डोमेन कैश्ड पासवर्ड रिकवर करना

पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

Table contents

परिचय

1 परिचय

जैसा कि आप शायद पहले से ही जानते हैं, Windows NT आधारित ऑपरेटिंग सिस्टम स्थानीय मशीन पर डोमेन अकाउन्ट के पासवर्ड को अधिक सटीक रूप से संग्रहीत करते हैं या कैश करते हैं। यह किसी कारणवश लॉगिन सर्वर उपलब्ध नहीं होने पर भी यूजर्स को उनके अकाउन्ट में लॉग इन करने की अनुमति देने के लिए किया जाता है। इस मामले में, यूजर के पास ऐसे किसी भी नेटवर्क संसाधन तक पहुंच होगी, जिसके लिए यूजर प्रमाणीकरण की आवश्यकता नहीं होती है।

विंडोज NT में पासवर्ड कैशिंग

2 विंडोज NT में पासवर्ड कैशिंग

Windows NT ऑपरेटिंग सिस्टम दो सामान्य प्रकार के पासवर्ड कैशिंग का उपयोग करते हैं:

- सामान्य कैशिंग
- डोमेन-लेवल कैशिंग

डोमेन-लेवल कैशिंग कम से कम दो कार्य प्रदान करता है:

1. डोमेन नियंत्रक उपलब्ध न होने पर भी कंप्यूटर संसाधनों तक पहुँच प्रदान करें। उदाहरण के लिए, लैपटॉप पर यूजर अपने डोमेन खाते में लॉग ऑन करता है। फिर यूजर लैपटॉप को उस स्थान पर ले जाता है जहां डोमेन उपलब्ध नहीं है। ऐसे मामले में, विंडोज़ स्थानीय रूप से सिस्टम में लॉग ऑन करने और कंप्यूटर के स्थानीय संसाधनों तक पहुंच सुनिश्चित करने के लिए कैश्ड डेटा का उपयोग करेगा।
2. सिंगल साइन-ऑन (SSO) - कार्यक्षमता पहले इंटरेक्टिव साइन-ऑन के दौरान प्राप्त डेटा का उपयोग करके और इसे फिर से दर्ज करने को छोड़कर एक बार नेटवर्क प्रमाणीकरण करती है।

यदि डोमेन कैशिंग डिसेबल है, तो सर्वर पर लॉगऑन करने का प्रयास करने पर निम्न संदेश मिलेगा:

सिस्टम आपको अभी लॉग ऑन नहीं कर सकता क्योंकि डोमेन DOMAIN_NAME उपलब्ध नहीं है

यदि डोमेन नियंत्रक उपलब्ध नहीं है, तो सिस्टम पहले कैश में सहेजे गए डेटा का उपयोग करता है। तो संदेश थोड़ा अलग दिखाई देगा:

आपके डोमेन के लिए एक डोमेन नियंत्रक से संपर्क नहीं किया जा सका। आप केश की हुई अकाउन्ट जानकारी का उपयोग करके लॉग ऑन कर चुके हैं। पिछली बार लॉग ऑन करने के बाद से आपकी प्रोफ़ाइल में परिवर्तन उपलब्ध नहीं हो सकते हैं।

कैशिंग विकल्प सेट करना

3 कैशिंग विकल्प सेट करना

क्लाइंट साइड पर संग्रहीत कैश्ड क्रेडेंशियल्स की संख्या

विंडोज रजिस्ट्री को एडिट करके, आप ऑपरेटिंग सिस्टम द्वारा कैश किए जाने के लिए आवश्यक संख्या में लॉगऑन प्रयासों को मैन्युअल रूप से सेट कर सकते हैं। वह वेल्यु 0 और 50 के बीच भिन्न हो सकता है। यदि वेल्यु 0 पर सेट है, तो कैशिंग डिसेबल हो जाएगी। डिफ़ॉल्ट रूप से, Windows 10 सफल लॉगऑन प्रयासों को संग्रहीत करता है। कैशिंग को निम्न रजिस्ट्री की से नियंत्रित किया जाता है:

की का नाम : **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**
वेल्यु का नाम : **CachedLogonsCount**
डेटा का प्रकार : **REG_SZ**
वेल्यूज : **0 - 50**

डोमेन कैश्ड पासवर्ड का उपयोग करने पर अधिसूचना

डिफ़ॉल्ट रूप से, यदि आप डोमेन नियंत्रक के उपलब्ध न होने पर (Windows-आधारित वर्कस्टेशन का उपयोग करके) किसी डोमेन से कनेक्ट करने का प्रयास करते हैं, तो आपको कोई चेतावनी संदेश नहीं दिखाई देगा और इसलिए, शायद ही ध्यान दें कि कैश्ड क्रेडेंशियल्स का उपयोग करके साइन ऑन किया है। यदि आप विंडोज को इस तरह से कॉन्फ़िगर करना चाहते हैं कि हर बार जब आप कैश्ड पासवर्ड का उपयोग करके साइन इन करते हैं तो यह संबंधित चेतावनी दिखाएगा, तो इन दो रजिस्ट्री कीज को सेट करें:

की का नाम : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Winlogon**
वेल्यु का नाम : **ReportControllerMissing**
डेटा का प्रकार : **REG_SZ**
वेल्यूज : **TRUE**

और फिर सिस्टम के प्रत्येक यूजर के लिए:

की का नाम : **HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon**
वेल्यु का नाम : **ReportDC**
डेटा का प्रकार : **REG_DWORD**
वेल्यूज : **1**

डोमेन कैश्ड क्रेडेंशियल्स की सुरक्षा

4 डोमेन कैश्ड क्रेडेंशियल्स की सुरक्षा

'डोमेन कैश्ड क्रेडेंशियल्स' शब्द विंडोज कैश और निजी जानकारी को स्टोर करने के तरीके को पूरी तरह से प्रतिबिंबित नहीं करता है। Windows 2000 से शुरू होकर, यूजर पासवर्ड को प्लेनटेक्स्ट के रूप में स्टोर नहीं किया जाता है। इसके विपरीत, सिस्टम एक पासवर्ड हैश को संग्रहीत करता है, नमक के साथ थोड़ा संशोधित (यानी नमकीन हैश), जहां नमक यूनिकोड प्रारूप में यूजर का नाम है।

Microsoft का दावा है कि इस एन्क्रिप्शन एल्गोरिथम से निम्नलिखित निष्कर्ष निकाले जा सकते हैं:

- नमकीन हैश का उपयोग किए जाने के बाद से प्रीकंप्यूटेड टेबल लागू नहीं होते हैं
- DCC हैश का उपयोग अन्य सिस्टम पर साइन ऑन करने के लिए नहीं किया जा सकता है

इस मुद्दे को दूसरे बिंदु से देखने से पता चलता है कि:

- उपनामों के लिए पूर्व-गणना टेबल बनाई जा सकती हैं, अर्थात ज्ञात यूजर नामों के लिए; उदाहरण के लिए, अंतर्निहित एडमिनिस्ट्रेटर या गेस्ट अकाउन्ट के लिए। दूसरी ओर, यह समय की बर्बादी हो सकती है, क्योंकि एक अंतर्निहित एडमिनिस्ट्रेटर या गेस्ट अकाउन्ट अक्सर इसे हल्के ढंग से इनेबल करने के लिए सक्षम नहीं होता है।
- अन्य सिस्टम पर साइन इन करने की संभावना को पूरी तरह से समाप्त करने के लिए, यूजर नाम के साथ डोमेन नाम को भी नमकीन किया जाना चाहिए।

डोमेन कैश्ड पासवर्ड पर संभावित हमले

5 डोमेन कैश्ड पासवर्ड पर संभावित हमले

कंप्यूटर तक पहुंच प्राप्त करने के लिए एक संभावित पुरुष कारक, आसानी से एक नया जोड़ सकता है या अपने स्वयं के मूल्य के साथ मौजूदा हैश को अधिलेखित कर सकता है। प्रक्रिया कंप्यूटर तक भौतिक पहुंच मानती है।

हालांकि, कैश्ड पासवर्ड को केवल पुनर्लेखन या प्रतिस्थापन निजी यूजर डेटा, एन्क्रिप्टेड फ़ाइलों, DPAPI (इंटरनेट एक्सप्लोरर, आउटलुक, विंडोज मेल, WPA पासवर्ड, और अन्य डेटा) के साथ संरक्षित डेटा तक संभावित हानिकारक पहुंच प्रदान नहीं करता है।

डोमेन कैश्ड क्रेडेंशियल - भीतर से एक नज़र

6 डोमेन कैश्ड क्रेडेंशियल - भीतर से एक नज़र

डोमेन कैश्ड डेटा निम्न स्थान पर Windows रजिस्ट्री में एन्क्रिप्टेड संग्रहीत किया जाता है: **HKEY_LOCAL_MACHINE\SECURITY\Cache.** बाइनरी वेल्यु **NL$x** एक कैश रिकॉर्ड को इंगित करता है, जहां 'x' रिकॉर्ड संख्या के लिए है। इस रजिस्ट्री की तक पहुंच केवल सिस्टम को दी जाती है।

प्रत्येक रिकॉर्ड में शामिल हैं:

- यूजर पर विस्तृत जानकारी। अर्थात्: यूजर का संक्षिप्त और पूरा नाम, अंतिम पहुंच का समय, सिस्टम में पहचानकर्ता, डोमेन नाम, डोमेन DNS नाम, साइन-ऑन डोमेन, स्क्रिप्ट, यूजर प्रोफ़ाइल का पाथ, होम निर्देशिका, होम निर्देशिका ड्राइव, समूहों में सदस्यता, आदि।
- पासवर्ड हैश, अतिरिक्त रहस्य, और Pbkdf2 पुनरावृत्ति काउंटर (Windows Vista और बाद के OSes में एन्क्रिप्शन के लिए प्रयुक्त) सहित निजी जानकारी।

डोमेन कैश्ड डेटा के एन्क्रिप्शन में LSA गुप्त NL$KM शामिल होता है, जिसमें 64-बाइट मास्टर की स्थानीय सिस्टमर से जुड़ी होती है। NL$KM सुरक्षा रजिस्ट्री फ़ाइल में स्थित है और बदले में, **SYSKEY** के साथ एन्क्रिप्ट भी किया गया है।

इस प्रकार, समग्र डोमेन रिकॉर्ड डिक्रिप्शन योजना इस तरह दिखती है:

- SYSKEY + LSA Master Key + NL$KM = DCC Master Key
- DCC Master Key + NL$x entry = Decrypted DCC entry

एक बार कैश्ड डोमेन प्रविष्टि डिक्रिप्ट हो जाने के बाद, हम यूजर अकाउन्ट के नमकीन हैश तक पहुंच प्राप्त करते हैं। नमकीन हैश का उपयोग तब प्लेनटेक्स्ट लॉगऑन पासवर्ड का अनुमान लगाने के लिए किया जा सकता है:

Windows 2000-2003 के लिए: हैश = MD4 (MD4(user password) + lowercase(user name))

Windows Vista से शुरू होकर, एन्क्रिप्शन एल्गोरिथम थोड़ा बदल गया है। अब इसे SHA-1 हैश के अतिरिक्त पुनरावृत्तियों के साथ लागू किया गया है:

hash = PBKDF2_SHA(MD4 (MD4(user password)+lowercase(user name)), iterations)

डिफ़ॉल्ट रूप से, पुनरावृत्तियों काउंटर 10240 के बराबर है।

डोमेन कैश्ड क्रेडेंशियल्स को रिकवर करने पर प्रेक्टिकल मार्गदर्शिका

7 डोमेन कैश्ड क्रेडेंशियल्स को रिकवर करने पर प्रेक्टिकल मार्गदर्शिका

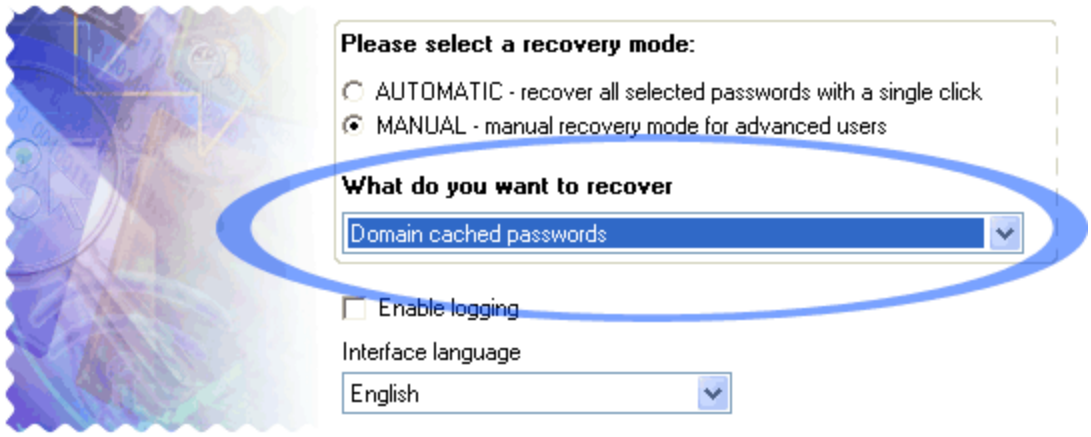
संपूर्ण रिकवरी दुःस्वप्न से गुजरने के लिए हमें एकमात्र टूल नेटवर्क पासवर्ड रिकवरी विज़ार्ड की जरुरत है। आइए पूरे वर्कफ़्लो को तीन टुकड़ों में विभाजित करें:

1. डोमेन कैश्ड रिकॉर्ड का डिक्रिप्शन
2. डिक्रिप्टेड रिकॉर्ड का विश्लेषण
3. चयनित प्रविष्टि की पासवर्ड रिकवरी

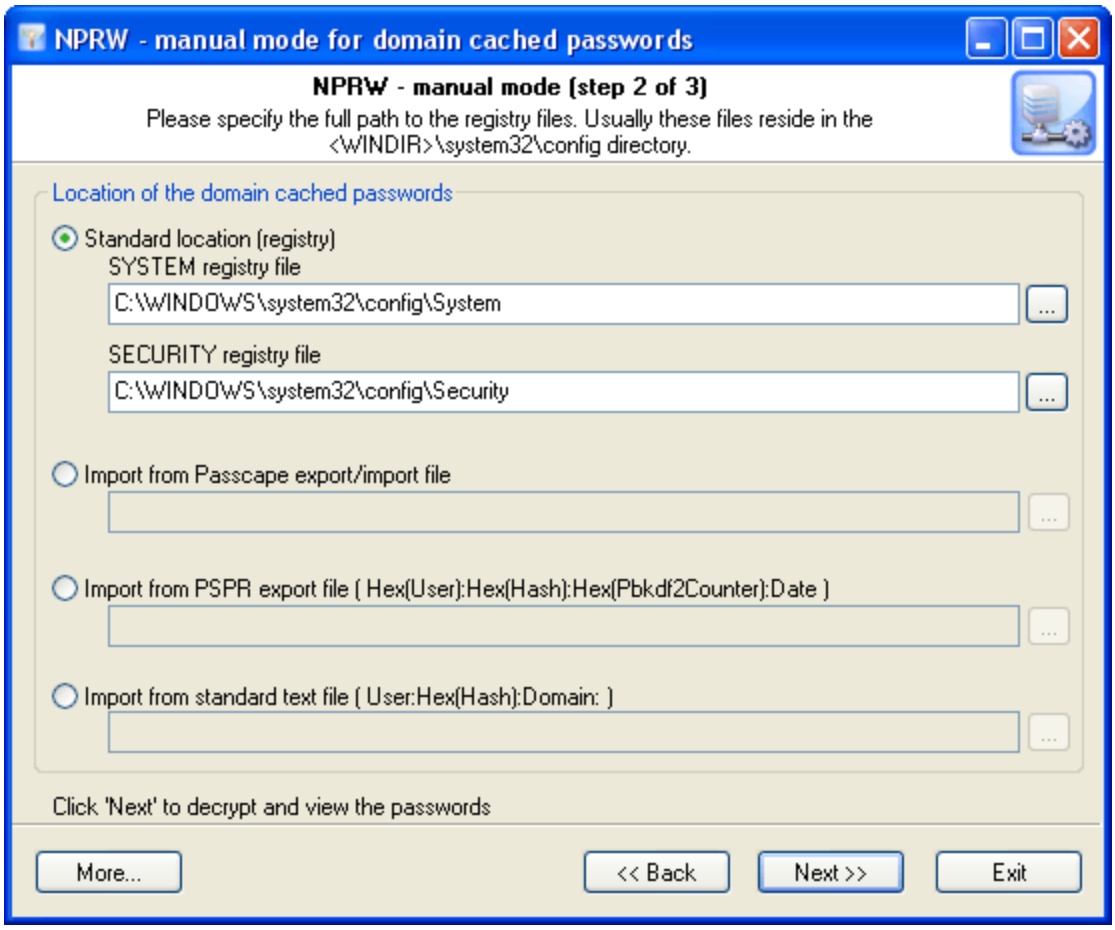
तो चलिए चलते हैं।

1. डोमेन कैश्ड रिकॉर्ड का डिक्रिप्शन

एप्लिकेशन लॉन्च करें और ड्रॉप-डाउन मेनू से चुनें कि हम क्या रिकवर करना चाहते हैं: डोमेन कैश्ड पासवर्ड। यदि कैश्ड रिकॉर्ड स्थानीय कंप्यूटर पर हैं, तो आत्मविश्वास के साथ स्वचालित मोड को सक्रिय करें और आगे बढ़ें।



मैनुअल ऑपरेटिंग मोड बहुत अधिक लचीला है और यूजर्स को मैन्युअल रूप से डेटा स्रोत का चयन करने की अनुमति देता है, चाहे वह मानक स्थान (रजिस्ट्री फ़ाइलें), पास्केप की मूल आयात/निर्यात फ़ाइल या किसी अन्य प्रोग्राम से आयात किया गया डेटा हो।

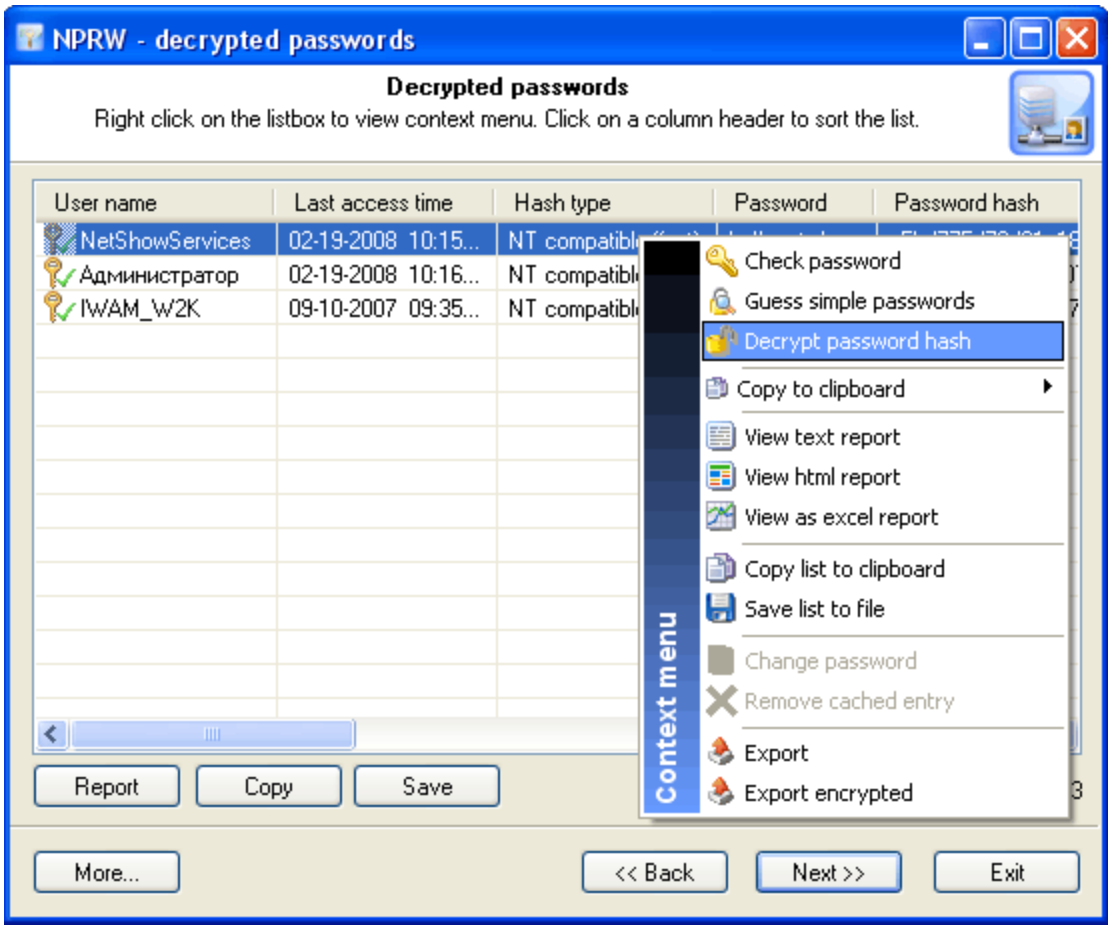


'Next' पर क्लिक करें और तब तक प्रतीक्षा करें जब तक प्रोग्राम इनपुट डेटा को संसाधित करना समाप्त न कर दे।

2. डिक्रिप्टेड रिकॉर्ड का विश्लेषण

एक सफल डिक्रिप्शन और क्रेडेंशियल आयात करने पर, यूजर्स को डिक्रिप्टेड रिकॉर्ड की एक सूची मिलनी चाहिए। प्रत्येक रिकॉर्ड में कई डेटा फ़ील्ड होते हैं; उदाहरण के लिए, यूजर नाम, सर्वर, समूहों में सदस्यता, आदि।

राइट-क्लिक करके संदर्भ मेनू खोलना कार्यक्रम की विस्तारित क्षमताओं को संलग्न करने की अनुमति देता है। पूरी सूची के लिए: कॉपी करना, सेव करना, रिपोर्ट देखना या पूरी सूची को निर्यात करना। एक व्यक्तिगत रिकॉर्ड के लिए: पासवर्ड बदलना, रिकॉर्ड हटाना, पासवर्ड को मान्य करना, सरल और अक्सर उपयोग किए जाने वाले संयोजनों को खोजकर पासवर्ड रिकवर करना, या पूर्ण पैमाने पर हमला करना।



चयनित पासवर्ड के लिए हमला शुरू करने से पहले, इन दो क्षेत्रों पर ध्यान दें: 'पासवर्ड' और 'हैश टाइप'। कभी-कभी एक कैश्ड पासवर्ड का आसानी से अनुमान लगाया जा सकता है बिना पूरी तरह से स्केलेबल हमले का उपयोग किए, बल्कि एक साधारण अटैक को लॉन्च करके। ऐसी स्थिति में, 'पासवर्ड' फ़ील्ड में प्लेन टेक्स्ट पासवर्ड प्रदर्शित किया जाएगा, और रिकॉर्ड को संबंधित आइकन से चिह्नित किया जाएगा।

'हैश प्रकार' फ़ील्ड में एक पासवर्ड हैश प्रकार होता है, जो 3 में से एक हो सकता है: 'NT compatible instant, - instant recovery, 'Win2K compatible fast' - प्रति सेकंड कई लाख पासवर्ड की गति से त्वरित रिकवरी या 'Vista, धीमा' - एक आधुनिक कंप्यूटर पर रिकवरी गति केवल कई सैकड़ों पासवर्ड प्रति सेकंड है।

3. चयनित प्रविष्टि की पासवर्ड रिकवरी

इसलिए, चयनित रिकॉर्ड की पासवर्ड रिकवरी शुरू करने के लिए, उस पर राइट-क्लिक करें और फिर संदर्भ मेनू पर 'डिक्रिप्ट पासवर्ड हैश' चुनें। यह डिक्रिप्शन मेथड डायलॉग को खोलेगा। सभी प्रकार के हमलों का वर्णन करने का कोई मतलब नहीं है। उस पर विस्तृत जानकारी कार्यक्रम के मैनुअल में पाई जा सकती है।

एक अपरिष्कृत यूजर पूरी तरह से उचित और सुसंगत प्रश्न पूछ सकता है: "रिकवरी की कोई 100% गारंटी नहीं है, हालांकि कई विधियां हैं। इसके सफल समापन की संभावना बढ़ाने के लिए कौन सा हमला शुरू किया जाना चाहिए?"

हमलों के प्रकार और अनुक्रम को चुनने के लिए, हम इस एल्गोरिथम का पालन करने की सलाह देते हैं, जो कि अधिकांश मामलों में पासवर्ड प्रकार की विस्तृत श्रृंखला पर लागू होता है:

- सबसे पहले, प्रारंभिक हमले के विकल्प को एनेबल करें, यदि यह उपलब्ध है। यह सरल और अक्सर उपयोग किए जाने वाले संयोजनों को रिकवर करने में मदद करता है।
- दूसरा, यदि आप अपने द्वारा खोजे जा रहे पासवर्ड के बारे में जानते हैं, तो पहले मास्क अटैक या बेस-वर्ड अटैक का प्रयास करना अच्छा होगा। विशेष रूप से, यदि आप पासवर्ड का एक हिस्सा जानते हैं तो मास्क अटैक का उपयोग करना अधिक प्रभावी होगा। यदि आप पासवर्ड के मूल घटक को जानते हैं या, उदाहरण के लिए, पासवर्ड जानते हैं, लेकिन इसमें कैप्स और लोअरकेस वर्णों का क्रम याद नहीं है, तो बेस-वर्ड अटैक बेहतर काम करेगा।

यदि आपके पास उस पासवर्ड के बारे में कोई जानकारी नहीं है जिसे आप ढूंढ रहे हैं, तो चरणों के निम्नलिखित अनुक्रम द्वारा निर्देशित रहें:

1. AI अटैक को म्यूटेशन और इंडेक्सिंग विकल्पों के साथ न्यूनतम पर सेट करें।
2. यदि पासवर्ड नहीं मिला, तो बस पुनः प्रयास करें और उत्परिवर्तन विकल्प को 'सामान्य' स्तर पर सेट करें और अनुक्रमण को 'deep' पर सेट करें।
3. म्यूटेशन विकल्प डिसेबल के साथ डिक्शनरी अटैक लॉन्च करें।
4. इनेबल म्यूटेशन विकल्प के साथ डिक्शनरी अटैक लॉन्च करें; उत्परिवर्तन की गहराई उपलब्ध समय की मात्रा और हमले की गति पर निर्भर करती है। राष्ट्रीय कीबोर्ड लेआउट में टाइप किए गए पासवर्ड की खोज करते समय, उत्परिवर्तन की गहराई को मजबूत पर सेट किया जाना चाहिए।
5. ऑनलाइन शब्दकोश चुनें और डाउनलोड करें और चरण 3 - 4 दोहराएं।
6. पास-फ्रेज अटैक को उत्परिवर्तन विकल्प डिसेबल के साथ लॉन्च करें।
7. पास-फ्रेज अटैक को उत्परिवर्तन विकल्प एनेबल के साथ लॉन्च करें और अधिकतम उत्पादकता पर सेट करें। यह राष्ट्रीय कीबोर्ड लेआउट में टाइप किए गए पासवर्ड का अनुमान लगाने की अनुमति देगा।
8. ऑनलाइन पास-वाक्यांश शब्दकोश चुनें और डाउनलोड करें और चरण 6 - 7 दोहराएं।
9. वाक्यांश निर्माण नियमों के साथ संयुक्त शब्दकोश अटैक शुरू करें।
10. संयुक्त हमले के लिए ऑनलाइन शब्दकोश चुनें और डाउनलोड करें और चरण 9 दोहराएं।
11. ब्रूट-फ़ोर्स अटैक के लिए एक वर्णसेट का चयन करें, हमला शुरू करें।
12. यदि आवश्यक हो, एक नया चुनें या पुराने केरेक्टर सेट को पूरा करें और ब्रूट-फ़ोर्स अटैक को दोहराएं; यानी चरण 11।

चरण 1-2 - प्लेन टेक्स्ट पासवर्ड के लिए अपने स्थानीय सिस्टम को स्कैन करें।
चरण 3-5 - एक-शब्द पासवर्ड निकालें।
चरण 6-10 - बहु-शब्द पासवर्ड उत्पन्न करें।
चरण 11-12 - संपूर्ण खोज।

Outro

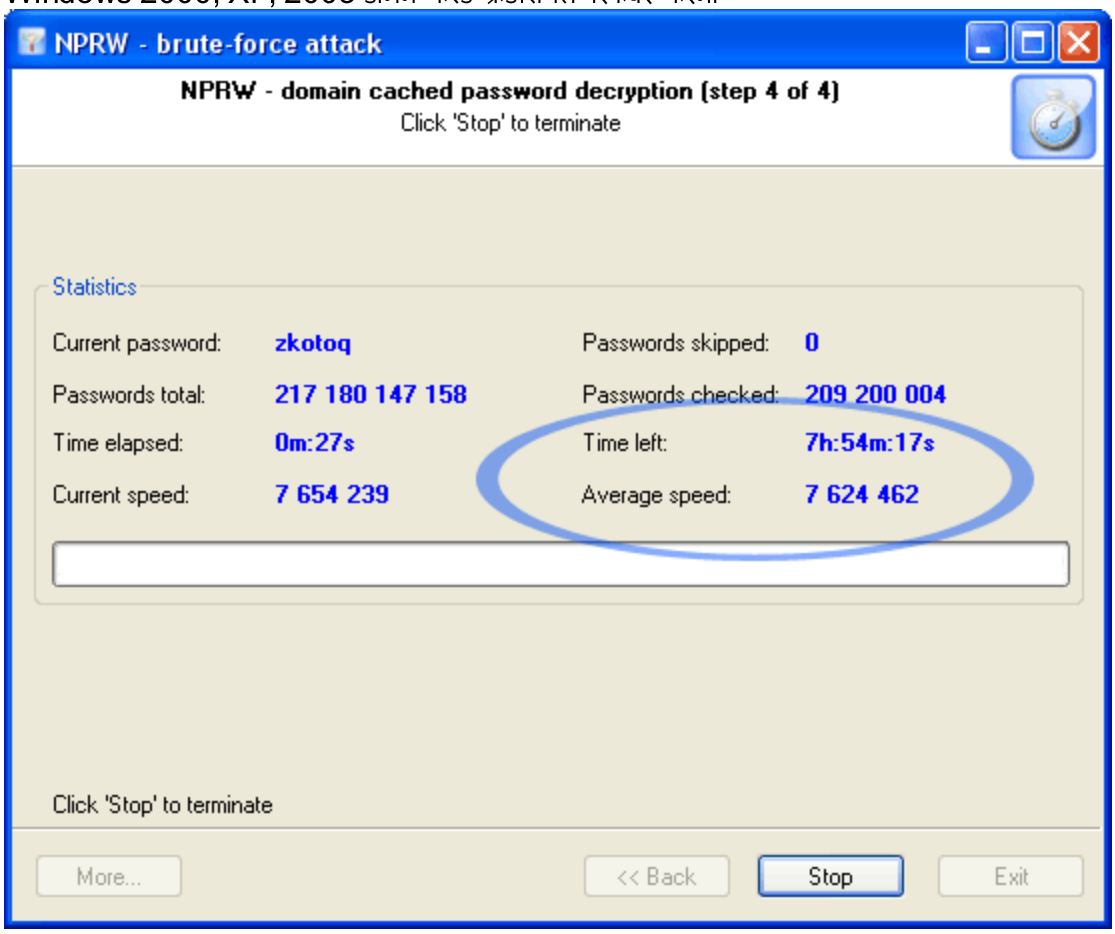
8 Outro

Windows 2000 डोमेन कैश्ड क्रेडेंशियल को डिक्रिप्ट करते समय आप सभी प्रकार के अटैक का पूरा लाभ उठा सकते हैं। हालांकि, जब विंडोज विस्टा-संगत डोमेन कैश को पुनर्प्राप्त करने की बात आती है, तो डिक्शनरी हमले के अलावा किसी भी चीज़ पर गंभीरता से भरोसा करना मुश्किल होता है।

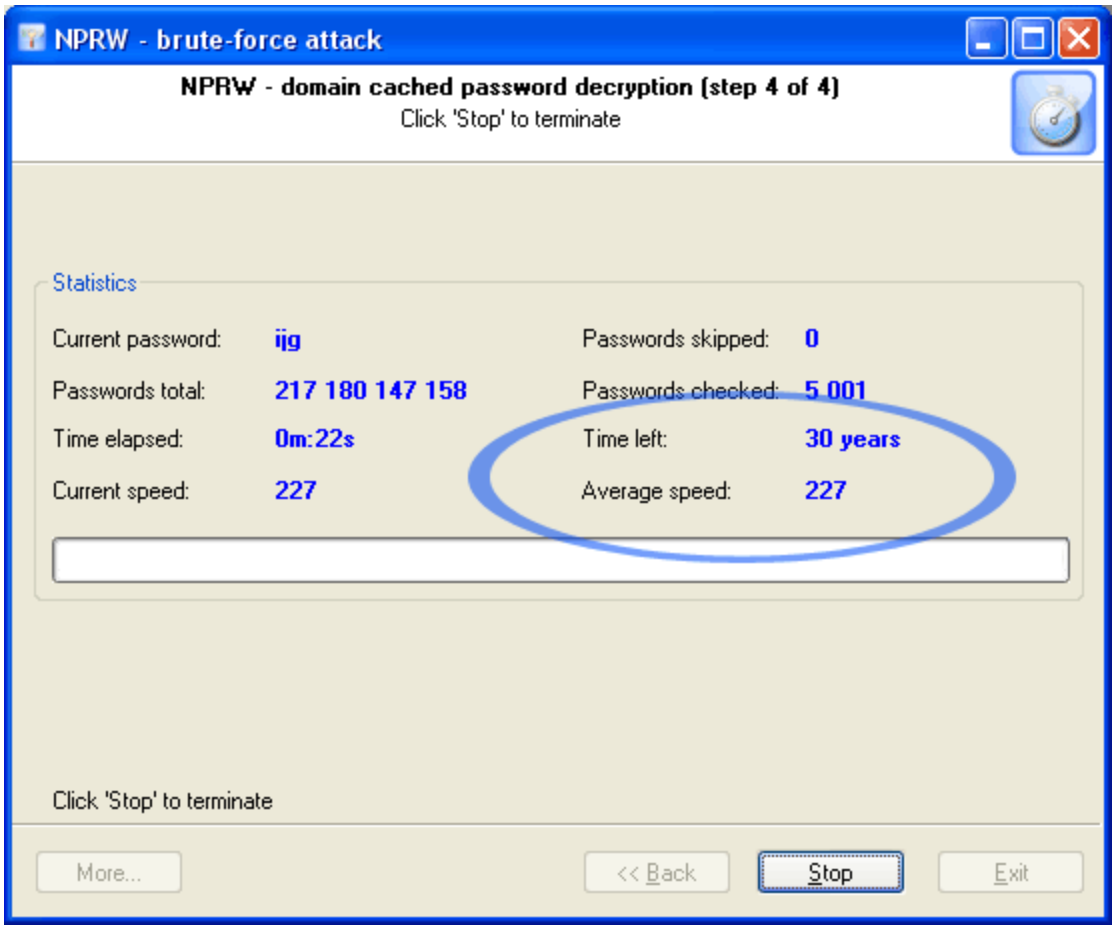
आइए जानें कि दोनों ही मामलों में एक सरल, आठ-वर्णों वाला पासवर्ड रिकवर करने और एक संपूर्ण खोज को पूरा करने में कितना समय लगता है। a..z वर्णों की पूरी श्रृंखला के माध्यम से खोजने के लिए, हमें बहुत अधिक और बहुत कम नहीं बल्कि 217 180 147 158 पासवर्ड संयोजन को मान्य करने की आवश्यकता होगी।

आइए अब समय पर एक नजर डालते हैं।

Windows 2000, XP, 2003 डोमेन कैश्ड क्रेडेंशियल रिकवर करना



Windows Vista कैश्ड क्रेडेंशियल रिकवर करना


NPRW - brute-force attack
NPRW - domain cached password decryption (step 4 of 4)
Click 'Stop' to terminate
Statistics
Current password: ijg
Passwords skipped: 0
Passwords total: 217 180 147 158
Passwords checked: 5 001
Time elapsed: 0m:22s
Time left: 30 years
Current speed: 227
Average speed: 227
Click 'Stop' to terminate
More...
<< Back
Stop
Exit

परिशिष्ट

9 परिशिष्ट

Windows 2000, XP, 2003 में डोमेन कैश्ड पासवर्ड को मान्य करने के लिए C++ एल्गोरिथम:

```
BOOL CheckCachedDomainPassword(LPCTSTR cszUserName, LPCTSTR
cszPassword, BYTE pCheckHash[0x10])
{
   WCHAR wsz[256];
   BYTE pHash[0x10];
   INT iLen;

   iLen=strlen(cszPassword);
   MultiByteToWideChar(CP_ACP
,MB_PRECOMPOSED,cszPassword,iLen,wsz,256);
   Md4Init();
   Md4Update((LPBYTE)wsz,iLen*2);
   Md4Final(pHash);

   iLen=strlen(cszUserName);
   MultiByteToWideChar(CP_ACP
,MB_PRECOMPOSED,cszUserName,iLen,wsz,256);
   CharLowerW(wsz);
   Md4Init();
   Md4Update(pHash,0x10);
   Md4Update((LPBYTE)wsz,iLen*2);
   Md4Final(pHash);

   return ( memcmp(pCheckHash,pHash,0x10)==0 );
}
```