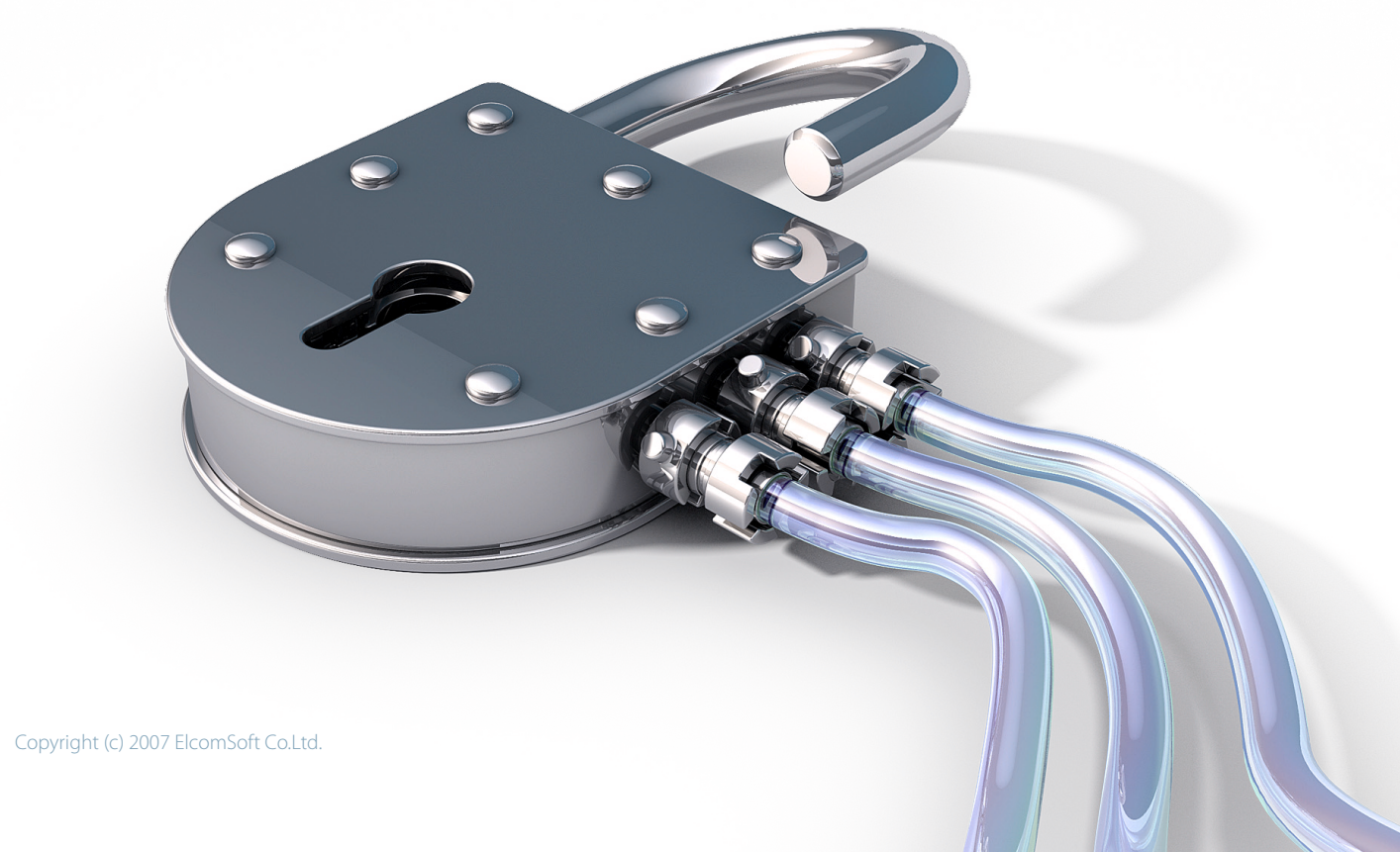
ELCOMSOFT
PROACTIVE SOFTWARE

LIEBER PROAKTIV STATT RÜCKWIRKEND

TESTEN DER PASSWORTSICHERHEIT – EIN SCHLÜSSEL ZUR SICHERHEIT DES FIRMENNETZWERKES



ELCOMSOFT
PROACTIVE SOFTWARE

INHALTE

EINFÜHRUNG

Informationsschutz bekommt heutzutage immer mehr und mehr Beachtung. Viele haben realisiert, dass deren Daten ein Schatz sind, die nicht nur entsprechend behandelt, sondern auch geschützt werden müssen. Vorbeugung und Minimieren der Risiken ist viel besser, als die Beseitigung der Konsequenzen. Diese einfache Regel gilt auch für die Informationssicherheit jedes Unternehmens.

Somit sind ein paar Dollars, die in den Schutz der Sicherheit investiert werden, nichts im Vergleich zu dem, wie viel Sie sparen werden und Verluste, die aufgrund der Hackerattacken auf Ihr Unternehmens-Netzwerk aufkommen könnten, vermeiden. Folgen von Informations-Leckstellen zu bekämpfen kostet viel mehr und kann sogar Ihr Geschäft ruinieren.

Durchschnittliche Firmen-Netzwerksicherheit ist generell auf einem niedrigen Level. In vielen Fällen genügt ein unsicheres Passwort, um das gesamte Sicherheitssystem eines Unternehmens lahm zu legen.

Dieser Artikel ist über die Risiken der Nutzung unsicherer Passwörter innerhalb eines Firmennetzwerkes, sowohl über die Wege, diese Risiken zu minimieren.

NICHT ALLE PASSWÖRTER WERDEN GLEICH ERSTELLT

Passwortschutz ist die gebräuchlichste Methode des Identifikationsnachweises, die von Windows-Betriebssystemen benutzt wird. Obwohl viele andere Methoden auf dem Markt existieren (zum Beispiel, Smartcards oder Biometrie), benutzt die Mehrheit der Arbeitsplätze die "Login-Passwort"-Kombination.

Einige Firmen verlangen nach Grundanforderungen beim Erstellen der Passwörter. Es wird "Passwort-Politik" (Politik der Passwort-Verwaltung) genannt und ist ein Teil der allgemeinen Sicherheitspolitik. Passwort-Politik wird benutzt, um Grundparameter, wie Länge, Struktur und Gültigkeitsdauer für Nutzerpasswörter zu bestimmen.

Doch im Allgemeinen haben die meisten Organisationen keine ausführliche Passwort-Politik; diese wird nicht richtig vollstreckt, weswegen die Nutzer diese ignorieren. Demnach variiert die Komplexität der Passwörter vom Fall zu Fall.

Viele Firmen wurden durch regelnde Gesetze, wie Sarbanes-Oxley (USA), HIPAA (USA), J-SOX (Japan), LSF (Frankreich) beeinflusst und führten bestimmte Regeln zum Erstellen der Passwörter ein. Diese Regeln betreffen solche Sachen, wie Passwort-Länge oder -struktur. Trotz dieser Maßnahmen sind die Passwörter nicht wirklich sicher und können einen Angriff nicht gefahrlos überstehen.

Die Mehrheit der populären Passwörter sind einfach nur Wörter, aus der Muttersprache des Nutzers abgeleitet. Manchmal können die Wörter, die als Passwörter benutzt werden, im Alltagsleben gefunden werden: Geburtsjahr, Telefonnummer, Tiername, Kreditkarten-Nummer etc. Besitzen die Eindringlinge solche Informationen, stehen die Opfer ziemlich ungeschützt da.

Das Ändern des Passwortes verbessert die Situation nicht wirklich. Ein neues Passwort kann eine leicht modifizierte Variante des vorherigen Passwortes sein oder wurde nach gleichem Prinzip erstellt (zum Beispiel, wird aus John1 Mary2). Dies ist ein Weg, wie die meisten Nutzer die Situation mit regelmäßiger Passwort-Änderung lösen, die von den Sicherheitsvorschriften vorgegeben wird.

Mehr noch – wenn in den PC eingedrungen wurde, kann ein erfahrener Eindringling zu einem 'unsichtbaren Meister' werden und den PC mithilfe der Spyware, Remote-Zugriffs-Tools etc für längere Zeit überwachen.

WIE MAN EIN UNSICHERES PASSWORT FINDET?

Zurzeit gibt es einige Grundmethoden, wie man die Passwörter mithilfe der Software findet:

1. Brute-Force-Angriff
2. Maskenattacke
3. Wörterbuch-Suche
4. Rainbow-Table-Angriff

Lasst uns einige dieser Methoden detailliert betrachten, weil es entscheidend für das Verstehen der Charakteristiken von unsicheren Passwörtern ist.

Brute-Force-Angriff

Brute-Force-Angriff ist einfach: bei der Suche nach einem Passwort probiert ein Programm jede mögliche Symbolkombination aus. Die Suche kann auf bestimmte Länge, Symboltyp (Buchstaben, Zahlen oder anderes) eingeschränkt werden, beziehungsweise auf Symbole, die als erstes ausprobiert werden müssen.

Die Zeit, die für das Herausfinden des Passwortes nötig ist, hängt von vielen Faktoren ab: Passwort-Länge, Symbolreihe und PC-Leistung, sowohl passwortgeschützter Dateityp.

Natürlich kann ein Passwort sehr schnell gefunden werden, und das Programm muss nicht alle möglichen Kombinationen ausführen. Jedoch kann diese Aufgabe Jahre dauern, falls sie auf einem Durchschnitts-PC ausgeführt wird. Sehen Sie selbst:

Passwort-Suchgeschwindigkeit für Windows-Anmeldung ist 10 Millionen Kombinationen pro Sekunde. LM-Hash – maximale Passwortlänge ist 7 Symbole (Passwortlänge ist auf 14 begrenzt, und das Passwort ist in zwei geteilt), unbeachtet der Klein- oder Großschreibung. Falls ein Passwort 7 Symbole enthält, wird die Brute-Force-Attacke 2 Stunden dauern.

NTLM-Hash braucht mehr Zeit – über 4 Tage – um ein 7-stelliges Passwort zu finden, weil die kleingeschriebenen Buchstaben benutzt werden. Falls ein Passwort 8 Symbole enthält, dauert das 'Hacking' über 8 Monate. Angriff auf die komplexeren Passwörter, wie zum Beispiel solche, die Interpunktions-Zeichen enthalten, dauert mit dem Brute-Force Jahre.

Passwortlänge ist der angemessene Schutz gegen die Brute-Force-Technologie.

Maskenattacke

Vielleicht wissen Sie noch die Länge des Passwortes oder einiger Symbole? Falls Sie Informationen über das Passwort besitzen, können Sie es mithilfe des Masken-Angriffs wiederherstellen, indem Sie die Suchreihe eingrenzen.

Falls Sie, zum Beispiel, wissen, dass das Passwort mit dem Namen "john" anfängt oder mit dem Datum "1977" endet, können Sie die Suchschablonen benutzen – "john???" und "????1977". Unbekannte Symbole - als ‚Jockerzeichen' bekannt – werden mit Fragezeichen markiert.

Maskenattacke macht Sinn: ein Programm muss weniger Kombinationen ausprobieren, so dass das Passwort in kürzerer Zeit gefunden wird. Um sich gegen den Einbruch zu schützen, vermeiden Sie Wörter und Kombinationen, die leicht von anderen Quellen abgeleitet werden können.

Wörterbuch-Suche

Eine andere Methode ist die Wörterbuch-Suche. Die Nutzer neigen oft zur Benutzung gebräuchlicher Wörter bei der Erstellung der Passwörter. Allgemein könnten es Wörter, wie "öffnen", "Zugriff" oder "Passwort" sein. Im Vergleich zu den chaotischen Kombinationen der Zeichen und Zahlen sind solche Passwörter schneller einzuprägen. Bereits fertig gestellte Wörterbücher können online gefunden oder manuell erstellt werden. In vielen Fällen enthält das Wörterbuch die populärsten Passwörter, wie admin, 1234, abc123, passwort, 12/3/75/, asdf, qwerty, aaa.

Vor dem Einbruchversuch würde der Hacker wahrscheinlich die Nutzerinformationen analysieren. Beliebige private Daten sind nutzvoll: Namen, Familiennamen, Geburtsdaten, Tiernamen etc. Einige Daten können von öffentlichen Quellen, wie Blogs, erfahren werden. Andere personelle Informationen können beim Nutzer selbst, unter verschiedenen Vorwänden, herausgefunden werden.

Diese Methode hat offensichtliche Vorteile. Die Liste der allgemeinen Wörter, die in den Passwörtern benutzt werden, ist begrenzt; sie enthaltet nie mehr als 100 000 Wörter. Das Ausprobieren von 100 000 Kombinationen ist eine leichte Aufgabe für die modernen PCs.

Um sich gegen solche Angriffe zu schützen, vermeiden Sie die Passwörter, die aus einfachen Wörtern oder Kombinationen bestehen, oder Daten, die von jemandem eingeholt werden können, der Ihre Person detailliert studiert hat.

Rainbow-Table-Angriff

Eine Methode zur Benutzung der ‚Regenbogen-Tabellen' (Rainbow-Table-Angriff) wird benutzt, um das Problem zu eliminieren. Die Grundlage dieser Methode ist die Nutzung der Vorberechnung von Passwort-Varianten für eine bestimmte Symbolreihe.

Die Idee des Ersetzens der ressourcenintensiven Berechnungen durch eine Nachschlagetabelle, die zuvor vorbereitet wurde, ist nicht neu. Nachschlagetabellen werden benutzt, wenn es leichter ist, die Daten aus dem Speicher zu extrahieren, als zu erstellen. Das einzige Manko an der Nachschlagetabelle ist deren Größe: nicht jedes Unternehmen kann sich erlauben, Terabytes von Daten zu speichern. Deswegen wurden die Rainbow-Tabellen (oder optimierte Nachschlagetabellen) ins Leben gerufen. Die Größe der Rainbow-Tabelle ist viel kleiner, als die von der Nachschlagetabelle.

Die Tabellengröße kann bei der Generierung bestimmt werden: je größer die Tabelle, desto höher ist die Wahrscheinlichkeit, das Passwort zu finden, etc. Demnach ist es in relativ kurzer Zeit möglich, Tabellen zu bekommen, mit deren Hilfe Sie schnell ein Passwort finden können.

Im Vergleich zu den einfachen Nachschlagetabellen ist die Wahrscheinlichkeit der Passwort-Wiederherstellung mithilfe des Rainbow-Angriffs niedriger als 100%, doch das Ergebnis ist es wert. So ermöglicht, zum Beispiel, der Rainbow-Angriff, der auf der Tabelle mit 7 alphanumerischen Symbolen (innerhalb einer Woche aufgebaut) basiert, die Wiederherstellung eines Passwortes mit 7 alphanumerischen Symbolen innerhalb der 20-30 Sekunden. Bei der Brute-Force-Attacke würden Sie dafür über 24 Stunden brauchen.

Die Wahrscheinlichkeit, ein Passwort mithilfe des Rainbow-Table-Angriffs wiederherzustellen, ist niedriger im Vergleich zu den traditionellen Methoden. Es ist möglich, das Risiko des Rainbow-Attacke zu reduzieren, indem man längere Passwörter benutzt.

WELCHE PASSWÖRTER SIND UNSICHER?

Wenn wir diese möglichen Angriffsmethoden betrachten, können wir daraus schließen, welche Passwörter unsicher sind. Folgende Liste gibt allgemeine Richtlinien zur Vermeidung bestimmter Passwörter, da diese unsicher und leicht angreifbar sind.

1. Alle Passwörter, die standardmäßig in der Software benutzt werden;
2. Populäre Passwörter (qwerty, 123, Passwort, p@$$\/\/0rd, abc123 etc);
3. Wiederholte Symbolkombinationen (aabbcc, 123123, aaaa etc);
4. Umkehrung allgemeiner Wörter (trowssap, nimda etc);
5. Passwörter, die sich mit dem Nutzernamen überschneiden (beziehungsweise Variationen davon);
6. Kurze Passwörter bis zu 7 Symbolen, die mithilfe des Brute-Force- oder Rainbow-Table-Angriffs gefunden werden können;
7. Passwörter, die aus allgemeinen Wörtern oder Wortkombinationen bestehen, die somit leicht mit einer Wörterbuch-Suche zu finden sind;
8. Passwörter, die von privaten Daten oder Nutzercharakteristiken abgeleitet werden; veränderte Versionen alter Passwörter, die leicht mit Wörterbuch-Suche oder Masken-Angriff gefunden werden können;
9. Passwörter, die mit relativ populären Rainbow-Tabellen gefunden werden können;
10. Passwörter, die in verschiedenen Windows-Systemdateien oder im Cachespeicher gespeichert sind (solche Passwörter sind vielleicht sicher, doch unzulässige Systemeinstellungen verraten diese im Nu).

Es sind viel mehr Kriterien, die auf die Passwort-Unsicherheit hinweisen können. In Wirklichkeit können sie alle nicht von der Firmen-Passwortpolitik berücksichtigt werden. Demnach ist der beste Weg, unsichere Passwörter aufzudecken, das ganze System regulär zu überprüfen.

NICHT SICHERE PASSWÖRTER – GROSSE GEFAHR

BENUTZEN WIR OFT NICHT SICHERE PASSWÖRTER?

Laut einer Untersuchung der Informationssicherheit großer Unternehmen, die von einer Consulting-Gruppe Deloitte Touche[1] ausgeführt wurde, standen 14% der Firmen innerhalb der letzten 12 Monate dem Problem der unsicheren Passwörter gegenüber. In 9% der Fälle waren es standardmäßige Passwörter, in 7% der Fälle waren es einfache Passwörter, die von den Eindringlingen leicht herausgefunden wurden.

Wenn man die Untersuchungsdaten zusammenfasst, muss gesagt werden, daß 30% aller Unternehmen alljährlich dem Problem der unsicheren Passwörter gegenüberstehen. In 16% der Fälle ist es grobe Vernachlässigung einfachster Sicherheitsregeln und Passwort-Politik.

Laut Untersuchungsdaten von Bruce Schneier[2] wählen 3.8% der Nutzer die simplen Passwörter, die leicht im Wörterbuch zu finden sind. 12% der Nutzer nutzen auch simple Passwörter, doch sie fügen ein Symbol an Ende ein. 28% der Nutzer nutzen nur kleingeschriebene Buchstaben und Zeichen, die das Passwort anfällig für Brute-Force-Angriffe machen.

Diese Statistiken zeigen einige Risiken, die durch unsichere Passwörter erzeugt werden. Die Reihe der wirklichen Gefahren kann variieren.

POTENTIELLE PROBLEME, DIE DURCH NICHT SICHERE PASSWÖRTER VERURSACHT WERDEN

Lasst uns die potentiellen Gefahren detailliert betrachten. Es bestehen zwei Gefahren:

1. **Aussere Gefahr.** Angriff kommt aus dem Nichts. Das Passwort wurde dank einem direkten Hackerangriff herausgefunden.
2. **Innere Gefahr.** Unerlaubter Zugriff auf die vertraulichen Informationen erhalten, indem ein skrupelloser Mitarbeiter oder Insider das Nutzerpasswort herausgefunden hat.

Im ersten Fall wird das Passwort ein Ziel der direkten Hacker-Attacke. Der unsichtbare Zugriff auf die Ressourcen innerhalb der Firmen-Infrastruktur erleichtert die Abwicklung dieses Angriffes. Falls der Eindringling Zugriff auf die unbefugten Informationen mithilfe der Spyware (zum Beispiel, Programme, die Zugriffsschlüssel oder vertrauliche Informationen, die durch autorisierte Nutzer eingegeben werden, aufnehmen) oder Social-Engineering-Software bekommen hat, hat er einen weiteren Vorteil.

Wir sollten verstehen, dass diese Attacken nicht einfach aus Spass durchgeführt werden. Hackers sind an den Zugang zu den wertvollen Firmenressourcen interessiert. Diese Ressourcen sind das Ziel. Ein unsicheres Passwort zu finden ist der erste Schritt in der Ausnutzung des Zielnetzwerkes.

[1] „2007 Global Security Survey", Deloitte Touche (http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901(1).pdf,)
[2] „MySpace Passwords Aren't So Dumb", Bruce Schneier, 2006 (http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300)

Die Situation kann sogar gefährlicher werden, falls die Firmensicherheit vom Insider bedroht wird. Dem Insider könnten die beachtlichen EDV-Ressourcen zur Verfügung stehen. Firmen-PCs können dazu benutzt werden, passwortgeschützte Ressourcen zu attackieren. Der Insider ist gut in allen möglichen Angriffsvarianten: Brute-Force, Masken-Angriff, Wörterbuch-Suche oder Methoden, die auf privaten Nutzerdaten basieren (Geburtdaten, Namen, Familiennamen etc). Der Insider ist nicht gehindert, an den Ziel-PC physisch zu gelangen; dann würde vielleicht auch nicht der beste Passwortschutz helfen.

Materielle Schaden, die durch Hackerattacken verursacht werden, unbefugter Zugriff auf vertrauliche Informationen und finanzieller Betrug können sich auf große Geldsumme belaufen, je nach Ausmaß und Firmentyp.

Hier sind noch mehr Fakten, um die Situation zu illustrieren. Laut einer Untersuchung unter 370 US-Firmen, die durch Computer Security Institute[3] ausgeführt wurde, betragen die durchschnittlichen Verluste im Jahre 2007, die durch den Sicherheitsmissbrauch verursacht wurden, $345K. Die Zahlen haben sich seit 2006 verdoppelt.

In einigen Geschäftsbereichen, wie Finanzen oder Versicherungen, ist Reputationsverlust ausschlaggebend. Sollten die privaten Kundendaten in Gefahr gebracht werden, genügt ein einzelner Skandal, um die Firma am Rande des Bankrotts zu bringen.

Der erschreckendste Fakt ist, der Passwort-Mißbrauch kann, im Unterschied zur Virusattacke, nicht sofort aufgedeckt werden. Demnach kann der Eindringling Zugang zu vertraulichen Daten, strategischen oder finanziellen Informationen über eine längere Zeit haben. Hackerattacken und Leckstellen sind oft erst dann entdeckt, nachdem die Informationen bereits entnommen wurden und der Schaden nur bedingt zu beseitigen sind.

Passwortänderungs-Bestimmungen, die in vielen Firmen gültig sind, sind nutzlos, wenn erfahrene Hacker an der Arbeit sind, die das neue Passwort aus dem vorinstallierten Keylogger bekommen.

Um die Risiken, die aufgrund der unsicheren Passwörter bestehen, zu minimieren, sollten die Passwörter regelmäßig überprüft werden. Das nächste Kapitel diskutiert die Wege der Systemüberprüfung.

[3] „Computer Crime and Security Survey", Computer Security Institute (CSI), 2007 (http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf)

UNSICHERE PASSWÖRTER AUFDECKEN

Wie zuvor gesagt, ist die Firmen-Passwortpolitik, die Passwortlänge oder Passwortstruktur reguliert, nicht genug, um den Zugang zu Firmendaten zu sichern. Diese Maßnahmen bieten keinen Schutz für die Firmenpasswörter gegen die Hackerattacken mithilfe der Wörterbuch- oder Schablonensuche (zum Beispiel, bestehen komplexe Passwörter normalerweise aus Wörtern am Anfang, die von Zahlen und Großbuchstaben gefolgt werden).

Mehr noch zwingen die regulären Änderungen der Passwörter, die von der Sicherheitspolitik großer Unternehmen verlangt werden, den Nutzer regelrecht, die Passwörter zu vereinfachen und zu kürzen oder diese nach gleichen Mustern zu gestalten (mit leichten Modifizierungen).

Es ist möglich, die oben genannten Risiken zu minimieren. Die präventive Massnahme ist die regelmäßige Überprüfung der Passwörter, die im Firmennetzwerk benutzt werden.

Wie funktioniert es? Es ist sehr leicht. Stellen Sie vor, Sie sind der Eindringling und wollen die Passwörter von Nutzerkonten herausfinden.

Dies ist mithilfe der speziellen Software sehr leicht gemacht; diese Software wird von vielen Sicherheitsabteilungen größerer Unternehmen und speziellen Services verschiedener Länder benutzt.

Routinemäßig entdeckt die Passwort-Überprüfungs-Software unsichere Stellen im Sicherheitsnetz des Unternehmens und entfernt diese. Weiterhin hilft sie, herauszufinden, welche Nutzer diszipliniert sind und welche Nutzer eine Extra-Lernstunde in Passwort-Sicherheits-Grundlagen brauchen.

WAS IST DIE BESTE SOFTWARE?

Überprüfung der Firmenpasswörter kann durch verschiedene Software-Produkte durchgeführt werden. Der Markt strotzt von solcher Software: angefangen mit selbst gemachten und kostenlosen Lösungen bis hin zu speziell entwickelten kommerziellen Lösungen. Bei der Produktwahl müssen Sie dessen Features und Bedienbarkeit beachten.

Die wichtigsten Features sind das Modellieren verschiedener Angriffstypen, Unterstützung des Remote-Netzwerkes, verschiedene Sprachen und Plattformen.

Eine der funktionellsten und leicht zu bedienenden Lösungen ist Proactive Password Auditor von ElcomSoft. Es wird später vorgestellt.

PASSWORT-ÜBERPRÜFUNG MIT PROACTIVE PASSWORD AUDITOR

Proactive Password Auditor (PPA) löst das Problem der Passwort-Überprüfung schnell und effizient. PPA unterstützt verschiedene Typen möglicher Angriffe: Wörterbuch-Suche, Brute-Force-Angriff und Rainbow-Table-Attacke.

Dieses Produkt wurde entwickelt, um die Passwort-Sicherheit unter Windows NT, Windows 2000, Windows XP, Windows 2003 Server, Windows Vista und dem aktuellsten Windows Server 2008 zu testen.

PPA wurde für den Firmengebrauch entwickelt. Das Produkt ermöglicht den Systemadministratoren, Nutzerkonten mit nicht sicheren Passwörtern zu identifizieren.

Das Hash-Prinzip erlaubt keine Wiederherstellung der ursprünglichen Passwörter aus dem Hash (entweder LM-Hash oder NTLM-Hash). Jedoch kann ein Passwort mithilfe der Brute-Force-Attacke, Wörterbuch-Suche wiederhergestellt werden, indem alle möglichen Kombinationen aus einer bestimmten Auswahl oder mit einer Wörterliste ausprobiert werden. Daher brauchen Sie zum Finden des Passwortes:

- Passwort-Hashes zu sammeln;
- Passwörter zu finden, die mit Hashes übereinstimmen.

Um Passwörter- Hashes mit PPA zu bekommen, müssen Sie entweder:

- Lokalen PC-Speicher durchsuchen;
- PC-Remote-Speicher durchsuchen (mit Active Directory - Support);
- Lokale PC-Registry durchsuchen;
- Ausgabedateien nutzen, die von Hilfstools, wie pwdump, eingeholt werden;
- Hashes laden, die mithilfe von Elcomsoft System Recovery erstellt wurden.

Proactive Password Auditor erlaubt die Ausführung der Passwort-Prüfung innerhalb einer bestimmten Zeitspanne. Dieses Produkt benutzt einzigartige Algorithmen samt Optimierung der Suchgeschwindigkeit. Nach dem Prüfungsende sollten Sie bedenken, dass das Ersetzen der nicht sicheren Passwörter nicht genug ist. Was ist, wenn neue Passwörter noch unsicherer sind? Denken Sie als erstes über die Firmen-Passwortpolitik und deren Effizienz nach. Falls reguläre PPA – Überprüfung weiterhin zu viele Passwörter ‚hackt', sollte diese Politik umgedacht werden.

Zusätzlich zum direkten Gebrauch kann PPA auch von Systemadministratoren benutzt werden, um ein Passwort eines beliebigen Nutzers (zur Wiederherstellung des Zuganges zu den verschlüsselten EFS - Daten, gespeicherte Internet-Passwörter etc) mit Brute-Force-Angriff, Wörterbuch-Suche und Rainbow-Table-Attacke wiederherzustellen.

Sie können die Testversion von Proactive Password Auditor hier downloaden.

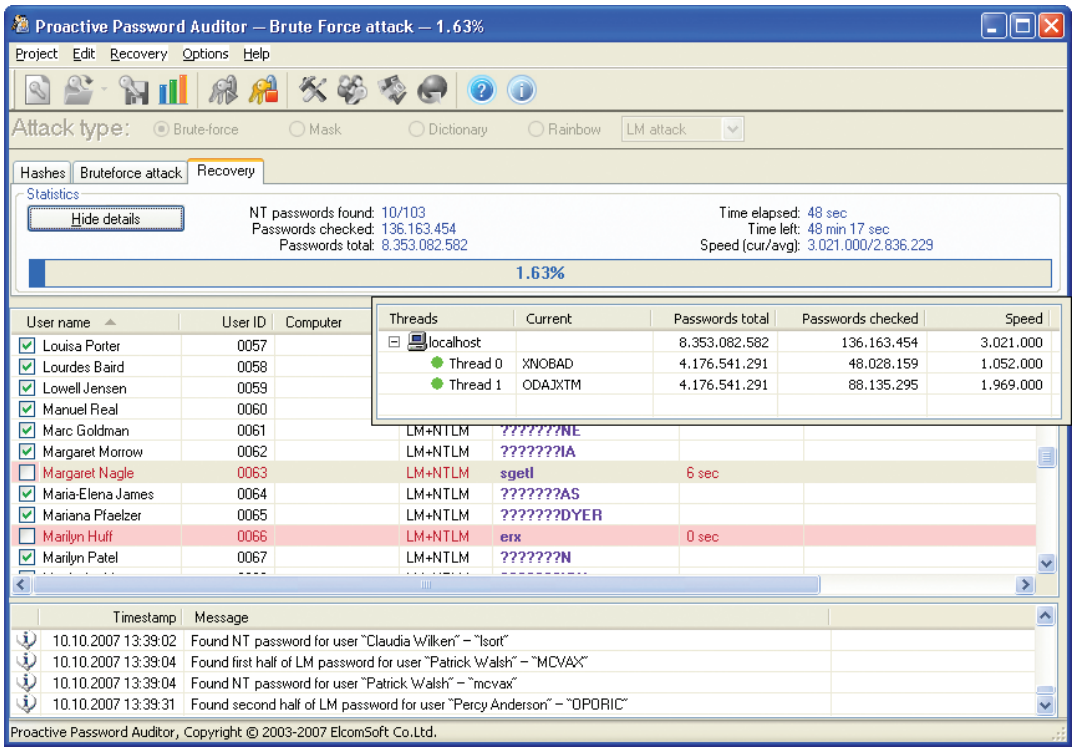


Bild 1. Proactive Password Auditor überprüft Nutzerpasswörter.

ÜBER ELCOMSOFT

Der 1990 gegründete russische Software-Entwickler ElcomSoft Co. Ltd. zählt zu den führenden Experten im Bereich Software zur Sicherheitsprüfung und Wiederherstellung von Passwörtern und Kennungen, mit denen sie Windows-Netzwerke sichern bzw. auf wichtige Dokumente zugreifen können. Dank der einzigartigen Technologien genießen die Produkte des Unternehmens weltweite Anerkennung.

Zu den Kunden von ElcomSoft zählen weltbekannte Unternehmen aus folgenden Branchen:

High Tech: Microsoft, Adobe, IBM, Cisco
Regierungseinrichtungen: FBI, CIA, US Army, US Navy, Department of Defence
Consulting-Unternehmen: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finanzdienstleistungen: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telekommunikation: France Telecom, BT, AT&T
Versicherungen: Allianz, Mitsui Sumitomo
Handel: Wal-Mart, Best Buy, Woolworth
Medien & Unterhaltung: Sony Entertainment
Hersteller: Volkswagen, Siemens, Boeing
Energie: Lukoil, Statoil
Pharmazie: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Das Unternehmen ist Microsoft Gold Certified Partner, Intel Software Partner, Mitglied der Russian Cryptologie Association (RCA), des Computer Security Institute (CSI) und der Association of Shareware Professionals (ASP).

Auf die technologischen Errungenschaften von Elcomsoft wird in vielen bekannten Büchern Bezug genommen, beispielsweise, in der Microsoft-Enzyklopädie „Microsoft Encyclopedia of Security", „The art of deception" (Kevin Mitnick), „IT Auditing: Using Controls to Protect Information Assets" (Chris Davis) und „Hacking exposed" (Stuart McClure).

Mehr über Elcomsoft können Sie auf der Webseite des Unternehmens erfahren.

ADRESSE:

ElcomSoft Co. Ltd.
Zvezdnyi blvd. 21, Office 541
129085 Moskau

FAX:

USA (toll-free): +1 (866) 448-2703
Großbritannien: +44 (870) 831-2983
Deutschland: +49 18054820050734

WEBSEITEN:

http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr