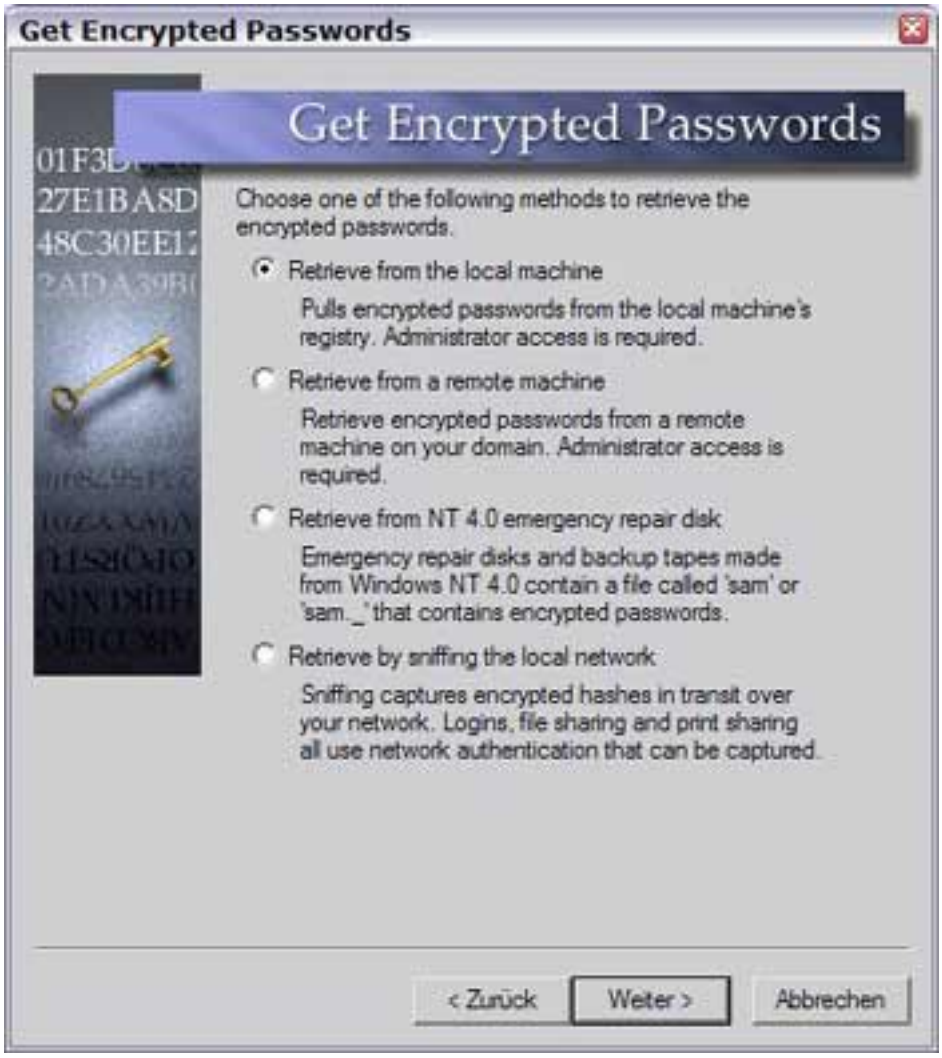
Login - Passwort für Windows vergessen?
Recover your Passwort

Mit diesem kleinen Bericht möchte ich Ihnen aufzeigen, welche Möglichkeiten Sie haben um Ihr Passwort von WindowsXP oder Windows2000 wieder zu bekommen, wenn Sie es einmal vergessen haben.
L00pht macht es möglich seinen Anmelde-Account im Computer wieder herzustellen und sich Zugang zum System zu verschaffen, auch wenn man sein Administratorpasswort vergessen haben sollte.
Windows verwendet hierfür ein verschlüsseltes Prozedere das unter Kerberos bekannt geworden ist und die Anmeldung unter Windows absichern soll.
Zuständig hierfür ist die so genannte SAM Datei, die von Windows bei der Anmeldung an einen Passwort geschützten Computer verwendet.
SAM heisst soviel wie Security Access Management und befindet sich unter Windows NT im Verzeichnis
%Systemroot%\winnt\system32\config\SAM.
Bei WindowsXP Professional hat sich etwas verändert und die Datei befindet sich hier im Verzeichnis
%Systemroot%\WINDOWS\system32\config\SAM.
Je nach Konfiguration des Systems kann es immer ein wenig variieren, da einige Installationen unter dem Dateisystem FAT32 oder NTFS gemacht werden.
Wie schon bei Windows2000 und Windows NT befindet sich die erste Datei der Installation im Verzeichnis
%Systemroot%\WINDOWS\repair\SAM.
Im Zweifelsfall verwenden Sie die Windows interne Suchfunktion und geben als Suchbegriff einfach den Dateinamen „SAM“ ein, das Ergebnis wird Sie überraschen. :-)

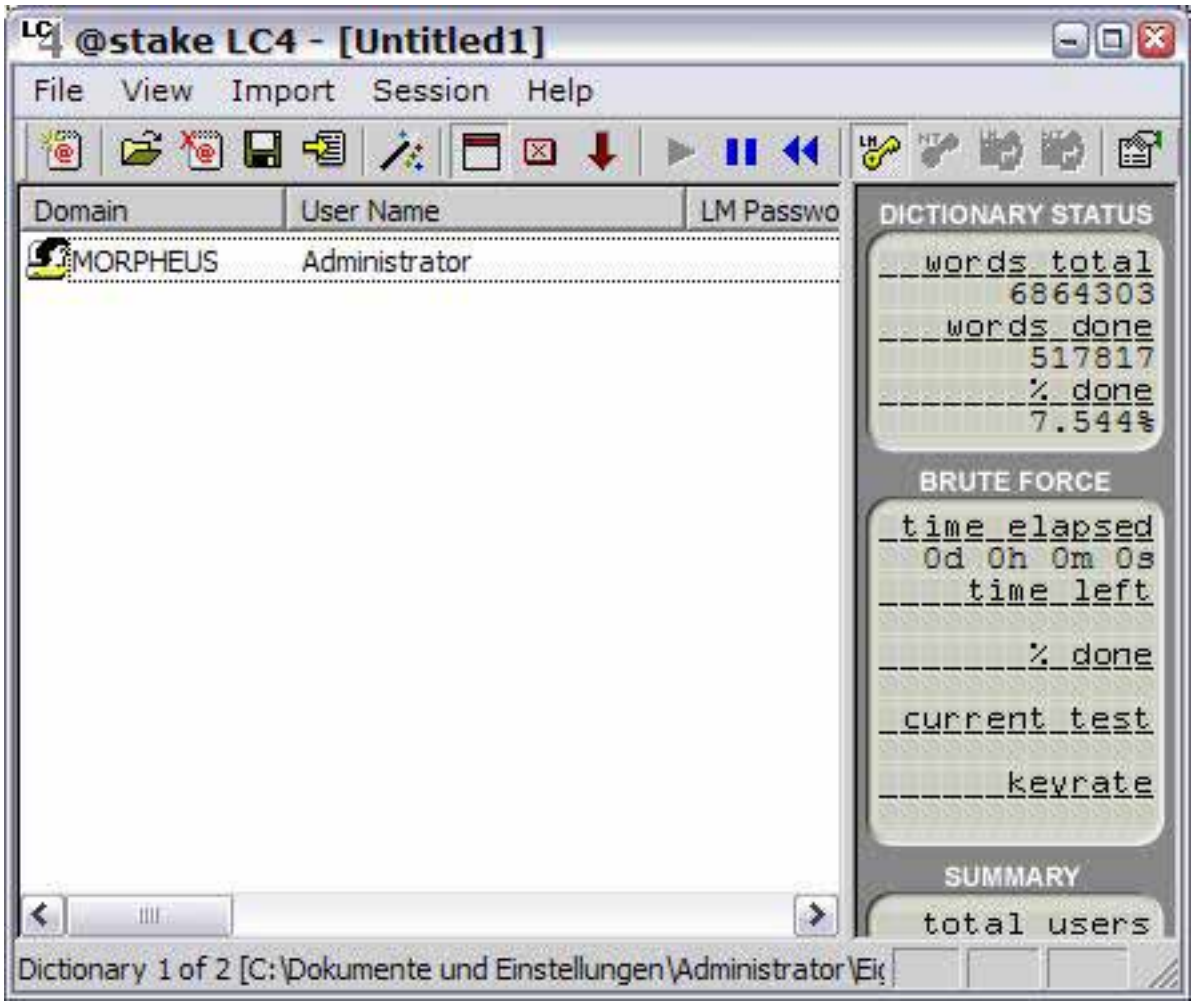
L00pht bietet nun hier einige Möglichkeiten, die SAM Datei zunächst einmal auszulesen und anschliessend per Brute Force und/oder Dictionary das Passwort wieder heraus zu finden.
Dictionary steht hier für eine *.txt Datei, die gängige Wörter und Wortkombinationen enthält. Hierbei empfehle ich jedoch, eine eigene Dictionary zu verwenden, die bereits über verschiedene Kombinationen verfügt.
Wenn Sie bereits über eine eigene Datei verfügen, dann können Sie auch eine .doc Datei verwenden, also eine Word Datei.
Nun kann man verschiedene Wege gehen, um an sein Passwort zu gelangen.

Um auf dem eigenen Rechner oder einem Rechner innerhalb eines Netzwerkes ein verlorenes Passwort wieder zu bekommen, kann man den Wizzard von LC4 verwenden, der bei Programmstart geöffnet wird und die Methoden abfragt.

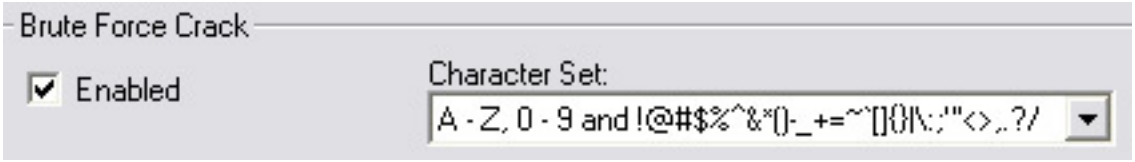


Ich möchte etwas näher auf die Möglichkeit eingehen um das entsprechende Passwort mit L00pht wieder herzustellen.
Sie benötigen 2 Disketten und das Programm sowie das Windows System auf welches sich das Passwort befindet.
Ein zweiter Computer bietet sich im Idealfall an, damit man keine wertvolle Zeit auf dem Computer verliert, dessen Passwort ja verschwunden bzw. vergessen wurde.
Am effizientesten ist es, man erstellt als erstes eine Boot Diskette für das NTFS-Dateisystem, auf die man zugreifen kann um an die SAM Datei zu kommen.
Hierzu bedient man sich eines kleinen Programmes, daß auf die Diskette für die NTFS Partition entpackt wird: ntfs20r.ace.
Mit einer erstellten Bootdiskette, die DOS 6.0 enthalten sollte sowie die ntfs20r.ace Datei, die in entpackter Form arbeiten kann.
Beide Disketten sollten Sie nun bereithalten und den Computer neu starten.
Der Computer sollte jetzt im DOS Modus von der DOS Diskette starten und Sie können den Befehl ntfsdos eingeben, um die NTFS Partition anzusteuern. (mounten)
Nun wechseln Sie auf die Festplattenpartition, auf der das Betriebssystem installiert wurde um die SAM Datei zu finden.
Da wir nun wissen in welchem Verzeichnis sich die SAM Datei befindet, können wir unmittelbar in das entsprechende Verzeichnis wechseln und die Datei suchen.
Dazu gibt man ein: *%Systemroot%\WINDOWS\system32\config* und sollte anschliessend eine Auflistung aller Dateien erhalten, die sich noch in diesem Verzeichnis befinden.
Die SAM Datei sollte nun in auf eine leere Diskette kopiert werden.
Sie müssen dazu lediglich folgenden Befehl eingeben: *copy SAM A:*
Nun haben Sie das wichtigste schon einmal geschafft, die verschlüsselte Datei haben Sie kopiert und kann nun mittels L00pht Crack ausgelesen werden.

Dazu sollte man sich L00pht installieren und ausführen, wobei die hier vorgestellte Version nur eine Testversion ist die 15 Tage funktionstüchtig arbeitet.
L00pht fordert Sie beim Start auf, den Wizard zu verwenden was man aber mit drücken der Schaltfläche Cancel beenden kann.
Anschließend öffnen Sie mit „File“ eine „New Session“ und der Bildschirm des Programmes verändert sich und wird weis.
Die SAM Datei liegt nach wie vor im Disketten Laufwerk und kann nun durch L00pht geladen werden.
Jetzt kann man auf dem Bildschirm die Benutzerkonten erkennen, die gefunden wurden.



Anschließend laden wir eine Dictionary Datei mit möglichst vielen Wörtern, um die SAM Datei damit zu kompromittieren.
Einige weitere Einstellungen sollte man ebenfalls vornehmen, damit der Erfolg nicht ausbleibt und Sie schnell Ihr Passwort wieder bekommen.
Dazu stellen Sie bei der Brute Force Möglichkeit ein Character Set ein, daß alle Kombinationen erlaubt, die somit versucht werden das Passwort zu knacken.



Sie haben alle Einstellungen erfolgreich ausgeführt und können in der Navigation auf den blauen Pfeil zum Start klicken.
Mit ein wenig Geduld und Zeit besteht eine sehr hohe Wahrscheinlichkeit, daß Sie ihr Passwort somit wieder erhalten und ordnungsgemäßen Zugriff auf Ihr System haben.

Haben Sie wieder regulären Zugriff auf das System, so können Sie alle Benutzerkonten sowie notwendige weitere Einstellungen vornehmen um sich zu schützen.
Sie erhalten L00pht unter folgender Internetadresse: http://www.atstake.com/lc4.
(Trialversion)

Was nun aber, wenn ich kein Programm wie LC4 zur Hand habe? Besteht dennoch die Möglichkeit mein Passwort wieder zu bekommen?
Ganz ohne Hilfsmittel wird man bei keiner der Möglichkeiten auskommen.
Eine weitere Möglichkeit möchte ich kurz aufzeigen, die auf Windows2000 sowie WindowsXP funktionieren dürfte.
Man benötigt hierfür das Programm John The Ripper sowie PWDump2 oder 3, um entsprechende Sicherungen und Passwortlisten abzufragen.
Handarbeit und ein wenig Verständnis für die Windowsstruktur sind nun erforderlich, da man sich mit der Komandozeile von WindowsXP/2000 bewegen sollte.
Also verwendet man "Ausführen - command.com" in Windows und das bekannte "DOS Fenster" öffnet sich.
Wechseln Sie gleich in den Ordner wo sich PWDump2 oder 3 befindet, nachdem Sie es installiert haben.
Sie können das Programm nun starten und werden eine Ausgabe der User erhalten, die sich auf dem System befinden.
Jetzt sollte man sich den String des Users heraus suchen, den man beabsichtigt wieder herzustellen, also nehmen wir einmal das Adminpasswort an: *Administrator:600: bfgd774ndhg9ssjcv4638sldlf::3847fgdbfh:mcndh* (als Beispiel)
Der String der ausgegeben wird sollte dann in eine .txt Datei gespeichert werden und irgendwo abgelegt werden, wo man sie gleich wieder finden kann.
Jetzt wird das Programm John the Ripper benötigt, um die Datei zu kompromittieren und entsprechend das Passwort zu entschlüsseln.
Dazu wird folgende Eingabe benötigt: *john.exe -i:all textdatei.txt* (wobei testdatei.txt die abgespeicherte Passwortdatei ist).
Anschliessend arbeitet John the Ripper um das Passwort zu entschlüsseln und meldet sich dann wieder, wenn das Passwort in Klartext erscheinen kann.
Je nach dem wie lang das Passwort ist, braucht das Programm auch, um es zu entschlüsseln.

Sichere Passwörter?
Für ein Passwort sollten Sie folgende Regeln beachten, was man NICHT benutzen sollte:

- eigenen Namen nicht verwenden
- Namen von unmittelbaren Familienmitglieder, Verwandten oder Freunden
- Prominente, Geburtstage, Telefonnummern
- Leichte Ziffern oder Buchstabenfolgen wie: 1234, 1357...., vfr, CFT, QAY etc.

Meine Empfehlung was besser wäre:
Achten Sie bei Passwörter darauf, daß Sie ein Sonderzeichen enthalten, daß Groß- und Kleinschreibung drin vorkommt sowie eventuell eine alphanummerische Folge.
Beispiel: 73%8=Gu4Wqµ
Achten Sie darauf, daß auf einem sensiblen System die Passwörter regelmäßig geändert werden, somit sichern Sie sich bereits einen weiteren Schritt zu Ihrer Sicherheit.

John The Ripper können Sie hier downloaden: http://www.openwall.com/john/ (Windows, Unix)
PwDump 3 kann man hier downloaden und mehr erfahren:
http://www.polivec.com/pwdump3.html

Fragen, Kritik oder Anregung: EMail

Best Regards & Greetings
M.Rogge; Brain-Pro Security // www.brain-pro.de