010 Passwortsicherheit (pwd)

In der heutigen Zeit müssen viele Benutzer mit einer Vielzahl von verschiedenen Accounts arbeiten, sei es der Offline-Account (z.B. Login am Arbeitsplatz oder Zuhause) oder Online-Account (z.B. Email-Dienste, Online-Shopping, Soziale Netzwerke etc.).

Bei der steigenden Anzahl an Accounts, die man managen muss, wird häufig der leichte Weg beschritten und dasselbe Passwort für eine Vielzahl von Accounts genutzt. Das alleine macht es einem Angreifer schon recht leicht. Noch schlimmer wird es, wenn das Passwort nicht mit Bedacht gewählt wurde und leicht zu erraten ist. Hat der Angreifer Kenntnis von dem Passwort erlangt, braucht es nicht mehr viel Mühe, die verschiedenen Accounts des Opfers zu kapern und für seine Zwecke zu missbrauchen.

Tools führen das sogenannte Passwort-Cracking vollautomatisch durch und haben bei einfachen Passwörtern eine hohe Erfolgswahrscheinlichkeit. Durch Wortlisten, ganzen Wörterbüchern mitsamt Anwendungsregeln oder auch mit Rainbow Tables erraten diese Tools das Passwort relativ effektiv.

Nutzen Sie für die folgenden Aufgaben, wenn erforderlich, die Tools **„John the Ripper“** und **„Ophcrack“**.

Aufgabe 1

Nennen Sie Maßnahmen, wie man es einem potenziellen Angreifer schwerer machen kann, das Passwort zu erraten.

Der Einsatz von Sonderzeichen, Groß- und Kleinbuchstaben und keiner Persönlichen Daten innerhalb

Aufgabe 2

Suchen Sie im Internet nach Tools für Wörterbuchangriffe. Welche On- bzw. Offline-Tools gibt es und welche Arten von Hashwerten können mit den jeweiligen Tools geknackt werden?

Offline: cowpatty (https://www.kali.org/tools/cowpatty/) generiert eine Hashfile und testet alles durch
Online: hydra (https://www.kali.org/tools/hydra/) (SSH)

Aufgabe 3

„John The Ripper“ ist als freie Version erhältlich. Erläutern Sie die Funktionsweise. Welche Algorithmen zur Hash-Berechnung beherrscht „John The Ripper“? Wie viele verschiedene Crack-Modi werden unterstützt? Nennen und erläutern Sie die Unterschiede.

Aufgabe 4

Welcher Schritt ist zunächst notwendig um auf Linux-Distributionen, die Passwörter in einer Shadow-Datei speichern, das Cracking der Passwortliste zu starten?

Aufgabe 5 - Praxis

Stellen Sie sich folgendes Szenario vor:

Sie haben durch einen schlecht gesicherten Account eines Users Zugriff auf ein System erlangt. Der User ist privilegiert und steht auf der sudo-Liste. Mit Hilfe des sudo-Befehls war es Ihnen möglich, die Inhalte der Dateien „/etc/passwd“ und „/etc/shadow“ in lokale Dateien zu kopieren. In der vorherigen Aufgabe haben Sie bereits einen Befehl recherchiert, mit dem Sie diese beiden Dateien für eine JTR-geeignete Datei zusammenführen können. Einen solchen schlecht gesicherten Account finden Sie möglicherweise auf ihrer GNS3-VM vor, auf die Sie auch direkt per SSH aus dem Kali-Linux zugreifen könnten. Um vollen Zugriff auf das System zu erlangen, wollen Sie nun das Passwort des root-Account cracken.

Loggen Sie sich dazu im GNS3-Client in das Kali-Linux ein und verwenden Sie „John The Ripper“ auf dem Terminal.

Starten Sie den Crackvorgang von der zusammengeführten Datei mit Hilfe der Wortliste „pwd.txt“. Die Wortliste liegt im Home-Verzeichnis. Beschränken Sie sich dabei nur auf den root-Account. Andere Passwörter sind nicht von Interesse! Wie lautet das Passwort von root? Wie lauten die Befehle, um das Passwort zu ermitteln?

Bemerkung: Das Root-Passwort wird für das nächste Praktikum benötigt!

Aufgabe 6

Mitunter kann der Vorgang zum Cracken per Brute-Force oder mit Wortlisten sehr lange dauern. Allerdings gibt es ein paar Möglichkeiten, in JTR das Cracken zu beschleunigen. Nennen Sie drei Methoden.

Aufgabe 7

Für Windows-LM-/-NTLM-Passworthashes gibt es eine effektivere und i.d.R. schnellere Methode das Klartext-Passwort herauszufinden - die Rainbow Tables.

Erklären Sie die Funktionsweise von Rainbow Tables. Welche Vorteile haben sie gegenüber Brute-Force- oder Wörterbuchattacken? Warum sind Rainbow Tables in der Regel effektiver?

Aufgabe 8

Die LM-/NTLM-Hashes von lokalen Benutzerkonten sind in einer SAM-Datenbank abgelegt. Wofür steht SAM und welche Funktion hat der Dienst? Kann man über die SAM-Datenbank auch Domain-Passwörter auslesen?

Aufgabe 9 - Praxis

Versuchen Sie nun das Passwort des Accounts 'Alice' von der VM 'win7-victim' mit dem Tool Ophcrack und einer Rainbow Table zu cracken. Laden Sie sich dazu zunächst die Rainbow Table 'vista free prohabilistic' von der Ophcrack-Webseite herunter (oder, falls die Verbindung zu langsam ist liegt die unter /root/ophcrack) und speichern Sie die Table im Ordner 'ophcrack/RainbowTables' im Home-Verzeichnis des Users 'root'.

In dem Ordner „ophcrack“ finden Sie außerdem einen Dump der SAM-Einträge (Security Accounts Manager) von der VM „win7-victim“.

Zum Cracken soll nur das Passwort von Alice betrachtet werden, ansonsten sind die Laufzeiten zu hoch! Hierzu kann bspw. nur ein Teil des SAM-Dump verwendet werden.

Starten Sie das Tool Ophcrack auf der Kommandozeile (ophcrack), laden Sie den SAM-Dump und versuchen Sie das Passwort des Accounts „Alice“ mit der heruntergeladenen Rainbow Table zu cracken.

Wie lautet das Passwort? Wie viel Zeit wurde benötigt?