KMU AWARE
AWARENESS IM MITTELSTAND

# Leitfaden für Sensibilisierungs-Events zum Thema „sichere Pass-wörter“

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Partner

SECUSO SECURITY · USABILITY · SOCIETY

more security. usd

# Inhaltsverzeichnis

# 1 Einleitung

Passwörter begleiten uns in der digitalen Welt auf Schritt und Tritt. Sie ermöglichen es uns über große Distanzen hinweg auf verschiedenste Inhalte zuzugreifen, sei es auf Webseiten oder im Intranet eines Unternehmens. Leider wählen Benutzer Ihre Passwörter häufig in einer vorhersehbaren Weise. Dies kann zu signifikanten Sicherheitsproblematiken führen.
Oftmals ist es Mitarbeitern nicht bewusst, wie einfach Ihre Passwörter für einen Angreifer zu brechen sind. Dieser Leitfaden erklärt wie Sie professionelle Angriffstechniken auf einfache Weise in Ihrem Unternehmen vorzuführen und die Sicherheit von Passwörtern vor Publikum darzustellen. Dazu stellen wir Ihnen eine spezielle Software (pwRecon) zur Verfügung. Diese erfüllt zwei Zwecke. Zum einen wurde sie vorkonfiguriert, um realistische Angriffe durchzuführen und sie dabei durch einfach zu bedienendes Interface zu unterstützen. Zum anderen können die Mitarbeiter damit die eigenen Passwörter am eigenen Rechner überprüfen, sodass individuelle Erfahrungen mit dem Thema Passwortsicherheit gemacht werden können, ohne dabei die Sicherheit der IT-Infrastruktur Ihres Unternehmens zu gefährden. Dieser Leitfaden enthält dabei alles was sie brauchen, um den Event durchführen zu können. Im Detail behandelt der Leitfaden die folgenden Themen:

- Welche Ziele der Mitarbeitersensibilisierung können durch den Einsatz dieses Leitfadens erreicht werden
- Vorstellung und Benutzung der Software *pwRecon*
- Hinweise und Anregungen für die Planung und Ausgestaltung eines Events zum Thema „Sichere Passwörter“

# 2 Ziele der Mitarbeitersensibilisierung

## 2.1 Ziel 1: Einfaches Durchführen des Events zum Thema „sichere Passwörter“

Mitarbeiter sollen durch die Vorführung von erfolgreichen Angriffen auf komplex erscheinende Passwörter sensibilisiert werden. Das Ziel des Events ist es Interesse zu wecken und die Mitarbeitern zu sensibilisieren.

## 2.2 Ziel 2: Mitarbeitern ohne Sicherheitsrisiko erlauben selbst konkrete Erfahrungen im Bereich „sichere Passwörter“ zu sammeln

Zusätzlich zur öffentlichen Vorführung sollen die Mitarbeiter dazu motiviert werden die eigenen Passwörter zu überprüfen und so nicht angemessen sichere Passwörter zu identifizieren ohne dass die Sicherheit der IT-Infrastruktur gefährdet wird.

# 3 Die Software *pwRecon*

Zur Durchführung des Events zum Thema „sichere Passwörter“ stellen wir Ihnen die eigens für diesen Zweck entwickelte Software pwRecon (PassWord RECOvery for Non-experts) zur Verfügung, welche auf der bekannten Passwort-Wiederherstellungssoftware Hashcat aufbaut und diese für die durchgeführten Angriffe nutzt. Diese Software besitzt zwei primäre Einsatzzwecke:

1. Sie erlaubt es Ihnen realistische Angriffe auf Passwörter durchzuführen. Die Software ist entsprechend des Standes der Technik vorkonfiguriert. Damit lassen sich Passwörter vor Publikum auf einfache Weise auf Ihre Sicherheit überprüfen.
2. Sie erlaubt es auch unerfahrenen Mitarbeitern einzelne Passwörter zu überprüfen ohne dabei die Sicherheit des Systems, auf dem sie arbeiten, oder der Services, die sie benutzen, zu gefährden.

In diesem Kapitel werden zunächst die Software vorgestellt sowie Installationshinweise gegeben. Danach werden die verschiedenen Betriebsmodi der Software vorgestellt.

## 3.1 Vorstellung der Software *pwRecon*

pwRecon bietet ein graphisches Benutzerinterface für das Profi-Kommandozeilen-Tool *Hashcat*. Dabei übernimmt pwRecon die Konfiguration dieses Profi-Tools automatisch für Sie. Da somit alle Fähigkeiten des Profi-Tools genutzt werden können, erlaubt dies realistische Angriffe durchzuführen. Aber keine Sorge, alle diese Fähigkeiten werden automatisch für Sie konfiguriert. In Abbildung 1 sehen Sie das Interface von pwRecon.

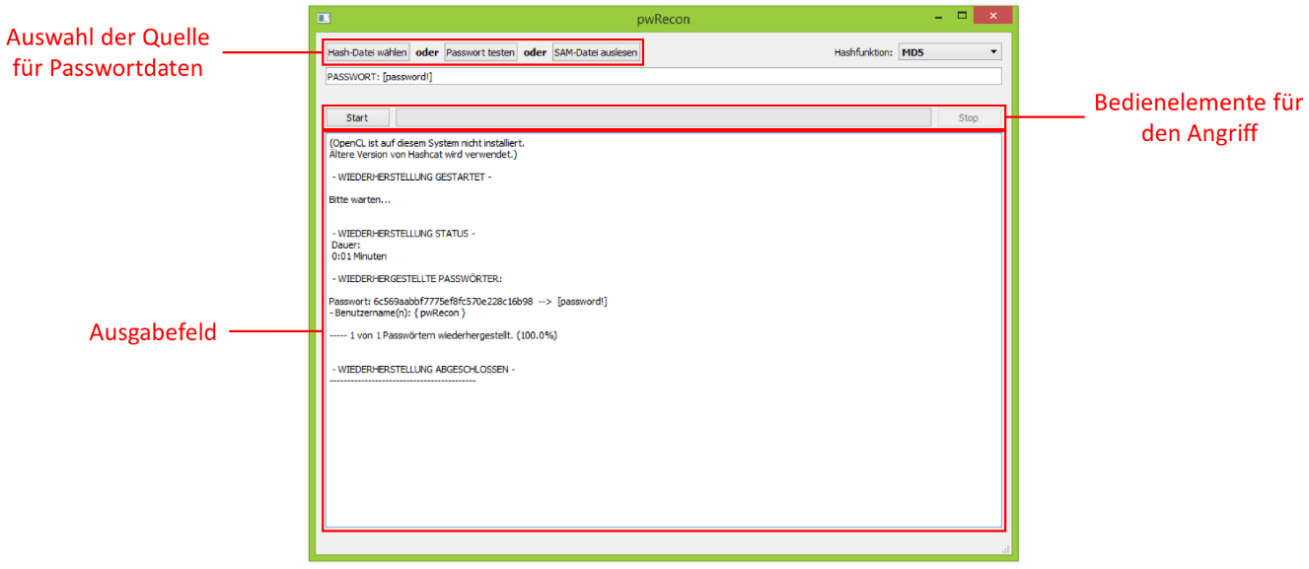



*Abbildung 1 - Das Interface der Software pwRecon*

Das Interface der Software ist in drei Bereiche eingeteilt, die im Folgenden besprochen werden: der Auswahl der Quelle für die Passwortdaten, die Bedienelemente für den Angriff und das Ausgabefeld zur Anzeige der Ergebnisse.

Als Quelle für die Passwortdaten stehen drei Optionen zur Verfügung. Die erste Option „Select Hash File“ ist für den Einsatz beim Testen von vielen Passwörtern gedacht. Das genaue Vorgehen in Bezug auf diese Option wird in Abschnitt 0 genauer erklärt. Die zweite Option „Test Password“ sowie die dritte Option „Scan SAM file“ sind für den Einsatz von den einzelnen Mitarbeitern direkt gedacht. Sie werden in Abschnitt 3.3 und 3.4 genauer vorgestellt.

Den zweiten Bereich stellen die Bedienelemente für den Angriff dar. Sie bestehen aus zwei Buttons zum Starten („Start Password Recovery“) und Stoppen („Stop“) des Angriffes sowie einem Aktivitätsindikator, welcher zwischen diesen beiden Buttons positioniert ist.

Das dritte Element stellt das Ausgabefeld dar. In ihm zeigt pwRecon alle Statusmeldungen an. In Abbildung 1 ist hier zu sehen, dass eine ältere Version von Hashcat verwendet wird, da keine dedizierte Grafikkarte für den Angriff zur Verfügung steht (eine der Profi-Fähigkeiten, die pwRecon automatisch für sie konfiguriert). Danach wird die übliche Ausgabe angezeigt. In diesem Fall wurde nur ein Passwort eingegeben (zweite Quellen-Option) und das Passwort („passwort“) binnen Sekunden gefunden.

Wenn Sie pwRecon starten, wird zunächst ein Dialog angezeigt. In diesem können Sie einstellen, ob Passwörter, die während eines Angriffes gefunden wurden, angezeigt werden sollen. Diesen Dialog sehen Sie in Abbildung 2.


*Abbildung 2 - In diesem Dialog können Sie wählen ob die gefundenen Passwörter angezeigt werden sollen.*

Beachten Sie, dass die Angriffe von pwRecon aufgrund der genutzten Verfahren sehr lange dauern können. Einen realen Angreifer stört es nicht, wenn sein Rechner mehrere Tage braucht um die Passwörter zu rekonstruieren. Da wir davon ausgehen, dass dies bei Ihnen nicht der Fall ist, sollten Sie den Angriff im Regelfall vorzeitig mit dem „Stop“-Button beenden. Wenn Sie an den technischen Details bezüglich der verwendeten Angriffe Interessiert sind, finden Sie diese als Anhang im Abschnitt 5.

### 3.1.1 Installationshinweise

Die Software muss nicht gesondert installiert werden. Sie laden diese als gepacktes Archiv (Dateiendung „zip“) von der Awareness Plattform herunter[1]. Nach dem Entpacken des Archivs können Sie pwRecon im entpackten Ordner durch einen Doppelklick auf die Datei „pwRecon.exe“ starten (je nach Konfiguration und Windows-Version kann es sein, dass die Dateiendung „.exe“ nicht angezeigt wird). Startet das Programm nach einem Doppelklick und es wird ein Fenster wie in Abbildung 1 angezeigt, müssen Sie nichts weiter tun,

[1] Alternativ steht die Software unter https://github.com/secuso/pwrecon zur Verfügung.

sondern können direkt mit Angriffen beginnen. Sollten Sie stattdessen die Fehlermeldung angezeigt bekommen, wie sie in Abbildung 1 zu sehen ist, müssen Sie noch eine benötigte Komponente auf Ihrem Rechner installieren: Microsoft Visual C++ 2015. Diese Komponente erhalten Sie am einfachsten direkt bei Microsoft[2].

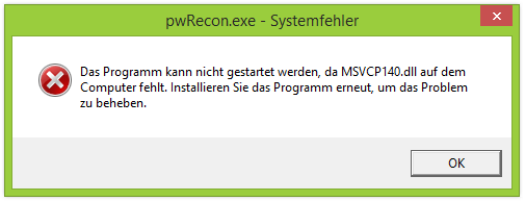



*Abbildung 3 - Wenn Sie diese Fehlermeldung sehen müssen Sie noch eine benötigte Komponente installieren.*

Wird im Ausgabefeld die Meldung „OpenCL not installed. Using older Hashcat version." angezeigt, können Sie optional noch OpenCL-Treiber-Komponenten für Ihr Betriebssystem installieren. Dies ist optional, beschleunigt die durchgeführten Angriffe jedoch je nach System erheblich und kann daher zu realistischeren Ergebnissen führen. Ist eine neuere Grafikkarte (Baujahr 2011 oder jünger) der Hersteller Nvidia[3] oder AMD[4] in Ihrem Rechner eingebaut, reicht es den aktuellsten Grafikkartentreiber von den Hersteller-Webseiten zu installieren. Auch bei neueren Prozessoren (Baujahr 2011 oder jünger) der Hersteller AMD[5] oder Intel[6] können Sie einfach die Treiber über die Webseite beziehen. Bei älteren Prozessoren und Grafikkarten gestaltet sich das Finden der passenden Treiber etwas aufwendiger und es wird empfohlen den Rat eines Fachkundigen zu suchen.

## 3.2 Betriebsmodus 1: Angriffe auf Listen von Passwörtern

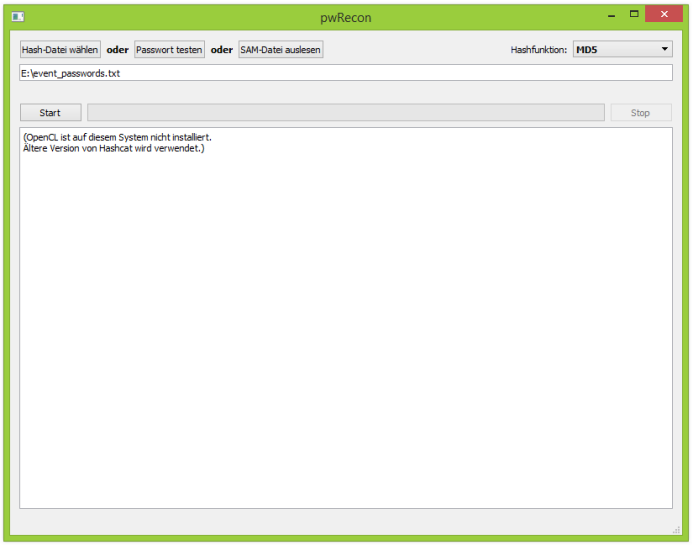
Dienstanbieter speichern Passwörter üblicherweise nicht als Klartext auf ihren Servern, sondern als sogenannte Hashes. Ein Hash ist ein verschleierter Wert, der auf einfache Weise für jedes Passwort berechnet werden kann. Aus dem Hash das Passwort zu berechnen ist nicht möglich. So kann ein Angreifer im Falle eines digitalen Einbruchs auf den Servern nur die Hashes entwenden und nicht die eigentlichen Passwörter. Um mehrere Passwörter in einem Angriff zu berücksichtigen, muss eine Liste solcher Passwort-Hashes in pwRecon geladen werden. Daraufhin kann der automatisierte Angriff gestartet werden. Im Folgenden wir dieser Prozess vollständig und Schritt für Schritt erklärt.

**1. Passwörter in pwRecon laden**

Eine Liste können Sie mit der Schaltfläche „Select Hash File" als Quelle für die Passwortdaten wählen. Wenn Sie darauf klicken, öffnet sich der übliche Datei-Auswahl-Dialog von Windows. In dem entpackten Verzeichnis finden Sie eine vorgefertigte Passwort-Liste, die Sie bei Events verwenden können. Wählen Sie dazu die Datei

[2] https://www.microsoft.com/de-de/download/details.aspx?id=48145
[3] http://www.nvidia.de/Download/index.aspx?lang=de
[4] https://support.amd.com/de-de/download
[5] http://developer.amd.com/tools-and-sdks/opencl-zone/
[6] https://software.intel.com/en-us/articles/opencl-drivers

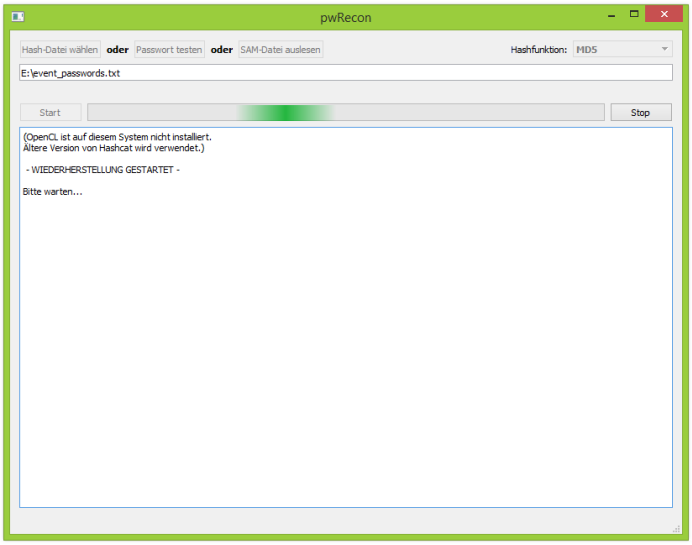
„event_passwords.txt“ aus. Als nächstes müssen Sie oben links den „Hash Type“ auf „MD5“[7]. Danach sollte das Interface von pwRecon wie folgt aussehen:




Als Quelle für die Passwortdaten wird in der Textzeile oben in pwRecon der Pfad zu der von Ihnen spezifizierten Passwort-Liste angezeigt.

### 2. Starten des Angriffs

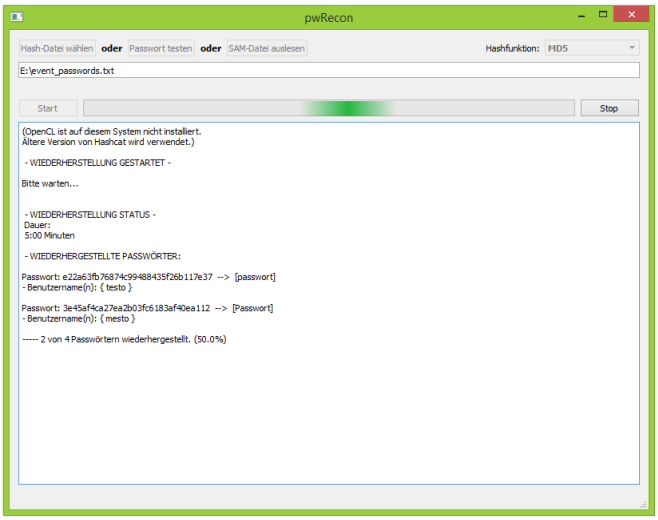
Danach starten Sie den Angriff durch einen Klick auf den Button „Start Password Recovery“. Der Angriff läuft im Hintergrund. Alle 5 Minuten (und sobald alle Passwörter gefunden sind) gibt pwRecon eine Statusmeldung im Ausgabefeld aus.




[7] Beachten Sie: Die mitgelieferte Datei verwendet zur Verschleierung der Passwörter den Hash-Typ MD5. Dieser Hash-Typ ist schnell zu berechnen und daher gut für den Event geeignet, für Produktiv-Systeme ist er jedoch ungeeignet. Dort sollten stattdessen immer sicherere Alternativen verwendet werden: z.B. SHA-256, SHA-512 oder bcrypt.

**3. Interpretation der Ergebnisse**

Ist der Angriff durch pwRecon erfolgreich, wird das Ergebnis im Ausgabefeld angezeigt. Zu diesem Ergebnis gehört die benötigte Zeit um das Passwort zu finden sowie das Passwort selbst:

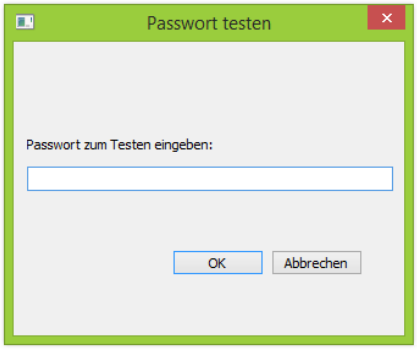



Je nachdem, wie sicher die Passwörter in der Passwort-Liste sind und wie stark die Hardware auf der sie den Angriff ausführen, kann es sein, dass der Angriff eine lange Zeit in Anspruch nehmen würde. pwRecon wird alle 5 Minuten eine Statusmeldung ausgeben. Solch eine Statusmeldung sehen sie im oben abgebildeten Interface. Sie können den Angriff jederzeit mit einem Druck auf den „Stop“-Button unterbrechen und beenden, sobald die gewünschte Anzahl an Passwörtern gefunden wurde oder die zur Verfügung stehende Zeit abgelaufen ist. Beachten Sie: Bei der Benutzung der Passwort-Liste „event_passwords.txt“ ist es insbesondere so, dass sie der Anschauung halber einige Passwörter enthält, bei denen ein erfolgreicher Angriff eine sehr viel Zeit benötigt.

## 3.3 Betriebsmodus 2: Direkte Eingabe eines Passwortes

**1. Passwörter in pwRecon laden**

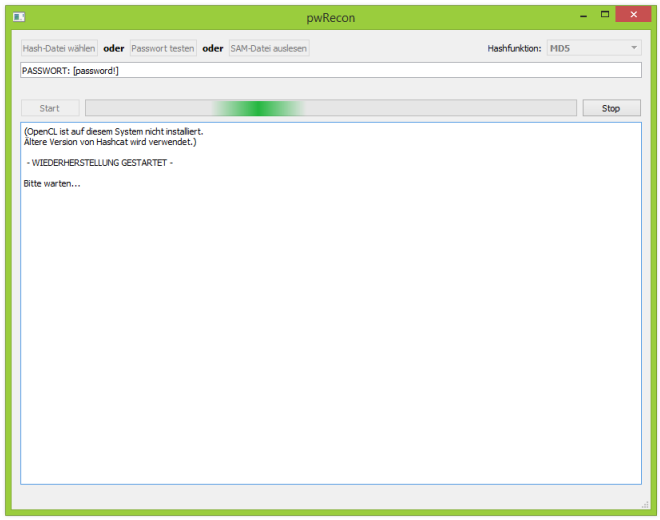
Ein einzelnes Passwort können Sie mit der Schaltfläche „Test Password“ als Quelle für die Passwortdaten wählen. Daraufhin öffnet sich ein Dialog, in den Sie das Passwort eingeben können und mit einem Klick auf den „OK“-Button den Angriff starten (den Hash Type müssen Sie im Gegensatz zu Betriebsmodus 1 nicht selbst wählen, dies geschieht hier automatisch für Sie):



*Achtung*: Wenn Sie bei Programmstart gewählt haben, dass die Passwörter im Klartext angezeigt werden sollen, wird dies auch während der Eingabe und nach dem Klicken auf „OK“ in pwRecon im Klartext angezeigt. Seien Sie vorsichtig, dass Sie niemand bei der Verwendung der Software beobachtet.

### 2. Starten des Angriffs

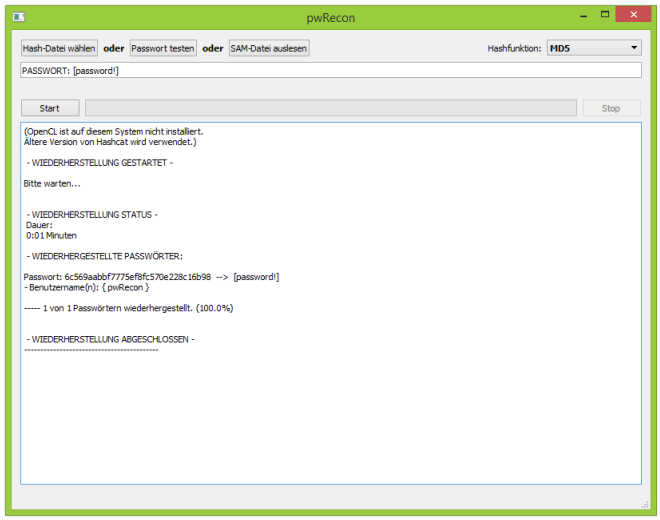
Nach der Passworteingabe startet pwRecon den Angriff automatisch. Es sind keine weiteren Aktionen durch Sie nötig. Dies wird im Aktivitätsindikator durch einen laufenden Balken angezeigt.




Als Quelle für die Passwortdaten wird in der Textzeile oben im Programm das von Ihnen eingegebene Passwort angezeigt.

### 3. Interpretation der Ergebnisse

Ist der Angriff durch pwRecon erfolgreich, wird das Ergebnis im Ausgabefeld angezeigt. Zu diesem Ergebnis gehört die benötigte Zeit um das Passwort zu finden sowie das Passwort selbst, wenn während des Programmstarts die entsprechende Option gewählt wurde:

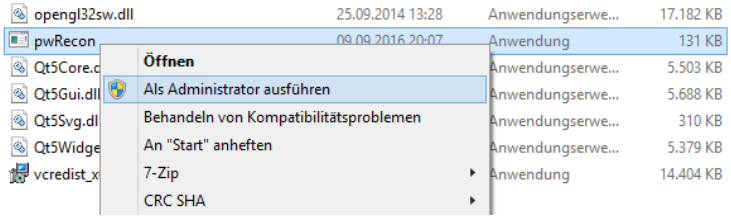


Je nachdem, wie sicher das Passwort ist, das angegriffen wird, kann es sein, dass der Angriff eine lange Zeit in Anspruch nehmen würde. pwRecon wird alle 5 Minuten eine Statusmeldung ausgeben. Sie können den Angriff jederzeit mit einem Druck auf den „Stop“-Button unterbrechen und beenden.

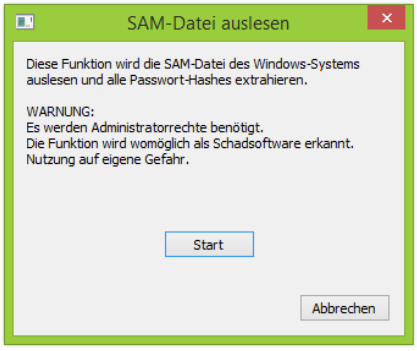
## 3.4 Betriebsmodus 3: Passwortdaten aus dem laufenden System

**1. Passwörter in pwRecon laden**

pwRecon erlaubt es die Passwortdaten für lokale Benutzer direkt aus dem laufenden System zu extrahieren und diese als Quelle zu nutzen. Dafür muss pwRecon jedoch mit Administratorrechten ausgeführt werden. Starten Sie pwRecon daher NICHT über einen Doppelklick, sondern machen Sie einen Rechtsklick und wählen Sie aus dem erscheinenden Menü den Punkt „Als Administrator ausführen“ und bestätigen Sie dies im darauffolgenden Sicherheitsdialog von Windows noch einmal.



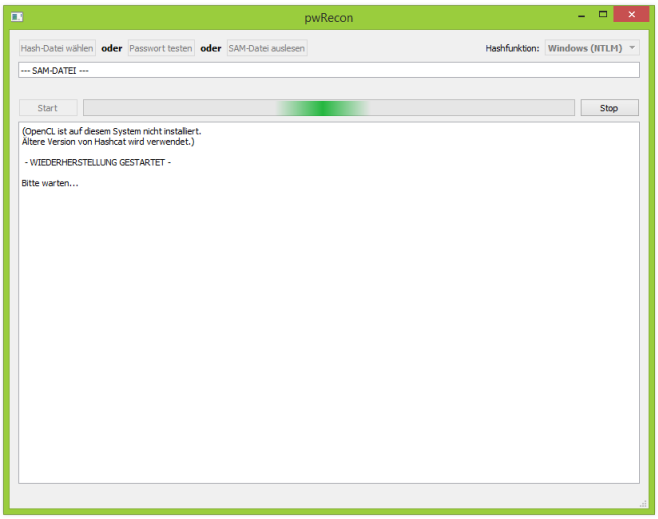

Danach wird sich das Interface von pwRecon wie gewohnt öffnen. In Windows enthält die geschützte Systemdatei „SAM“ die Passwortdaten. Zum Auslesen der Passwortdaten des laufenden Systems klicken Sie auf den Button „Scan SAM file“. Daraufhin wird sich ein Dialog öffnen.




Mit einem Klick auf den „Start“-Button starten Sie den Extraktionsprozess. Dieser kann eine Weile dauern, in der pwRecon nicht auf Eingaben reagiert. Es ist möglich, dass Sie Ihr Anti-Virus-Programm nun vor pwRecon warnen wird. Dies ist ganz normal und weist nicht auf eine tatsächliche Infektion hin, sondern ist eine Reaktion auf die Extraktion der Passwortdaten, was üblicherweise auch von Schadsoftware versucht wird. Daher können Sie Warnungen diesbezüglich ignorieren. Ist die Extraktion erfolgreich, schließt sich der Dialog automatisch. Als Quelle für die Passwortdaten wird in der Textzeile oben in pwRecon „SAM DATEI“ angezeigt.

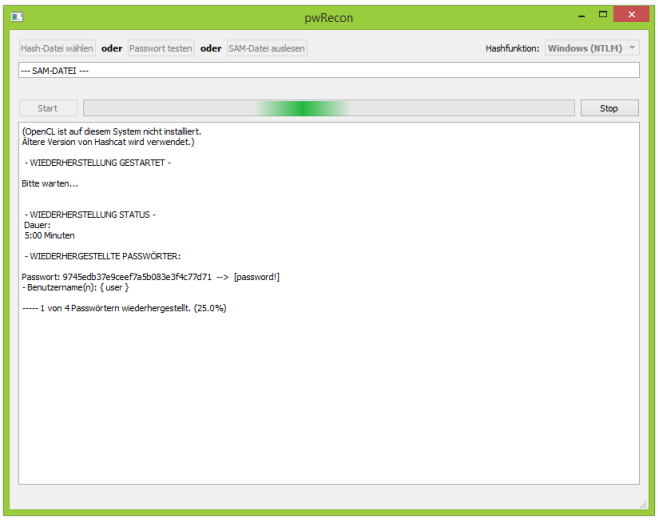
## 2. Starten des Angriffs

Nach der erfolgreichen Extraktion startet pwRecon den Angriff automatisch. Es sind keine weiteren Aktionen durch Sie nötig (auch hier müssen Sie den Hash Type nicht selbst wählen, dies geschieht automatisch für Sie). Die Durchführung des Angriffs wird im Aktivitätsindikator durch einen laufenden Balken angezeigt.




## 3. Interpretation der Ergebnisse

Ist der Angriff durch pwRecon erfolgreich, wird das Ergebnis im Ausgabefeld angezeigt. Zu diesem Ergebnis gehört die benötigte Zeit, um das Passwort zu finden, sowie das Passwort selbst:




Je nachdem, wie sicher die Passwörter in der SAM-Datei sind, kann es sein, dass der Angriff eine lange Zeit in Anspruch nehmen würde. pwRecon wird alle 5 Minuten eine Statusmeldung ausgeben. Solch eine Statusmeldung sehen sie im oben abgebildeten Interface. Sie können den Angriff jederzeit mit einem Druck auf den „Stop“-Button unterbrechen und beenden, sobald das Passwort des Benutzerkontos bzw. der gewünschten Benutzerkonten gefunden wurde.

# 4 Planen und Ausgestalten eines Events

Bei der Ausgestaltung des Events gibt es einige Punkte zu beachten. Im Folgenden werden wir Hinweise zu diesen Punkten geben.

- Entscheiden Sie sich frühzeitig, welche **Betriebsmodi** von pwRecon Sie in den Event integrieren wollen. Der Angriff auf ganze Listen von Passwörtern (vgl. Abschnitt 3.2) ist vor allem für Vorführungen vor Publikum gut geeignet, benötigt aber am besten potente Hardware. Die zur Verfügung gestellte Liste für einen solchen Angriff enthält Passwörter die schnell zu finden sind und Passwörter, bei denen ein erfolgreicher Angriff sehr lange dauern würde. Diese Übersicht kann den Mitarbeitern des Unternehmens ein Gefühl dafür vermitteln, wie angemessen sichere Passwörter aussehen. Der Angriff auf ein einzelnes Passwort (vgl. Abschnitt 3.3) eignet sich vor allem dafür, dass Mitarbeiter eigene Passwörter testen. Das Einlesen der Passwortdaten aus dem laufenden System (vgl. Abschnitt 3.4) eignet sich nur in speziellen Situationen, da Mitarbeiter Administratorrechte auf dem Rechner benötigen, um diesen Modus zu benutzen. Oftmals kann eine Kombination der ersten beiden Betriebsmodi sinnvoll sein: Zuerst eine Live-Demo und dann können die Mitarbeiter selbst Hand anlegen und Angriffe austesten.
- Zur Planung sollte auch das frühzeitige Abklären von **Voraussetzungen** zählen. Hierzu zählt insbesondere ein entsprechend ausgestatteter Raum für eine Vorführung vor Publikum. Als Mindestausstattung sollte (a) ein Rechner auf dem pwRecon vorbereitet wurde (vgl. Abschnitt 0), (b) ein Beamer mit Projektionsfläche oder ein großer Bildschirm, sodass das Publikum die Anzeige gut einsehen kann und (c) passende Sitzgelegenheiten vorhanden sein. Sollen die Mitarbeiter selbst Hand anlegen, müssen auch hierfür Gelegenheiten geschaffen werden (z.B. durch bereitgestellte Laptops/Rechner oder durch Bereitstellung der Software für die Benutzung auf dem eigenen Rechner).
- Achten Sie auf eine klare Kommunikation passender **Verhaltensweisen**. Insbesondere ist darauf hinzuweisen, dass pwRecon gefundene Passwörter im Klartext anzeigen kann und einzeln eigegebene Passwörter im Feld zur Auswahl der Passwortquelle im Klartext angezeigt werden. Daher sollten die Teilnehmer untereinander Diskretion wahren.
- Machen Sie vor dem eigentlichen Event einen **Testlauf**, in dem Sie sich mit pwRecon vertraut machen. So vermeiden Sie Wartezeiten des Publikums während des Events und können mögliche Fehlerquellen frühzeitig erkennen.
- Planen Sie eine angemessene **Nachbereitung** mit ein. Wenn Sie die zur Verfügung gestellte Passwort-Liste „event_passwords.txt“ verwenden, wird es Passwörter geben, die nicht erraten werden können. Eine Liste aller Passwörter finden Sie in der (auch zur Verfügung gestellten) Datei „event_passwords_plaintext.txt“. Hier sollten Sie auch die angemessen sicheren Passwörter vorstellen, die nicht geknackt werden konnten. Zudem sollten Sie auf jeden Fall weiterführende Materialien anbieten, falls Mitarbeiter im Rahmen des Events nicht angemessen sichere Passwörter identifizieren und diese ändern wollen. Diesen Mitarbeitern muss eine Möglichkeit geboten werden sich weitergehend zu informieren. Dazu können Sie z.B. unsere Schulungsmaterialien verwenden.

# 5 Beschreibung der Angriffsverfahren

pwRecon verwendet drei Angriffstechniken in sequentieller Reihenfolge. Zunächst wird ein Wörterbuch häufig verwendeter Passwörter getestet. Dieses Wörterbuch beinhaltet Passwörter aus Hacks bekannter Webservices, die im Internet veröffentlicht wurden sowie eine Vielzahl deutscher Wörter (um der Ausrichtung auf deutsche KMUs zu verstärken).
Danach werden alle Einträge des Wörterbuchs erneut getestet, jedoch mit der zusätzlichen Anwendung von sogenannten Mangling-Rules. Diese Mangling-Rules verändern die Einträge des Wörterbuchs, indem Sie beliebte Techniken zur Erstellung von Passwörtern imitieren (z.B. anhängen eines Sonderzeichens wie „!“ oder Ersetzen von Buchstaben durch Sonderzeichen wie etwa „a“ durch „@“ oder „4“.
Die dritte und letzte Technik verwendet das Wörterbuch nicht. Sie ist ein sogenannter Brute-Force-Angriff (engl.: Brute Force = Rohe Gewalt). Bei einem solchen Brute-Force-Angriff werden alle möglichen Kombinationen an Buchstaben und Zahlen durchprobiert. Ein solcher Angriff kann theoretisch jedes Passwort finden. Allerdings dauert dies in der Praxis oft zu lange, je nachdem wie sicher das angegriffene Passwort ist.