HACK EENS...

EEN WINDOWS-WACHTWOORD

Als u ooit een Windows-wachtwoord heeft ingevoerd om vervolgens te ontdekken dat u het wachtwoord niet meer weet, dan bent u niet de enige. Wij laten u hier zien hoe u Windows-wachtwoorden kraakt. Ook geven we aan hoe lang u daarmee bezig bent, zodat u enige indicatie heeft van de juiste stap: kraken of opnieuw installeren?

Naast vergeten wachtwoorden is er nog een tweede belangrijke en bovenal legitieme reden om in te breken in een computer: namelijk om te kijken hoe veilig u bent als een ander om minder legale redenen wil inbreken. Ook bij deze gids willen we duidelijk stellen dat inbreken in systemen van anderen zeer onbeleefd, weinig smaakvol en mogelijk zelfs strafbaar is. Doe dat daarom niet.

Windows 9x/Me

Voor de vorm beginnen we met de antieke versies van Windows, namelijk 95, 98, 98SE en Millennium. De hack voor deze wachtwoorden was zo eenvoudig dat gebruikers van deze systemen regelmatig hun eigen computer zonder wachtwoord in gingen, zonder dat te beseffen. U klikte bij het verzoek om een wachtwoord op ANNULEREN en de computer startte door. Niet helemaal overigens, want u miste dan een paar netwerkopties. Als u op het gestarte systeem in C:\Windows het bestand <gebruikersnaam>.pwl verwijderde en herstartte, werd het wachtwoord probleemloos verwijderd. Alleen Apple-computers zijn tegenwoordig nog zo makkelijk te hacken (zie kader).

Windows XP

Inbreken op een standaard Windows XP-installatie, die niet is opgenomen in een domein, is bijna triviaal. Het eenvoudigst is Windows XP Home. Dit OS vraagt tijdens de installatie namelijk niet om een wachtwoord voor de standaard geïnstalleerde beheeraccount. Door bij het inlogscherm op Ctrl+Alt+Delete te drukken kunt u als gebruikersnaam ADMINISTRATOR invullen; laat vervolgens het wachtwoord achterwege en u krijgt toegang tot alle bestanden op het systeem. Dit werkt ook op Windows XP Professional-installaties waar de gebruiker tijdens de installatie de dialoog voor een beheerwachtwoord heeft genegeerd.

Windows XP Professional bevat de mogelijkheid om met EFS-encryptie delen van de harde schijf te beveiligen. Wie dit via Windows Verkenner inschakelt, kan eenvoudig bestanden versleutelen zonder daar tijdens een werkdag steeds weer wachtwoorden voor in te geven. EFS kraken is zeer lastig en beheerders kunnen niet zo bij de EFS-bestanden van andere beheerders. In die gevallen kunt u het wachtwoord van de machine kraken middels Ophcrack (http://ophcrack.sourceforge.net).

De gratis versie van Ophcrack heeft ongeveer vijf minuten nodig om een wachtwoord te achterhalen. Dat geldt zelfs voor sterke wachtwoorden, mits ze korter zijn dan veertien karakters. Een sterk wachtwoord van meer dan veertien karakters helpt daarom tegen normale aanvallen. Het spreekt voor zich dat dit qua gebruikersgemak niet zo praktisch is. Door wachtwoorden op deze manier te kraken, heeft EFS-encryptie geen zin. U geeft uiteindelijk het correcte wachtwoord op.

Windows Vista

Vista voegt extra beveiliging toe om triviaal kraken te voorkomen. Twee onderdelen daarvan zijn zeer belangrijk. Allereerst kunt u op een standaardinstallatie niet meer inloggen met andere gebruikersnamen door op Ctrl+Alt+Delete te drukken. Dat voorkomt dat u eenvoudig binnenkomt via een onbeveiligde beheeraccount.

Nog belangrijker is dat uw versleutelde wachtwoord in twee delen gesplitst wordt en deze delen worden in twee verschillende bestanden opgeslagen. Nu is de grap dat dit in Windows XP ook mogelijk is, maar de optie staat hier in verband met compatibiliteit uit. In Vista staat de optie aan. Het ene bestand met een deel van het wachtwoord is identiek aan de standaardplek voor Windows XP-wachtwoorden, en in theorie net zo eenvoudig te kraken, maar het tweede deel van het wachtwoord staat in een bestand dat vooralsnog niet eenvoudig te kraken is. Het resultaat is dat u op Windows Vista terug moet vallen op een brute force-aanval (zie kader 'Sterke wachtwoorden kraken').

Helaas is Vista niet onkwetsbaar. De eenvoudigste manier om binnen te komen is starten met een Linux-distributie vanaf een cd-rom of USB-stick die raad weet met NTFS. Wij gebruiken bij voorkeur Backtrack 3 (www.remote-exploit.org) dat eenvoudig te installeren is op een USB-stick met UNetBootin (http://unetbootin.sourceforge.net). Binnen Linux dient u een console te openen (de kleine monitor linksonder in beeld naast de K) om onderstaande commando's in te voeren. Let hierbij op dat Linux hoofdlettergevoelig is. Om typefouten te voorkomen en tijd

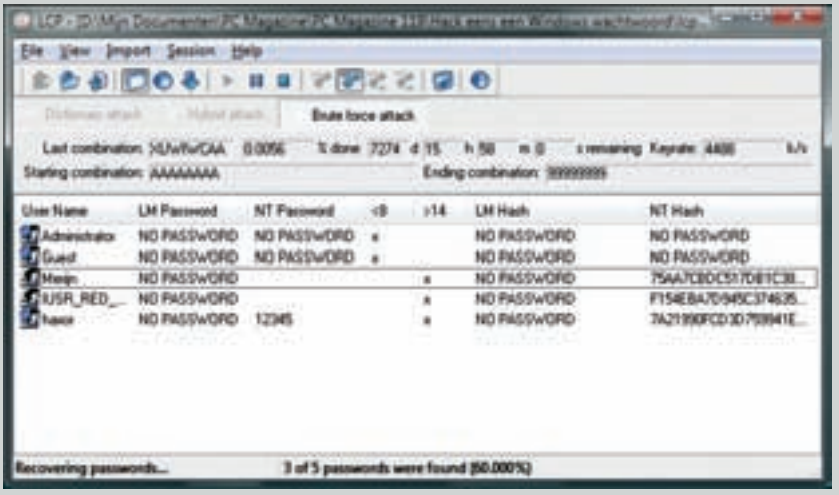
Windows-installatiemap

In de tekst gaan we ervan uit dat Windows in de standaardmap C:\Windows is geïnstalleerd. Heeft u een andere map voor Windows gebruikt, dan dient u dat natuurlijk aan te passen. Heeft u geen idee waar uw Windows-installatie geïnstalleerd is, typ dan %WINDIR% in de adresbalk van Windows Verkenner om de mapnaam te achterhalen.

Sterke wachtwoorden kraken

Sterke wachtwoorden kunt u proberen te kraken met brute kracht (brute force). Daarvoor zijn toepassingen als LCP of John the Ripper beschikbaar. Voor deze gids hebben we getest met LCP omdat het in een Windows-omgeving werkt en een grafische interface heeft. LCP voert drie aanvallen uit; allereerst probeert het gebruik te maken van een woordenboek om standaardwachtwoorden te proberen. Daarbij worden de woorden los van elkaar en in combinatie met elkaar gebruikt. Vervolgens schakelt het over naar een hybride modus. Daarin worden woorden uit het woordenboek gecombineerd met getallen en vervangen getallen delen van woorden. Wachtwoorden die uit combinaties van woorden en getallen bestaan zijn hiermee binnen redelijke tijd te kraken. Sterke wachtwoorden, die uit getallen, letters en leestekens bestaan, komen als laatste aan bod. De software probeert alle combinaties, beginnend met alle wachtwoorden van één karakter.

Werkt dit niet, dan probeert het alle combinaties uitgaande van twee karakters, enzovoort. We proberen een sterk wachtwoord van acht karakters op deze manier te kraken en helpen de software een handje door vooraf te vertellen dat het wachtwoord



Zelfs een eenvoudige brute force-aanval op een acht karakters lang wachtwoord, dat alleen uit getallen en letters bestaat, neemt bijna twintig jaar in beslag.

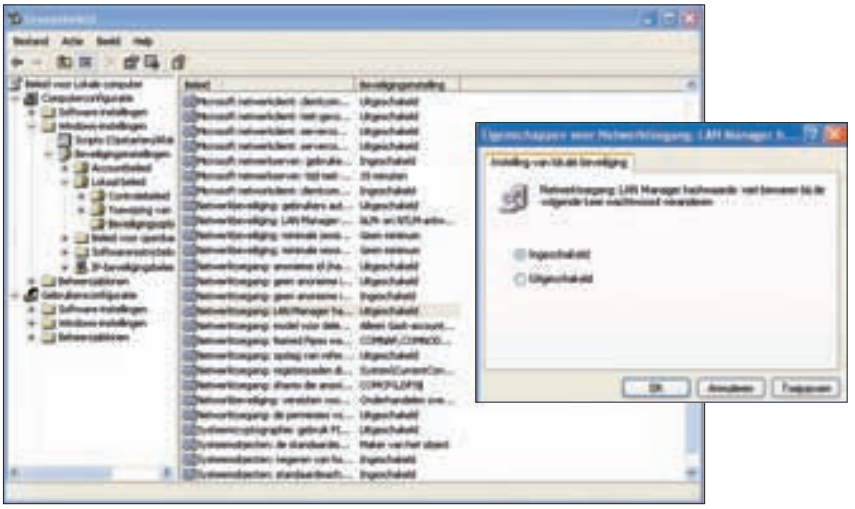
acht karakters lang is. Ons testsysteem, uitgerust met een Core 2 Duo 8200-processor en 8 GB geheugen, kan 4.500 combinaties van acht karakters per seconde proberen. Dat lijkt hoopgevend, maar acht willekeurige karakters levert, uitgaande van 82 bruikbare tekens op een toetsenbord, 2.044.140.858.654.976 (meer dan twee biljard) mogelijke wachtwoorden op. Met 4.500 wachtwoorden per seconde rekenen we daar met ons testsysteem in het slechtste geval 5.257.563 dagen op, wat neerkomt op 14.394 jaar. Dat is de reden dat bij het kraken van wachtwoorden bij voorkeur niet met brute force gewerkt wordt, maar dat de aanvallen zich richten op fouten in de gebruikte encryptiemethode. Om aan te geven hoe snel het dan kan gaan: hetzelfde wachtwoord in de Windows XP-installatie kraken we met een tool die de zwakte in de oude Windows-encryptie uitbuit in 2 minuten en 46 seconden.

te sparen, helpt het om de tabtoets in te drukken na een paar toetsaanslagen; indien mogelijk vult Linux dan zelf de tekst aan.

Aanval met opdrachtregel

Typ in de console CD /MNT/<SDA1>/WINDOWS/SYSTEM32/. Hiermee gaat u naar de bestandsmap van de Windows-installatie van het systeem dat u geladen heeft. De <>-haakjes bij SDA1 dient u achterwege te laten, maar de naam moet u mogelijk op uw systeem veranderen. Probeer in de /mnt/-bestandsmap gewoon alle mappen uit die er staan om op de juiste plaats te komen. Eenmaal verplaatst naar de System32-map typt u MV UTILMAN.EXE UTILMAN.OLD. Hiermee maakt u een back-up van Utilman.exe met als naam Utilman.old. Door op een later tijdstip hier het commando MV UTILMAN.OLD UTILMAN.EXE te typen herstelt u de installatie. Typ als laatste CP CMD.EXE UTILMAN.EXE; u maakt dan een kopie van cmd.exe, de Windows-opdrachtprompt, met als naam Utilman.exe. Herstart vervolgens de computer door SHUTDOWN -R NOW te typen. Verwijder tijdens de herstart de opstartbare USB-stick of cd-rom.

U komt nu weer bij het Windows-inlogscherm terecht. Hier kunt u naast inloggen met de aangegeven gebruikersnaam of uitschakelen/herstarten ook opties bereiken voor de toegankelijkheid van Windows. Maar met de bovenstaande commando's hebben wij de toepassing die deze opties aanbiedt, vervangen door de opdrachtregel. Als we in het inlogvenster op de Windows-toets en 'U' drukken, starten daarom niet de toegankelijkheidsopties, maar een opdrachtregel met volledige beheerrechten. Typ hier NET USER <GEBRUIKERSNAAM> <WACHTWOORD> /ADD, met een gebruikersnaam en wachtwoord naar keuze. Typ daarna NET LOCALGROUP ADMINISTRATORS <GEBRUIKERSNAAM> /ADD om die gebruikersnaam beheerrechten te geven. Herstart daarna de computer en log in met uw nieuwe beheerderaccount.



Door de netwerktoegang van de LAN Manager aan te passen, schakelt u een zwakke plek in het wachtwoordbeheer van Windows XP uit.

Binnen met limieten

U bent nu binnen in Vista en u kunt door op DOORGAAN te klikken bij UAC-MELDINGEN rondsnuffelen in de bestandsmappen van andere beheerders. Toch heeft u geen volledige vrijheid; u kunt namelijk niet bij mappen die met EFS versleuteld zijn. Wel is het mogelijk om het wachtwoord van de andere beheerder te verwijderen of te veranderen, waardoor u toegang heeft tot alle toepassingen die automatisch wachtwoorden opslaan. Daarmee komt u nog steeds niet bij de EFS-bestanden. Als u het wachtwoord verwijdert of verandert, dan worden de sleutels om de EFS-bestanden te openen namelijk door Windows gewist. Dus zelfs met deze methode heeft u geen toegang tot de versleutelde bestanden.

Professionele software om EFS-sleutels te kraken biedt eveneens geen uitkomst; deze software is bedoeld voor legitiem gebruik, bijvoorbeeld om de sleutels terug te halen van iemand die per ongeluk het wachtwoord op een andere beheeraccount gewist heeft. Ze kunnen alleen door EFS breken als u het oorspronkelijke wachtwoord opgeeft. De enige manier om door EFS te breken is daarom een brute force-aanval op het oorspronkelijke wachtwoord (zie kader).

Veilig werken

Voordat u in paniek raakt over uw veiligheid of overstapt op monsterlijke wachtwoorden van meer dan veertien willekeurige karakters, is het verstandig om eerst het risico in kaart te brengen. Voor alle bovenstaande aanvallen op uw wachtwoord is fysieke toegang tot uw machine noodzakelijk. De grootste kans dat een ander met uw computer op de loop gaat, is bij diefstal van uw computer, en dat zal meestal een notebook zijn. Een verstandige eerste stap is daarom om op een notebook voor onderweg zo min mogelijk gevoelige bestanden te zetten. Als u niet zonder kunt en de kans is groot dat u bijvoorbeeld e-mails en zakelijke documenten mee moet nemen, versleutel deze bestanden dan met behulp van EFS. Dat doet u door met de rechtermuisknop op het bestand of op een map te klikken, te kiezen voor EIGENSCHAPPEN | GEAVANCEERD en dan INHOUD VERSLEUTELEN OM GEGEVENS TE BEVEILIGEN.

Om die stap uit te voeren, heeft u Win-

Back-up en EFS

Door uw bestanden te versleutelen met EFS wordt het voor een ongewenste bezoeker heel lastig om bij uw gegevens te komen, maar er zit een addertje onder het gras. Gaat er iets mis met uw Windows-installatie, dan kunt u na een herinstallatie zelf ook niet meer bij uw versleutelde bestanden, zelfs niet als u dezelfde gebruikersnaam en wachtwoord aanmaakt. Als dit gebeurt, kunt u terugvallen op zeer prijzige reddingspakketten, maar voorkomen is beter dan genezen. Binnen Windows kunt u een reservekopie maken van uw EFS-sleutels op het moment dat u nog toegang heeft tot het systeem. Windows Vista biedt dit automatisch aan. In Windows XP is dit een stuk lastiger, maar op de ondersteuningswebsite van Microsoft kunt u in het Q241201-artikel nalezen hoe dit moet.

dows XP Professional, Vista Business of Vista Ultimate nodig. In het geval van Windows XP Professional dient u vervolgens ook nog de versleuteling van het wachtwoord sterker te maken door naar GROEPSBELEID te gaan (gpedit.msc) en hier onder COMPUTERCONFIGURATIE te kiezen voor WINDOWS-INSTELLINGEN | BEVEILIGINGSBELEID | LOKAAL BELEID | BEVEILIGINGSOPTIES. In de lijst met beschikbaar beleid klikt u vervolgens op INGESCHAKELD BIJ NETWERKBEVEILIGING: HASHWAARDE VAN LAN MANAGER NIET BEWAREN BIJ VOLGENDE WACHTWOORDWIJZIGING. Herstart daarna de computer en uw wachtwoorden worden veilig opgeslagen.

Gebruikmaken van Windows Vista in combinatie met EFS is op dit moment de beste manier om te voorkomen dat uw bestanden eenvoudig door derden te benaderen zijn. [M.G.]

Hack eens… een Mac

Alle verhalen over de vermeende veiligheid van een Mac ten spijt blijkt dat dit systeem in nog geen twee minuten te kraken is. Verbazingwekkend genoeg wordt de tool om op iedere Mac binnen te komen geleverd door Apple zelf in de vorm van de Mac Os X-installatieschijf. Als we vanaf deze schijf starten, kunnen we in het openingsvenster kiezen voor UTILITY | RESET PASSWORD. Daarna krijgen we een overzicht van de bestaande gebruikersaccounts op de machine. Kies de account waarmee u binnen wilt en selecteer RESET PASSWORD. U hoeft dan alleen een nieuw wachtwoord in te geven (geen wachtwoord ingeven is ook een optie). Vervolgens klikt u op SAVE, herstart u de machine en logt u als de nieuwe gebruiker in met uw net gegenereerde wachtwoord. Omdat u het juiste wachtwoord heeft ingegeven, krijgt u volledige toegang tot het systeem, inclusief de Keychain waarin de vorige gebruiker zijn andere wachtwoorden opslaat, waaronder de wachtwoorden om bij de versleutelde bestanden op de schijf te komen. Alleen mappen die vooraf zijn ingesteld om altijd om het wachtwoord te vragen en dit niet in de Keychain op te slaan, zijn dan nog veilig en kunnen alleen met andere middelen gekraakt worden.