Aufgaben -

Passwortwiederherstellung

W3WI_SE411 - Forschungsseminar Informatik / Advanced Practical IT Security

Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw-mannheim.de, Raum 149B

Version: 23SEB

Einführung

Ziel dieser Aufgabe ist es einen ersten Einblick in die Wiederherstellung von Passwörtern zu erhalten. Die Komplexität der Aufgaben steigt mit der Anzahl der erreichbaren Punkte. Komplexität kann sich direkt auf die Passwörter beziehen oder auf die notwendigen Schritte, die ggf. im Vorfeld zu unternehmen sind. Dies kann ggf. auch die Recherche nach weiteren Tools umfassen!

Der Einsatz von Kali Linux ist empfehlenswert, da dort sehr viele Tools (insbesondere Hashcat und John) schon installiert sind oder vgl. trivial nachinstalliert werden können. Unter Kali finden Sie interessante (Basis-)Wörterbücher an folgenden Stellen:

```
/usr/share/dict/wordlist-probable.txt
/usr/share/dict/cracklib-small
/usr/share/wordlist/rockyou.txt
/usr/share/wordlists/metasploit/*.txt
```

Achtung!

Auch in Kali Rolling sind nicht immer alle Tools auf dem allerneuesten Stand bzw. direkt verfügbar.

Achtung!

Es ist möglich, dass die Verwendung von Hashcat und/oder John nicht (direkt) möglich ist.

Bewertung

Aufgabe	Punkte
Arbeitsumgebungsbeschreibung	1
Number<X>.od?	4
Hurdle.jpg.7z	8
Star.pdf	9
MySheet.numbers	8
JavaHashcodes.txt	6
Max Müller.kdbx	7
Passwords.pages	7
	∑ 50

!! Wichtig

Es ist lediglich erforderlich 25 Punkte zu holen, um diesen Teil mit 100% Erfolg gewertet zu bekommen.

Überschüssige Punkte können im Allgemeinen nicht übertragen werden.

Für jedes Passwort, das sie exklusiv wiederherstellen, gibt es einen übertragbaren Bonuspunkte. D. h., sie können somit zum Beispiel mit 110% abschließen.

Bemerkung

Im Rahmen der Passwortwiederherstellung kann es immer mal wieder vorkommen, dass Ihnen eine Aufgabe mehr oder weniger liegt. Sie sollten deswegen die Punkte erst einmal außen vor lassen.

Bemerkung

Die aufgewandte Rechenzeit hat auf die Bepunktung keine Einfluss. D.h. im Falle eines „wenig durchdachten“ Wiederherstellungsversuchs kann es durchaus sein, dass sie Tage oder ggf. sogar Wochen brauchen bzw. bräuchten.

Abgaben

Beschreibung der Arbeitsumgebung [1 Punkt]

Eine kurze Beschreibung Ihrer Arbeitsumgebung: D. h. die eingesetzte Hardware und Software (OS, ob virtualisiert oder nicht ggf. inkl. Konfiguration der VM, eingesetzte Shell)

Lösungswegbeschreibungen

Für jede Aufgabe müssen Sie Ihren Weg genau beschreiben, da dieser essentieller Bestandteil der Prüfung ist.

Vorbereitungsschritte

01	[ggf.] Schritte zur Extraktion des Hashes
02	[ggf.] Schritte, die zur Aufbereitung des Hashes unternommen wurden
03	[ggf.] verwendete Quellen für (externe) Wörterbürcher
04	[ggf.] Schritte, die zur Erstellung des zum Angriff benutzten Wörterbuchs unternommen wurden
05	[ggf.] Schritte, die notwendig waren, um das notwendige Tooling bereitzustellen

Eigentlicher Angriff

01	den oder die Schritte, die zum Angriff auf den oder die „Hashes“ durchgeführt wurden
02	das oder die wiederhergestellten Passworte
03	Dauer der Suche nach dem Passwort (Dies ist die Zeit, die gebraucht wurde, um ihre Passwortkandidaten zu testen; d.h. die Zeit, die zum Beispiel Hashcat benötigt hat. Eine grobe Angabe in Minuten ist ausreichend.)

!! Wichtig

Aus Ihrer Beschreibung muss direkt nachvollzogen werden können, wie Ihr Vorgehen war. D. h. es sollte ggf. direkt möglich sein den Angriff in der beschriebenen Weise nachvollziehen zu können.

Ist nicht nachvollziehbar wie Sie das Passwort ermittelt haben, dann gibt es *nur auf das Passwort keine Punkte*.

Dokumentationstiefe

Dokumentieren Sie ggf. die Shellcommandos oder auch Skripte, die sie verwendet haben. Eine Prosaschreibung ist nicht ausreichend. Orientieren Sie sich ggf. an dem

entsprechenden Foliensatz zur Passwortwiederherstellung.

Nicht-standard Werkzeuge

Entwickeln Sie selber Tools/Skript, dann dokumentieren Sie diese (d. h. den Quellcode).

Laden und kompilieren Sie Skripte aus dem Internet, dann dokumentieren Sie die Quellen und ggf. die Schritte, um das Skript zu nutzen.

Wiederholung von Schritten

Sollten Sie ein oder mehrere Schritte wiederholen, dann dokumentieren Sie dies entsprechend. Es ist insbesondere denkbar, dass Sie die Schritte bzgl. Erstellung von Wörterbüchern mehrfach durchführen mussten. Dies ist dann entsprechend zu dokumentieren.

Bemerkung

Bei den folgenden Aufgaben ist es immer das Endziel das bzw. die Passwörter wieder herzustellen. Es ist jedoch so, dass auch der Weg bewertet wird. D. h. der Großteil der Punkte kann auch dann erworben werden, wenn das Passwort nicht erfolgreich wiederhergestellt wurde. Es ist ggf. sogar theoretisch möglich die volle Punktzahl zu bekommen ohne ein Passwort erfolgreich wiederherzustellen.

Numbers<X> Datei [4 Punkte]

Bzgl. des Passwortes und des Hintergrundes sind keine Informationen vorhanden.
Es bleibt Ihnen nichts anderes übrig als allg. *Best Practices* anzuwenden.

!! Wichtig

Bearbeiten Sie nur die `Number<X>` Datei, die Ihnen zugewiesen wurde. Das Bearbeiten anderer `Number<X>` Dateien bringt keine Punkte.

!! Wichtig

Sollten Sie das Passwort Ihrer `Number<X>` nicht wieder herstellen können, dann - und nur dann - können Sie sich auch an der Datei `Poem.pages` versuchen. In diesem Falle ist aber auch die vollständige Dokumentation Ihrer Versuche und Herangehensweise bzgl. Ihrer `Number<X>` Datei mit abzugeben.

Hurdle.jpg.7z [8 Punkte]

Ihnen liegt eine verschlüsselte, komprimierte Datei zur Entschlüsselung vor. Glücklicherweise(?) konnten sie auf einem Datenträger eine gelöschte Datei wieder herstellen, die `Passworte.txt` hieß und die folgenden Daten beinhaltet.

```
Der Lauf
Der Flug
Der Gesang
Der Fund
Der Stand
```

6

Star.pdf [9 Punkte]

Ihnen liegt ein verschlüsseltes PDF vor. Aus anderen Fällen in dem Umkreis des Beschuldigten wissen Sie, dass diese eine starke Tendenz haben Passworte zu bauen, die aus großen deutschen Städten zusammengesetzt sind und ergänzt werden um Zeichen, die notwendig sind, um ggf. die Passwortpolicies Ihrer Standardapps zu erfüllen. In diesem Fall ist die Passwortpolicy der verwendeten App bekannt:

- mind. 2 Großbuchstaben
- mind. 2 Kleinbuchstaben
- mind. 4 Ziffern
- mind. 4 Sonderzeichen
- mindestlänge: 16 Zeichen

Sie wissen auch, dass die verwendeten Sonderzeichen praktisch immer: $,€ oder ! sind und in den Passworten häufig einfach wiederholt werden. Weiterhin werden fast immer aktuelle Jahreszahlen verwendet (z. B. 2023 etc.) und der allgemeine Aufbau scheint:

```
<Jahreszahl><Stadt1><Stadt2><Sonderzeichen>
```

zu sein.

MySheet [8 Punkte]

Basierend auf anderen Passworten, die sie in einem Notizbuch gefunden haben, gehen Sie davon aus, dass für das Passwort nur reguläre Buchstaben verwendet wurden und Worte mit der korrekten Groß-Kleinschreibung geschrieben werden (z. B. Frankfurt). Wörter scheint er ggf. zusammenzuziehen (z. B. HausMaus, AffeAffe, alleLieben). Darüber hinaus konnten Sie nur noch die Erkenntnisse gewinnen, dass alle Passworte mindestens 8 Buchstaben haben.

8

Java Hashcodes [6 Punkte]

In einer Software wurde fälschlicherweise Javas `hashcode()` Funktion für das Hashen der Passworte verwendet. Aus der Datenbank konnte eine Liste von Hashes extrahiert werden. Diese Werte sind in der Datei `JavaHashcodes` gespeichert.

Ihre Aufgabe ist die Wiederherstellung *aller* Passworte.

9

Max Müller [7 Punkte]

Ihre Aufgabe ist das Passwort für die Datei `Max Müller.kdbx` wiederherzustellen.

Sie haben zur Unterstützung Ihrer Tätigkeit eine Profilbeschreibung erhalten:
`Max Müller.md`.

10

Passwords.pages [7 Punkte]

Ihnen liegt die vielversprechend klingende Datei `Password.pages` vor.

Ihre Aufgabe ist die Wiederherstellung des Passwortes.