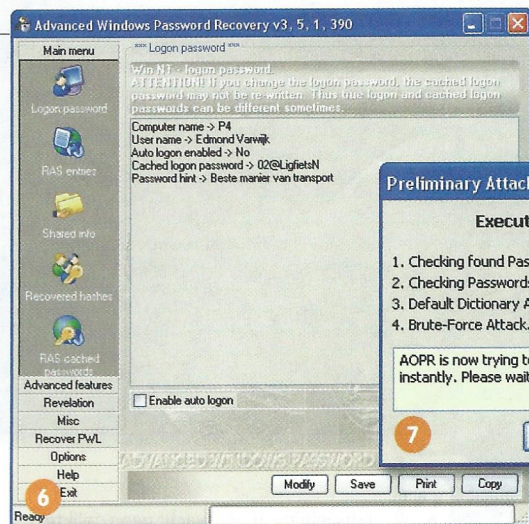
een ISO-image voor een bootable CD-ROM. Is de pc eenmaal met een van beide bootdisks gestart, dan zoekt Password Changer zelf de SAM-bestanden en zet het alle accounts in een logische volgorde met de Administrator bovenaan (afbeelding 1). Het wachtwoord wijzigen is daarna een kwestie van enkele toetsaanslagen. Vooral grafisch legt Password Changer het af tegen Locksmith van Winternals, dat onderdeel is van ERD Commander, een bekende suite van Windows-probleemoplossers. De hele suite is ook te groot voor gebruik vanaf diskette, maar een opstartbare cd-rom is met ERD Commander zo gemaakt. Locksmith is volledig wizard-gestuurd en lijkt ook erg op Windows zelf. Anders dan Active@ Password Changer, dat wachtwoorden alleen leegmaakt, vangt de Locksmith de wachtwoorden door nieuwe (afbeelding 2). Wel eist Locksmith na iedere aanpassing het rebooten van de computer, terwijl Password Changer meerdere wachtwoorden tegelijk kan resetten. Maar doorgaans hebt u zo'n tooltje alleen nodig om het Administrator-account te kraken. Als Administrator kon u eerst namelijk ook al de wachtwoorden van andere accounts wijzigen. Wilt u niet veel geld uitgeven aan een programma dat u niet zo vaak nodig hebt? Kies dan Offline NT Password & Registry Editor van Petter Nordahl. Dit is een Linux-distributie die FAT- en NTFS-partities mount, en het SAM-bestand naar het tijdelijke geheugen kopieert, wijzigt en terugschrijft

(afbeelding 3). Verwacht geen gelijke interface, maar het programma helpt u wel in vier stappen door alle tekstschermen. Wachtwoorden kunnen worden vervangen, maar de maker adviseert ze blanco te laten. Blijkbaar heeft hij zelf minder vertrouwen in zijn 'hashing' van nieuwe wachtwoorden. Vindt u het jammer een hele cd te branden voor alleen dit kleine programma, dan downloadt u de Emergency Boot CD van Mikhail Kupchik. Deze bevat nog een groot aantal andere systeemtools, maar ook de Offline NT Password & Registry Editor.

PROTECTED STORAGE, MAIL EN CHAT

De Protected Storage is een speciaal onderdeel van het Windows-register, waar wachtwoorden worden bewaard die bijvoorbeeld op websites worden gebruikt en/of in de browser automatisch worden aangevuld. Deze gegevens worden versleuteld, maar de gratis Protected Storage Password View van NirSoft leest ze voor u uit. Van dezelfde maker is MessenPass, dat wachtwoorden van verschillende chatprogramma's uitleest, en Mail Password View voor wachtwoorden van pop3- en smtp-accounts in Outlook en Outlook Express, en ook bijvoorbeeld Incremail en Thunderbird. Gebruikt u een minder bekend chat- of e-mailprogramma zoals Kellster Chatterfish, Blowsearch Messenger, TheBat of Calypso Mail, dan hebt u niets aan Mes-





senPass. In dat geval zoekt u uw toevlucht tot Advanced Instant Messengers Password Recovery en Advanced Mailbox Password Recovery van het Russische Elcomsoft (afbeelding 4). U kunt het ook eerst proberen met Mail Password Recovery, dat zichzelf als een mailrelay in uw computer nestelt. Daar wacht het af met welk wachtwoord het mailprogramma op hem af komt (afbeelding 5) nadat u het adres van de mailserver in 127.0.0.1 hebt gewijzigd. Voor ftp-accounts heeft de maker een soortgelijk programma gemaakt dat al even goed werkt.

NETWERKWACHTWOORDEN

De meeste netwerkwachtwoorden worden door Windows versleuteld opgeslagen in het Credentials-bestand in de map Documents and Settings\ <Gebruikersnaam>\Application Data\Microsoft\Credentials. Hierin staat het wachtwoord van het .NET Passport, maar ook die van netwerk- en inbelverbindingen, netwerkbronnen en ook VPN-verbindingen. Elcomsoft's Advanced Windows Password Recovery (AWPR) kan alle wachtwoorden in het Credentials-bestand voor u achterhalen (afbeelding 6). Hetzelfde geldt voor wacht-

woorden die in beeld verborgen blijven achter sterretjes. Twee losse programma's van NirSoft die ongeveer hetzelfde doen, maar net even minder uitgebreid zijn dan AWPR van Elcomsoft, zijn Network Password Recovery en Asterisk Logger. Beide zijn wel weer gratis.

WACHTWOORDEN VAN DOCUMENTEN EN ARCHIEFBESTANDEN

Wachtwoorden waarmee documenten zijn beveiligd, worden niet beheerd door Windows, maar zitten in het beveiligde document. De manier van

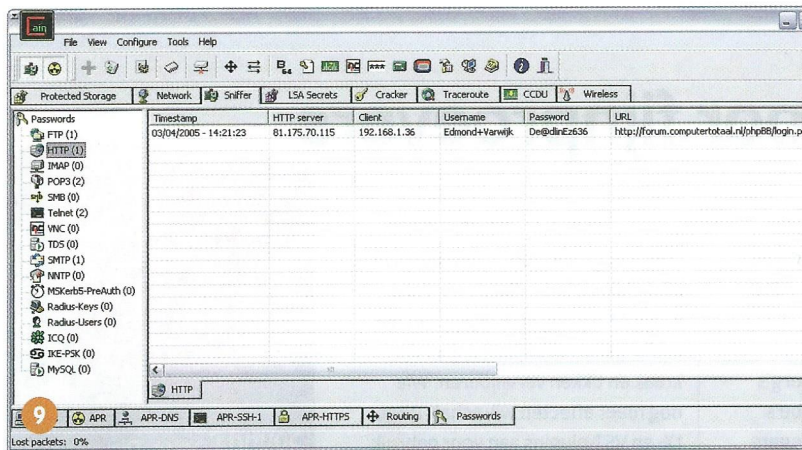
WACHTWOORDKRAKERS

Windows-inlogwachtwoorden

Product	Versie	Producent	Website (proefversie/volledige versie)	Prijs	Beperking proefversie	Grootte
Offline NT Password & Registry Editor	050303	P.Nordahl	http://home.eunet.no/~pnordahl/ntpasswd (http://home.eunet.no/~pnordahl/ntpasswd)	Gratis	Geen (freeware)	1,1MB (diskette); 3MB ISO
Emergency Boot CD-ROM Lite/Pro	0.6.1	Mikhail Kupchik	http://ebcd.pcministry.com (http://ebcd.pcministry.com)	Gratis	Geen (freeware)	5,32MB (Lite)
Password Changer Professional	2.1	LSoft	www.password-changer.com (www.password-changer.com/download.htm)	\$ 39,95	View only	1,54MB
ERD Commander (Workstation-versie)	2005	Winternals	www.winternals.com (niet beschikbaar)	\$ 149	N.v.t.	69,6MB

Windows-softwarewachtwoorden

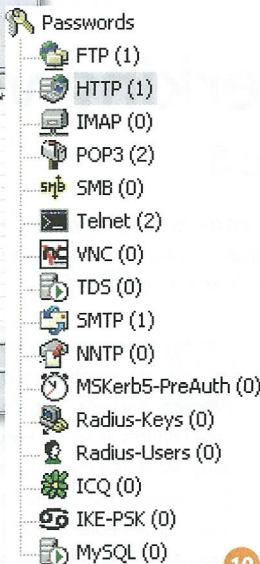
Product	Versie	Producent	Website	Prijs	Beperking proefversie	Grootte
Advanced Windows Password Recovery	3.5	Elcomsoft	www.elcomsoft.com (www.elcomsoft.com/awpr.html)	\$ 60	30 dagen en functioneel	1,84MB
Protected Storage PassView	1.62	NirSoft	www.nirsoft.com (www.nirsoft.net/utills/pspv.html)	Gratis	Geen (freeware)	28kB
Dialupass	2.43	NirSoft	www.nirsoft.com (www.nirsoft.net/utills/dialupass2.html)	Gratis	Geen (freeware)	40kB
FTP Password Recovery	1.1.0	Aleksandar Boros	www.gsmblog.com /freeware/fpr/index.htm (www.gsmblog.com/freeware/fpr/index.htm)	Gratis	Geen (freeware)	12kB
Network Password Recovery	1.0	NirSoft	www.nirsoft.com (www.nirsoft.net/utills/network_password_recovery.html)	Gratis	Geen (freeware)	78kB
Asterisk Logger	1.0.1	NirSoft	www.nirsoft.com (www.nirsoft.net/utills/astlog.html)	Gratis	Geen (freeware)	24kB
MessenPass	1.03	NirSoft	www.nirsoft.com (www.nirsoft.net/utills/mssp.html)	Gratis	Geen (freeware)	83kB
Advanced Instant Messengers Password Recovery	2.60	Elcomsoft	www.elcomsoft.com (www.elcomsoft.com/aimpr.html)	\$ 30	30 dagen en functioneel	497kB
Advanced Office Password recovery	3.03	Elcomsoft	www.elcomsoft.com (www.elcomsoft.com/aopr.html)	\$ 49 (Home Edition)	30 dagen en functioneel	3,13MB
Mail Pass View	1.31	NirSoft	www.nirsoft.com (www.nirsoft.net/utills/mailpv.html)	Gratis	Geen (freeware)	83,5kB
Mail Password Recovery	1.1.0	Aleksandar Boros	www.gsmblog.com /freeware/mpr (www.gsmblog.com/freeware/mpr/)	Gratis	Geen (freeware)	11kB
Cain & Abel	2.67	Massimiliano Montoro	www.oxid.it (www.oxid.it/cain.html)	Gratis	Geen (freeware)	4,93MB



beveiliging, verschilt enorm tussen de verschillende programma's. Lotus en WordPerfect gebruiken een eenvoudige versleuteling die bijna direct teruggeconverteerd kan worden, terwijl een programma zoals Adobe Acrobat wel het wachtwoord, maar niet het hele document versleutelt, waardoor het wachtwoord volgens Vladimir Katalov, Managing Director van ElcomSoft, toch gereset kan worden. Elcomsoft biedt voor het kraken van documenten en archiefbestanden een bijna oneindig aantal programma's. De bekendste hiervan richten zich op Office-documenten, pdf-bestanden en archiefbestanden. De werking van de verschillende programma's is grotendeels ge-

lijk, afgezien van kleine verschillen ten aanzien van specifieke bestandsformaten. Advanced Office Password Recovery kan bijvoorbeeld ook wachtwoorden van VBA-modules kraken.

Alle programma's gebruiken ook een 'dictionary attack' of 'brute force attack', die wel weken kan duren (afbeelding 7). Maar het is altijd mogelijk de recovery tijdelijk te onderbreken, zoals het ook mogelijk is de maximale systeembelasting in te stellen (afbeelding 8). Voor de dictionary attack is een cd met meer dan 20 woordenboeken, waaronder een Nederlandse, apart verkrijgbaar.



CAIN & ABEL

Cain & Abel is een combinatie van een wachtwoordkraker en een netwerkmonitor. Dit programma vangt netwerkverkeer op en filtert dit op wachtwoorden (afbeelding 9). Verder beschikt het over aanvullende gereedschappen, voor bijvoorbeeld 'dictionary attacks' en 'brute force attacks'. En u kunt de Protected Storage uitlezen, evenals de gebruikersnaam en het wachtwoord uit een configuratiebestand voor Extern Bureaublad. De download omvat zowel het eigenlijke programma als de noodzakelijke pakketdriver die nodig is voor het monitoren van het netwerkver-

keer. Wanneer u de 'Sniffer' laat meelopen bij het ophalen van e-mail en het inloggen op een website, is de werking van het programma al direct duidelijk (afbeelding 10). Open het onderdeel Sniffer en klik op het tabblad Passwords. U ziet dan de eigen wachtwoorden en gebruikersnamen die de computer over het netwerk verstuurd heeft. Voor geavanceerde mogelijkheden, zoals het afvangen

van netwerkverkeer op een geswitched netwerk en het analyseren van versleutelde protocollen zoals ssh en https, is behalve de handleiding ook bovengemiddelde netwerkkennis nodig.

CONCLUSIE

De geteste programma's maken het mogelijk verloren geraakte wachtwoorden terug te krijgen of met een blanco wachtwoord toch weer toegang te krijgen tot een document of Windows-pc. Het gemak waarmee dat soms gaat, is even bedreigend als geruststellend. Zolang u de programma's in dit artikel gebruikt om uw eigen wachtwoorden terug te vinden, zit u altijd aan de veilige kant van de soms dunne scheidslijn tussen hacker en gebruiker. ☺

WACHTWOORDKRAKERS

Windows-inlogwachtwoorden

Product	Wachtwoord-recovery van
Offline NT Password & Registry Editor	Reset gebruikersaccounts op Windows NT3.51/NT4/2000/XP/2003
Emergency Boot CD-ROM Lite/Pro	Reset gebruikersaccounts op Windows 95/98/ME/NT/2000/XP
Password Changer Professional	Reset gebruikersaccounts op Windows NT4/2000/XP/2003
ERD Commander (Workstation-versie)	Reset gebruikersaccounts op Windows NT4/2000/XP

Windows-softwarewachtwoorden

Product	Wachtwoord-recovery van
Advanced Windows Password Recovery	Login-password huidige gebruiker, .NET Passport, schermbeveiliging, RAS en netwerkverbindingen (RAS, VPN), netwerkshares, wachtwoorden achter sterretjes
Protected Storage PassView	Outlook, Outlook Express, Internet Explorer (AutoComplete), ftp-servers, MSN Explorer (Sign-up, AutoComplete)
Dialupass	Windows-netwerkverbindingen (RAS, VPN)
FTP Password Recovery	Ftp-accounts
Network Password Recovery	.NET Passport, netwerkverbindingen
Asterisk Logger	Wachtwoorden achter sterretjes
MessenPass	Chatprogramma's: MSN Messenger, Windows Messenger, Yahoo Messenger, ICQ Lite, AOL Instant Messenger, AOL Instant Messenger/Netscape 7, Trillian, Miranda, GAIM
Advanced Instant Messengers Password Recovery	Chatprogramma's: MSN Messenger, ICQ, ICQLite, AOL Instant Messenger, Yahoo! Messenger, Excite Messenger, Odigo, Trillian, AT&T IM Anywhere, T-Online Messenger, Match Messenger, Praise IM, ScreenFIRE, ACD Express Communicator, Imici Messenger, Prodigy IM, PowWow Messenger, Jabber IM, Kellster IM, PalTalk, Indiatimes messenger, Miranda, Tiscali, Ya.com Messenger, Rediff Bol, Sify Buzz, Devil, Tencent QQ, QQ (Africa Version), &RQ, Ipswitch Instant Messenger, Eighth Wonder Catx, Simple Instant Messenger, Vista IM, GAIM, Global-IM, Psi Jabber client, Messenger2, Picasa Hello
Advanced Office Password recovery	Office-documenten
Mail Pass View	E-mailaccounts: Outlook Express, Outlook 2000/XP/2003 (pop3, smtp, imap, http) IncrediMail, Eudora, Netscape, Thunderbird, Group Mail, Yahoo! Mail, Hotmail, MSN Mail, Gmail
Mail Password Recovery	E-mailaccounts: iedere client die pop3 gebruikt.
Cain & Abel	Netwerkwachtwoorden: ftp, http, imap, pop3, smb, telnet, vnc, tds, smtp, nnpt, Radius, ICQ, Ike-PSK, MySQL.