Zelf wachtwoorden kraken

Wachtwoord vergeten?

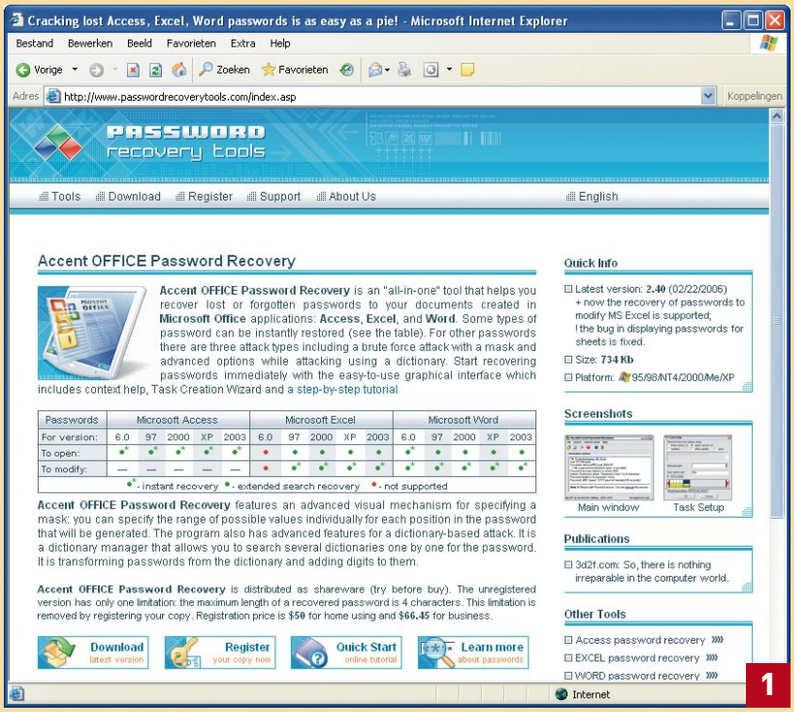
Heb je, aan de hand van ons praktisch dossier wachtwoordbeheer, al je wachtwoorden veiliger gemaakt? En gebruik je nu ook ingewikkelder wachtwoorden? Perfect... behalve als je een wachtwoord vergeten bent! Toch is niet meteen alles verloren, want sommige wachtwoorden kan je terugvinden. Clickx laat je zien hoe je je eigen wachtwoorden kraakt... FREDERICK GORDTS

Wachtwoord kwijt? Geen paniek. Als je software zoals Oubliette gebruikt, dan beschik je over een nette lijst met al je wachtwoorden. Is dat niet het geval, dan kan je nog altijd je wachtwoord terugvinden. We laten je zien welke wachtwoorden je via enkele 'achterpoortjes' kan achterhalen.

1. Office-wachtwoorden

STAP 1 / PASSWORD RECOVERY TOOLS DOWNLOADEN

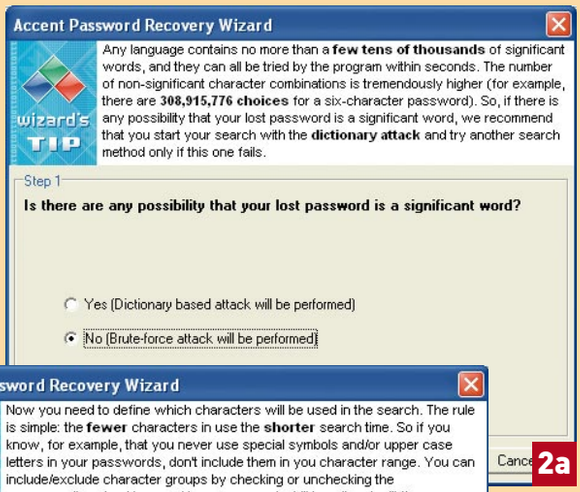
Er bestaan heel wat programma's om wachtwoorden van Office-documenten te kraken. De meeste kosten echter honderden euro's. Gratis programma's zijn er omzeggens niet, maar een goed alternatief is Password Recovery Tools (zie afbeelding 1), waarmee je gratis wachtwoorden tot 4 tekens kan 'kraken'. Registreren kost € 45. Ga naar www.passwordrecoverytools.com en klik op **Download**. Download Accent Office Password Recovery en sla het bestand ergens op, bijvoorbeeld op je bureaublad. Dubbelklik erop, en klik driemaal op **Next** en op **Install**.



1

Met Office Password Recovery kan je wachtwoorden van Office-documenten kraken.

We gaan voor een brute-force attack...



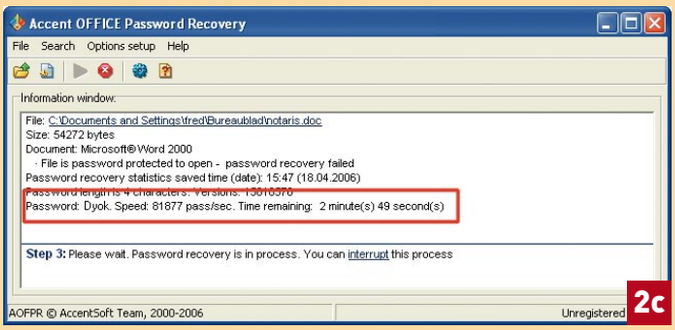
2a

2b

... en denken dat het wachtwoord uit deze tekens moet bestaan.

STAP 2 / BRUUT GEWELD GEBRUIKEN

Office Password Recovery gebruiken is erg eenvoudig: klik gewoon op het icoontje **Open a document** (het eerste icoontje) en ga op zoek naar een



Het kraken zelf gaat relatief snel.

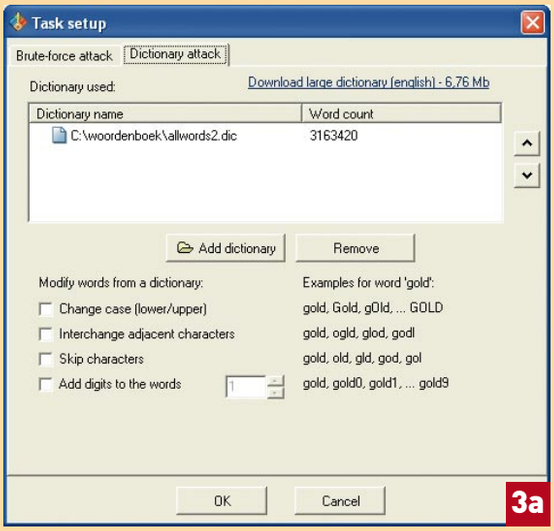
Access-, Excel- of Word-document. Bij wijze van test maakten wij een Word-document aan met een wachtwoord van vier tekens. Klik vervolgens op het derde icoontje, **Start a Search**. De wizard **Password Recovery** schiet in actie (zie afbeelding 2a). In de eerste stap duid je aan: **No (Brute-Force attack)**. Dit wil zeggen dat het programma alle mogelijke lettercombinaties zal proberen, ideaal als je denkt dat het wachtwoord geen bestaand woord is. In de tweede stap moet je een 'alfabet' kiezen. **English** is meestal goed, maar als je denkt dat het wachtwoord ook speciale tekens bevat, kies dan bijvoorbeeld **Dutch** (als er tekens zoals ë in voorkomen) of **French** (als er woorden met accenten in voorkomen, zoals é of à). Weet je nog een deel van het wachtwoord, duid dit dan in de derde stap aan. In de vierde stap moet je bepalen welke soort tekens er in het wachtwoord kunnen voorkomen: kleine letters, hoofdletters, cijfers, speciale tekens, enzovoort (zie afbeelding 2b). Hoe meer je aanvinkt, hoe langer het kraken zal duren. In stap 5, tenslotte, kies je de minimumlengte van het wachtwoord (bijvoorbeeld 1 teken). Klik op **Next** en op **Run a Search** om het zoeken te starten. De snelheid van het zoeken hangt vooral af van de processor van je computer. Op onze pc duurde het een tweetal minuten om een erg eenvoudig wachtwoord te vinden, aan een snelheid van 100.000 wachtwoorden per seconde (zie afbeelding 2c)!

STAP 3 / AANVAL MET EEN WOORDENBOEK

Een eenvoudig wachtwoord kraken, bestaande uit vier letters, duurde zo'n twee minuten. Maar als je vermoedt dat het wachtwoord een bestaand woord is, dan loont het de moeite om een zogenaamde 'dictionary attack' uit te voeren. Office Password Recovery probeert dan niet alle mogelijke letter- en cijfercombinaties uit, maar houdt zich aan

bestaande woorden. In het programma zit zo'n woordenlijst niet standaard ingebouwd, maar je kan wel makkelijk een Engelse lijst downloaden. Klik daarvoor op **Options setup**, **Tasks** en vervolgens op het tabblad **Dictionary attack**. Klik vervolgens op **Download large dictonary (English)**. Bewaar het bestand op je bureaublad, open het en pak het uit in een map, bijvoorbeeld c:\woordenboek. Klik daarna op **Add Dictionary** en ga op zoek naar het juiste bestand (zie afbeelding 3a). Je kan eventueel de opties onder de lijst met woordenboeken aanvinken, om bijvoorbeeld cijfers aan een woord toe te voegen (bijvoorbeeld **gold1**, **gold2**... **gold9** in plaats van enkel **gold**). Let op: daarmee duurt het kraken wel langer.
Ben je klaar, selecteer dan een bestand zoals in Stap 2, maar kies dit keer **Dictionary Attack**. Als het goed is, begint het kraken meteen. Alle drie miljoen Engelse woorden worden in minder dan 30 seconden doorlopen (zie afbeelding 3b)!
Je kan, via Google, ook woordenboeken in andere talen vinden. Zoek bijvoorbeeld maar eens naar **Dutch dic**. Op www.winedt.org/dict vind je alvast een heel pak talen, waaronder Nederlands. Dergelijke bestanden bevatten echter heel wat minder woorden dan het Engelse bestand van Office Password Recovery!

Voeg een woordenboek toe aan Office Password Recovery.

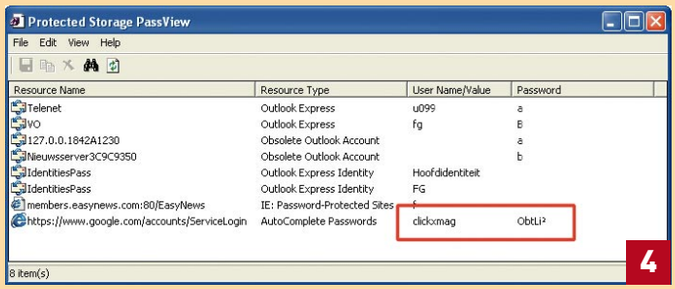


Drie miljoen Engelse woorden worden uitgeprobeerd.

2. Andere wachtwoorden

STAP 4 / WACHTWOORDEN ACHTERHALEN IN IE EN OUTLOOK

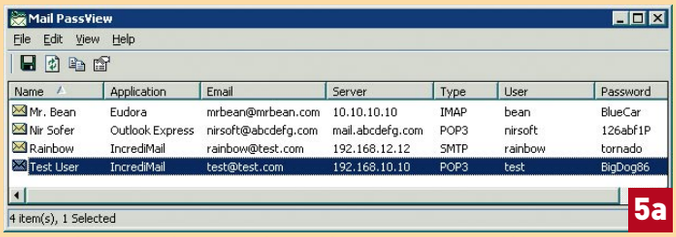
Gebruik jij ook de functie AutoAanvullen van Internet Explorer? Kies je een gebruikersnaam, dan zal Internet Explorer automatisch het wachtwoord invullen. Makkelijk, snel, en je hebt er geen apart programma voor nodig. Maar omdat het zo makkelijk is, zal je al snel het wachtwoord vergeten. Internet Explorer toont namelijk alleen maar sterretjes of bolletjes in de plaats van het wachtwoord.
Gelukkig bestaan er heel wat programmaatjes die je tonen (in het Engels 'revealen') wat er achter die bolletjes staat. Een ervan is het gratis pakket Protected Storage PassView www.nirsoft.net/utils/pspv.zip. Sla het bestand op, dubbelklik erop en pak de bestanden uit naar een map. Daarna klik je op pspv.exe en op **Uitvoeren**. Het programma toont je meteen de gebruikersnamen van websites, compleet met wachtwoorden, en ook die van je identiteiten in Outlook en Outlook Express (zie afbeelding 4)!



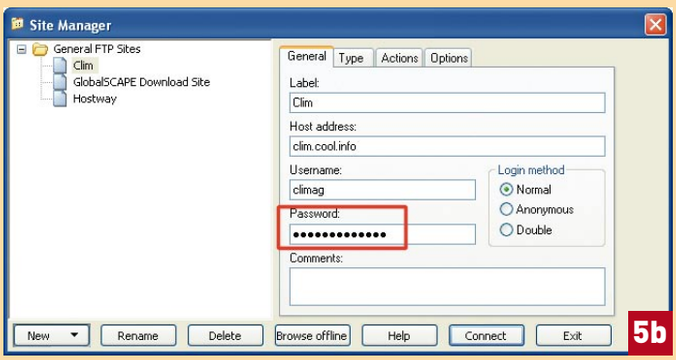
Protected Storage PassView toont je de wachtwoorden achter de 'bolletjes'.

STAP 5 / EN IN TAL VAN ANDERE PROGRAMMA'S

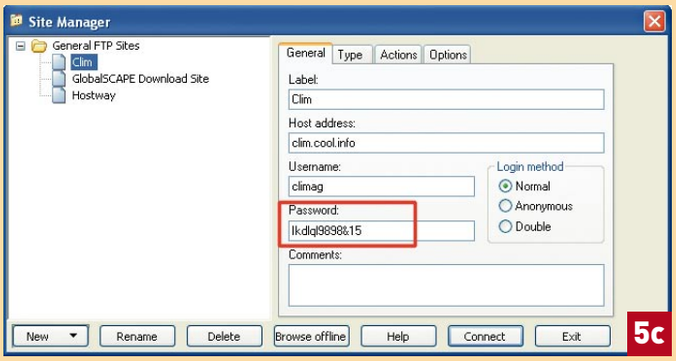
Hoewel je met Protected Storage PassView al een heel aantal wachtwoorden terug kan krijgen, zijn er toch nog programma's die wachtwoorden wel opslaan, maar ze niet laten zien. Met het programmaatje Mail PassView www.nirsoft.net/utils/mailpv_setup.exe, dat eveneens gratis is, kan je ook wachtwoorden uit programma's als IncrediMail, Eudora, Netscape en Mozilla halen (zie afbeelding 5a)!
En daar houdt het niet mee op: met het gratis MessenPass www.nirsoft.net/utils/mspass_setup.exe haal je wachtwoorden op uit MSN Messenger, ICQ, Trillian en nog een aantal andere instant messengers.
Ook erg handig is Asterisk Logger www.nirsoft.net/utils/astlog.zip, nog een gratis programmaatje dat wachtwoorden tevoorschijn tovert uit alle andere programma's die wachtwoorden in 'bolletjesvorm' laten zien, zoals je ftp-programma. Je vindt Asterisk Logger op de cd-rom bij dit nummer. Start het programma op, en je ziet het wachtwoord in Asterisk Logger én (zonder bolletjes) in het programma zelf (zie afbeelding 5b en 5c)! ♦



Met Mail PassView kan je wachtwoorden uit Netscape, Eudora en IncrediMail halen.



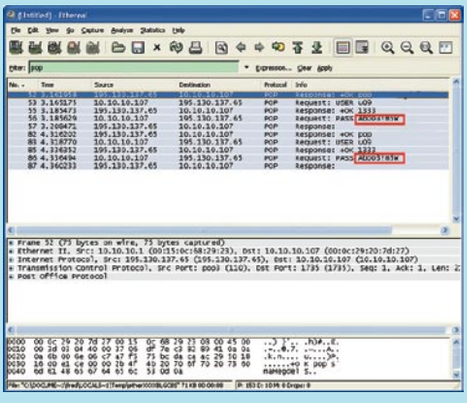
Zonder Asterisk Logger...



... en mét!

ECHT HACKEN... OP HET NETWERK

Bovenstaande methodes kan je enkel op je eigen pc gebruiken, of, in het geval van Password Recovery Tools, op bestanden die op je computer staan en waarvan je het wachtwoord vergeten bent. Maar wist je dat het meeste verkeer in een netwerk, of op internet, niet versleuteld wordt? Je kan dus zonder problemen zien wat het wachtwoord van een e-mailaccount is van een andere computer op je netwerk, met een programma als Ethereal www.ethereal.com. Het programma komt uit de Unix-wereld, maar er bestaat nu ook een redelijk gebruiksvriendelijke Windows-versie. Klik op **Download**, **Download Now** en kies de Windows-versie (12 MB). Dubbelklik vervolgens op het bestand en doorloop de wizard zonder opties te wijzigen.
Ethereal analyseert al het netwerkverkeer dat door, of langs, de netwerkkaart van je computer passeert, en soms is die trafiek niet voor jouw computer bestemd, bijvoorbeeld als je in je netwerk gebruik maakt van een hub. Zo'n hub stuurt namelijk alle pakketjes naar alle computers, en het is de computer die nagaat of een pakketje wel voor jou is. Met Ethereal kan je echter alle pakketjes 'inkijken'. Klik op **Capture Options** (het tweede icoontje), selecteer je netwerkkaart en klik vervolgens op **Capture**, **Start**. Check nu bijvoorbeeld je mail en klik op **Stop**. Je krijgt een hele lijst met ingewikkelde tekst te zien. Naast **Filter** tik je **pop** in, en je klikt op **Apply**. Als het goed is, zie je nu het wachtwoord van je mailaccount staan... of dat van je collega een computer verder!



Je wachtwoord... ontdekt door Ethereal.