Passwort Hacking: Vergleich von Brute-Force-Angriffen, Dictionary-Angriffen und Rainbow Tables zur Authentifizierungssicherheit

Seminararbeit

für die Prüfung zum

Bachelor of Science

des Studiengangs Informatik

an der

Dualen Hochschule Baden-Württemberg Lörrach

Marvin Obert

6. Juni 2023

Kurs	TIF21B
Ausbildungsfirma	VEGA Grieshaber KG, Schiltach
Wissenschaftlicher Betreuer	Prof. Dr. Hans Mustermann

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich meine Bachelorarbeit (bzw. Projektarbeit oder Seminararbeit) mit dem Thema:

Passwort Hacking: Vergleich von Brute-Force-Angriffen, Dictionary-Angriffen und Rainbow Tables zur Authentifizierungssicherheit

selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Lörrach, 15. Februar 2000

_____

Marvin Obert

Hinweis zum Umfang der Arbeit

Der Textteil der vorliegenden Arbeit - beginnend mit der Einleitung bis ausschließlich Quellenverzeichnis - umfasst 7 Seiten.

Kurzfassung

Hier beginnt die Kurzfassung ihrer wissenschaftlichen Arbeit…

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Einführung

> *„More companies are moving to new stronger technologies to authenticate user identities, like biometrics. Because it's just too easy for hackers to figure out usernames and passwords, like "password"" or 12345... 7. Those are some of my previous passwords. I've changed them since then."*
>
> Barack Obama[1]

In der heutigen Zeit sind Passwörter eine der grundlegendsten Methoden um Benutzer zu identifizieren. Allerdings ist die Komplexität der meisten Passwörter sehr gering und somit ist das Benutzernamen und Passwort erraten sehr leicht. Wie der ehemalige US-Präsident Barack Obama betont, haben Unternehmen erkannt, dass sie auf neue, stärkere Technologien umsteigen müssen, um die Identität von Benutzern zu authentifizieren, wie zum Beispiel biometrische Verfahren. Diese Authentifikationsmethoden sind angesicht der Passwörter des ehemalige Präsidenten ein deutlich stärkere und sichere Maßnahme.

1.2 Zieldefinition

Das Ziel dieser Seminararbeit besteht darin, eine umfassende Vergleichsanalyse ausgewählter Passwort-Hacking-Methoden durchzuführen. Dazu werden Brute-Force-Angriffe, Dictionary-Angriffe und Rainbow Tables im Hinblick auf Effizienz, Erfolgsrate und Ressourcenanforderungen untersucht. Zusätzlich erfolgt eine eingehende Untersuchung der Sicherheit des weit verbreiteten WLAN-Verschlüsselungsstandards WPA2 und der Diskussion möglicher Schutzmaßnahmen.

Um dieses Ziel zu erreichen, wird sowohl ein theoretischer Vergleich durchgeführt, bei dem eine Nutzwertanalyse erstellt wird, als auch ein praktischer Vergleich in einem konstruierten Testfall durchgeführt. Der praktische Vergleich ermöglicht eine Überprüfung der Wirksamkeit und Anwendbarkeit der verschiedenen Methoden.

[1] Nick Statt, 2015, Vgl.

Durch diese umfassende Herangehensweise soll ein fundiertes Verständnis für die Stärken und Schwächen der einzelnen Passwort-Hacking-Methoden gewonnen werden, um Empfehlungen für den Schutz vor solchen Angriffen abzuleiten. Die Kombination aus theoretischer Analyse und praktischer Anwendung ermöglicht eine ganzheitliche Betrachtung des Themas.

1.3 Methodik

1. Einführung der gängigen Hacking-Methoden: Als erster Schritt erfolgt eine umfassende Einführung in die verschiedenen gängigen Hacking-Methoden. Dabei werden die Methoden ausführlich erläutert, um den Leserinnen und Lesern einen fundierten Überblick über die unterschiedlichen Angriffstechniken zu geben.

2. Erklärung der Rainbow Tables: Im Anschluss daran erfolgt eine detaillierte Erklärung der Rainbow Tables, da diese für den praktischen Teil unverzichtbar sind. Es wird eine klare Definition der Rainbow Tables gegeben sowie ihre Funktionsweise und ihr Zweck im Kontext des Passwort-Hackings erläutert.

3. Aufstellung von Vergleichskriterien: Nach der Einführung und Erläuterung der Hacking-Methoden werden spezifische Vergleichskriterien aufgestellt, anhand derer die verschiedenen Methoden verglichen werden können. Diese Kriterien umfassen beispielsweise Effizienz, Erfolgsrate, Ressourcenbedarf und Anwendbarkeit. Dadurch wird eine strukturierte Grundlage für den Vergleich geschaffen.

4. Durchführung einer Nutzwertanalyse: Im nächsten Schritt erfolgt die Durchführung einer Nutzwertanalyse, um die verschiedenen Hacking-Methoden anhand der aufgestellten Kriterien zu bewerten. Dadurch können die Vor- und Nachteile jeder Methode objektiv beurteilt und eine Rangfolge erstellt werden.

5. Beschreibung der Testumgebung: Anschließend wird die Testumgebung detailliert beschrieben, die für die praktische Durchführung der Tests aufgesetzt wird. Dabei werden die verwendeten Hard- und Softwarekomponenten sowie die genauen Schritte und Vorgehensweisen für die Tests erläutert.

6. Praktische Durchführung der Tests: Die Tests werden gemäß der beschriebenen Testumgebung durchgeführt und die Ergebnisse sorgfältig dokumentiert. Es werden die angewandten Methoden, verwendeten Tools und erzielten Ergebnisse beschrieben. Dabei wird darauf geachtet, dass alle relevanten Informationen klar und präzise dargestellt werden.

7. Zusammenfassung der Ergebnisse: Am Ende der Methodik werden die Ergebnisse der praktischen Tests zusammengefasst und eventuelle Erkenntnisse oder Besonderheiten hervorgehoben. Es wird sichergestellt, dass die dokumentierten Ergebnisse den zuvor aufgestellten Vergleichskriterien entsprechen und eine Grundlage für die anschließende Diskussion bilden.

2 Grundlagen

2.1 Arbeitsumfeld

2.2 Begriffliche Grundlagen

2.2.1 BPMN

3 Ist- und Problemanalyse

4 Lösungskonzept

5 Fazit

Quellenverzeichnis

Internetquellen

Nick Statt (2015). *Obama, serious about cybersecurity, also delivers laughs*. URL: https://www.cnet.com/news/privacy/obama-serious-about-cybersecurity-also-delivers-laughs/ (besucht am 02. 06. 2023).

Anhang

1. Digitale Version der Arbeit

2. Interviews

    2.1. Expertmann 2018