# सुरक्षा ऑडिट: विंडोज़ ओएस में यूज़र प्लेनटेक्स्ट पासवर्ड


पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

# Table contents

# सुरक्षा ऑडिट: विंडोज ओएस में यूजर प्लेनटेक्स्ट पासवर्ड

# 1 सुरक्षा ऑडिट: विंडोज ओएस में यूजर प्लेनटेक्स्ट पासवर्ड

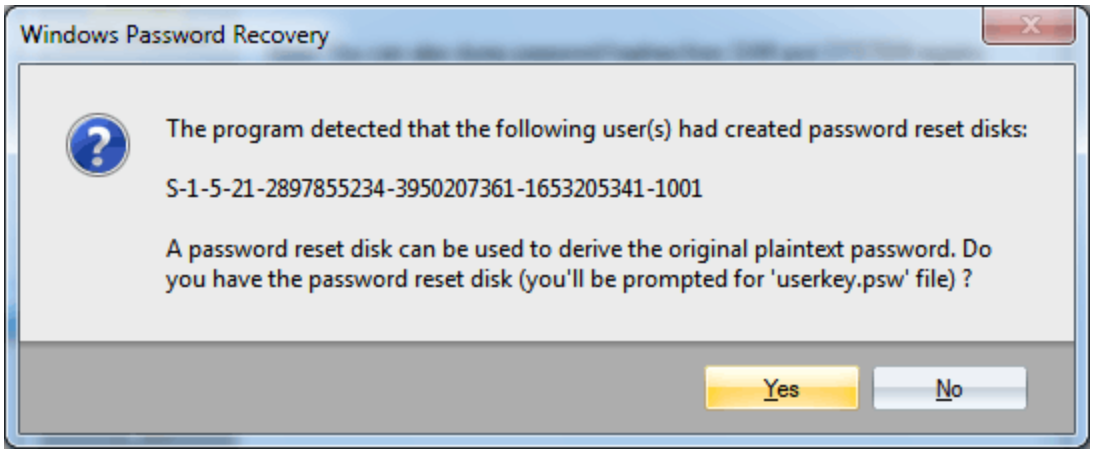
क्या आपका विंडोज लॉगऑन पासवर्ड 30 अक्षर लंबा है? आपको इसे तोड़ने के लिए खेद है, लेकिन यह बेकार है। आपके अकाउन्ट तक भौतिक पहुंच वाला कोई भी घुसपैठिया बिना किसी परेशानी के आपके पासवर्ड पर हाथ रख सकता है।

विंडोज ऑपरेटिंग सिस्टम को मूल रूप से यूजर पासवर्ड को खुले तौर पर स्टोर करने के लिए नहीं, बल्कि वन-वे फंक्शन (OWF) का उपयोग करने के लिए डिज़ाइन किया गया था, जिसे हैश फंक्शन भी कहा जाता है। उदाहरण के लिए, पासवर्ड **test** एक 16-सिम्बोल स्ट्रिंग **0CB6948805F797BF2A82807973B89537** या, अधिक सटीक रूप से, एक हैश उत्पन्न करता है जो SYSKEY यूटिलिटी का उपयोग करके अतिरिक्त रूप से एन्क्रिप्ट किया गया है और SAM रजिस्ट्री फ़ाइल में संग्रहीत है जो केवल सिस्टम के लिए सुलभ है। यदि आप पासवर्ड जानते हैं, तो आप इसका हैश उत्पन्न कर सकते हैं; लेकिन आप हैश से पासवर्ड को रिस्टोर नहीं कर सकते। यही कारण है कि हैशिंग फ़ंक्शन को वन-वे फ़ंक्शंस के रूप में भी जाना जाता है। जब यूजर सिस्टम में लॉग इन करता है, तो पासवर्ड इस प्रकार वेरीफाई होता है:

- यूजर एक टेक्स्ट पासवर्ड दर्ज करता है जिसे तब हैश किया जाता है।
- परिणामी हैश की तुलना SAM रजिस्ट्री में संग्रहीत संदर्भ हैश से की जाती है।
- यदि हैश मेल खाता है, तो दर्ज किया गया पासवर्ड सही माना जाता है।

मूल पासवर्ड को उसके हैश से रिस्टोर करने का सबसे प्रभावी तरीका क्या है? हम इस विशाल विषय पर लेखों की एक अलग श्रृंखला समर्पित करेंगे। अब हम कुछ अलग मुद्दे पर चर्चा करेंगे। अर्थात्: क्या उस यूजर का मूल टेक्स्ट पासवर्ड प्राप्त करने का कोई तरीका है जिसने अपने अकाउन्ट में लॉग इन किया है? इस प्रश्न का उत्तर हमेशा अकादमिक रूप से निश्चित रहा है: ऐसा नहीं है, क्योंकि यूजर द्वारा दर्ज किया गया टेक्स्ट पासवर्ड वेरीफाई होने के बाद मिटा दिया जाता है, और उसके बाद केवल उसके हैश का उपयोग किया जाता है। यही सिद्धांत हमें विश्वास दिलाएगा। फिर भी यह सिद्धांत व्यावहारिक रूप से इतना कठिन नहीं है, क्योंकि यह पता चलता है कि मूल पासवर्ड को रिस्टोर किया जा सकता है ... इसके लिए प्रतीक्षा करें ... सिस्टम में कई अलग-अलग स्थानों से! उदाहरण के लिए, यकीनन सबसे शक्तिशाली पासवर्ड ऑडिट एप्लिकेशन, विंडोज पासवर्ड रिकवरी, विभिन्न तरीकों का उपयोग करके मूल टेक्स्ट पासवर्ड को रिस्टोर और डिक्रिप्ट कर सकता है:

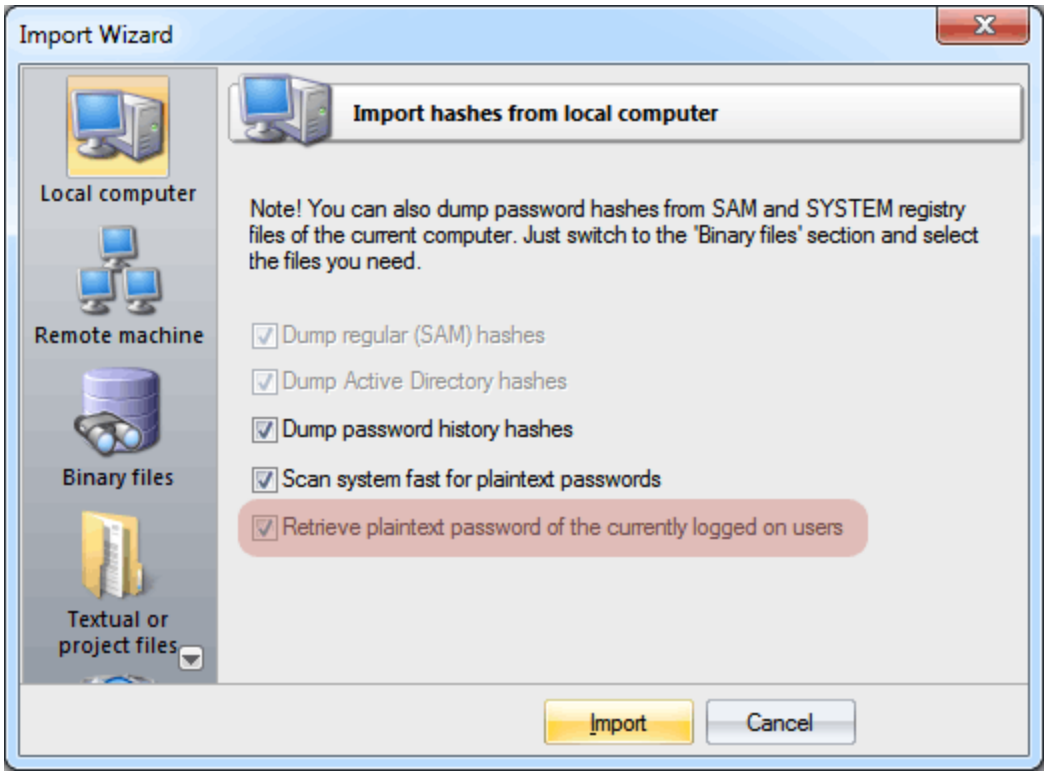
- एक साधारण सिस्टम मेमोरी डंप जनरेट करके Windows 2000 में एक अबाधित यूजर पासवर्ड आसानी से प्राप्त किया जा सकता है।
- HKLM रजिस्ट्री ट्री में, पुराने Windows वर्जन ऑटोमेटिक सिस्टम लॉगऑन के लिए पासवर्ड संग्रहीत करते थे यदि संबंधित विकल्प सक्षम किया गया था।
- LSA रहस्य। यह एक खुला रहस्य है (टॉटोलॉजी का बहाना) कि LSA रहस्य ऑटोमेटिक लॉगऑन के लिए व्यक्तिगत डेटा भी संग्रहीत करते हैं। कुछ मामलों में, मूल प्लेनटेक्स्ट पासवर्ड को रहस्य में सहेजा जाता है, भले ही ऑटोमेटिक सिस्टम लॉगऑन विकल्प सक्षम न हो। यह एक ज्ञात समस्या है जिससे Microsoft कई वर्षों से जूझ रहा है। हमारी टीम ने पाया है कि यह विंडोज 8 के बीटा वर्जन में भी मौजूद है।
- रहस्य कुछ सिस्टम अकाउन्ट के साथ-साथ लॉन्च की गई सेवाओं के टेक्स्ट पासवर्ड संग्रहीत करते हैं।
- यदि रिवर्स एन्क्रिप्शन विकल्प सक्षम है, तो प्लेनटेक्स्ट यूजर पासवर्ड एक डोमेन में संग्रहीत किया जा सकता है।
- विंडोज 8 के बीटा वर्जन में, प्लेनटेक्स्ट यूजर पासवर्ड को विंडोज वॉल्ट से आसानी से निकाला जा सकता है। आइए आशा करते हैं कि विंडोज 8 के अंतिम वर्जन में पासवर्ड सुरक्षा को बढ़ाया जाएगा।
- एक पासवर्ड रीसेट डिस्क (यदि कोई बनाई गई है) का उपयोग यूजर पासवर्ड को डिक्रिप्ट (विशेष रूप से डिक्रिप्ट, रीसेट नहीं) करने के लिए किया जा सकता है, जो इस मामले में रजिस्ट्री में एन्क्रिप्टेड रूप में संग्रहीत किया जाता है, जबकि डिक्रिप्शन की रीसेट डिस्क पर संग्रहीत होती है।




चित्र 1. पासवर्ड रीसेट डिस्क का उपयोग करके यूजर के प्लेन-टेक्स्ट पासवर्ड को डिक्रिप्ट करना

अब हम सबसे महत्वपूर्ण भाग पर आते हैं। यह पता चला है कि Windows XP से शुरू होने वाले सभी विंडोज वर्जनो में, लॉग-इन यूजर का टेक्स्ट पासवर्ड, जो कि कुछ प्रमाणीकरण प्रोटोकॉल, जैसे कि WDigest या TsPkg द्वारा उपयोग किया जाता है, को ब्लॉक साइफर का उपयोग करके सिस्टम मेमोरी में एन्क्रिप्ट किया जाता है, और इसलिए डिक्रिप्ट किया जा सकता है! विंडोज पासवर्ड रिकवरी का नया वर्जन यथार्थवादी मिशन के बावजूद इस गैर-तुच्छ के साथ सामना कर सकता है। आपके सिस्टम का एक सामान्य सुरक्षा ऑडिट चलाने के लिए, कंप्यूटर एडमिनिस्ट्रेटर के लिए यह पर्याप्त है कि वह एप्लिकेशन लॉन्च करे और पासवर्ड का स्थानीय आयात करने का प्रयास करे, और उसके परिणामों के आधार पर उचित निष्कर्ष निकाले।

विंडोज़ प्लेन टेक्स्ट पासवर्ड रिकवर करना




चित्र 2. यूजर लॉगऑन पासवर्ड रिकवर करना

आपके पीसी की सुरक्षा बढ़ाने के लिए, हम उस विकल्प को इनेबल करने की अनुशंसा करते हैं जिसके द्वारा SYSKEY को स्टार्टअप डिस्क पर संग्रहीत किया जाता है या SYSKEY बूटअप पासवर्ड का उपयोग किया जाता है। हालांकि यह पहले से लॉग-इन किए गए यूजर के पासवर्ड के डिक्रिप्शन को असंभव नहीं बनाएगा, यह आपके कंप्यूटर तक भौतिक पहुंच को रोक देगा, भले ही कोई संभावित घुसपैठिया आपके लॉगऑन पासवर्ड पर अपना हाथ पाने का प्रबंधन करता हो।