Research Report

Entropass

Jochem Stevense

A research report presented for the design & implementation of Entropass

Embedded Systems Engineering
Flexible Project
Hogeschool van Arnhem en Nijmegen
Ton Ammerlaan, Remko Welling
The Netherlands
2021
Version 0.1

Research Report

Entropass

Jochem Stevense

Abstract

put some text here

Preface

Contents

1 Introduction

This research report has been created for the Hogeschool van Arnhem en Nijmegen as part of the Bachelor Flexible Project of Jochem Stevense and investigates the possibilities of developing a tool to efficiently guess for passwords, targeting a single specific person. The purpose of such a tool is to show users the vulnerabilities introduced by using memorable passwords and to generate wordlists to be used for ethical hacking and penetration testing purposes.

Wordlists are used by threat actors to perform dictionary attacks on services that require authentication, parsing through a list of words and trying to login, using these words as passwords. The same can be done with usernames, although usernames are generally easier to discover, depending on the service to authenticate to.
Most of the wordlists available are simply a compilation of previously discovered passwords, resulting from data breaches, and often hold the most used ones or the ones found in a specific data breach. This can prove useful when targeting a large number of users, since it is likely that one of these users will use a password that is included in the list. However, when targeting a single user, the odds of the password being included in such a list can be small. The reason for this is that many users use personalised passwords to be able to memorise the credentials. Although these personalised passwords are unlikely to be included in a general wordlist, they are often not hard to guess, when personal information about a target user is known.
This research aims to gain insight into what functionality a password wordlist generating tool would need, to be able to guess these personalised passwords for a single user. To reach this goal, the following research question has been defined:

What functionalities should a password wordlist generating tool have to be able to utilise standard password practices when targeting a single, specific user?

The main research question has been divided into several sub-questions. These sub-questions are the following:

- *What are standard password formats?*
- *What personal information is relevant for password guessing?*
- *How can the processed information be structured efficiently, to allow for efficient dictionary attacks?*

- *How can the program remain up to date with changing password practices?*

This research will consist of a combination of qualitative and quantitative research to find the most used password formats, used personal information for passwords, how the information can be structured and how to remain up to date with changing password practices. Desk research will be used to find the most used password formats, by gathering leaked passwords, publically available and analysing the passwords for the formats, and most used characters. The found passwords will also be analysed to detect personal information embedded into the passwords. Once this information is found, field research will be used to test the structuring of the data and how to analyse the data automatically and keep up with changing password practices.

2 Research

2.1 Theoretical Framework

2.2 Methodology

2.3 Results

2.4 Sub-Conclusions

3 Conclusions

test [1]

4 Discussion

4.1 Recommendations

References

[1] Wanli Ma, John Campbell, Dat Tran, Dale Kleeman, Password Entropy and Password Quality, 2010, University of Canberra, Australia `https://ieeexplore.ieee.org/abstract/document/5635948`