Cracking notezilla passwords

Salman Asad | @LeoBreaker1411

10th May, 2022

Table of contents

1. Introduction
2. Key Terms
3. Definitions
4. Virtual Environment (Lab Setup)
5. Exploitation
6. References

Introduction

This research paper will shed light on cracking notezilla password hashes. The notezilla master password hashes are simply base64 encoding applied on SHA256 encryption. However local access is needed to obtain the password hash stored by notezilla.

Key Terms

NoteZilla, SHA-256, Base64, MDXfind.

Definitions

1. **NoteZilla**

   Notezilla is a sticky notes app for Windows & Phones designed to keep you well-equipped & well-organized. It lets you take quick notes on sticky notes, right on your Windows desktop & gives you the best sticky notes experience.

2. **SHA-256**

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.

3. **Base64**

   In computer programming, Base64 is a group of binary-to-text encoding schemes that represent binary data (more specifically, a sequence of 8-bit bytes) in sequences of 24 bits that can be represented by four 6-bit Base64 digits. Common to all binary-to-text encoding schemes, Base64 is designed to carry data stored in binary formats across channels that only reliably support text content.

4. **MDXfind**

   MDXfind is another password cracking tool with advanced features.

Virtual Environment

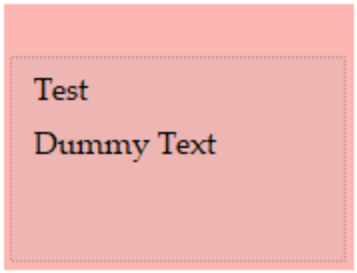
Attacker machine: Kali Linux 2022.1 (Virtual Machine running on VMWare)

Target machine: Windows 10 (Virtual Machine running on VMWare)

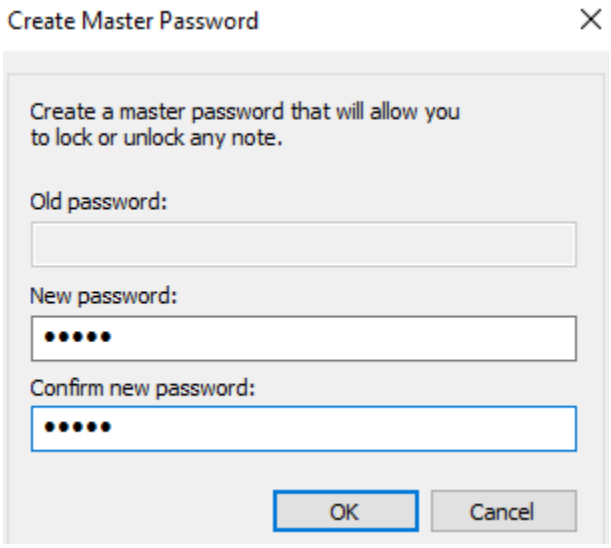
1. Install notezilla on the target machine, use default settings when prompted.

```
PS C:\Users\vagrant\Downloads> wget
https://www.conceptworld.com/Downloads/Notezill
a/NotezillaSetup.exe -outfile notezilla.exe
```

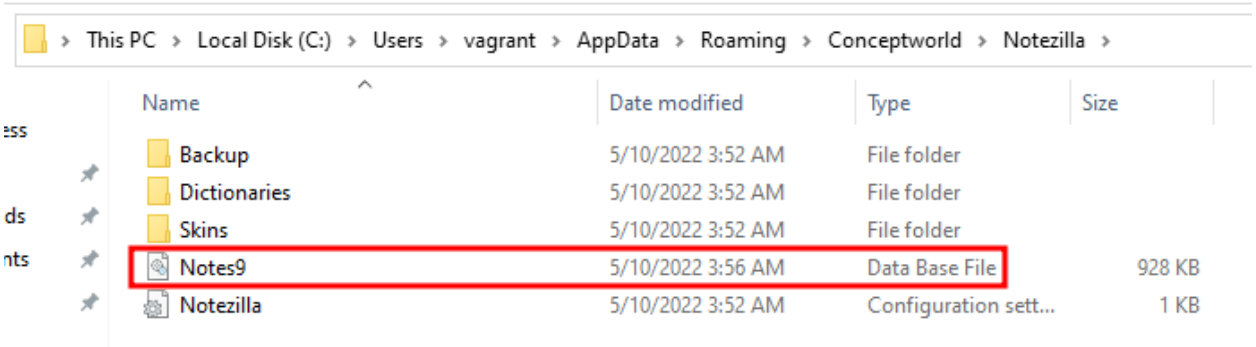
2. Create a new note with some dummy content

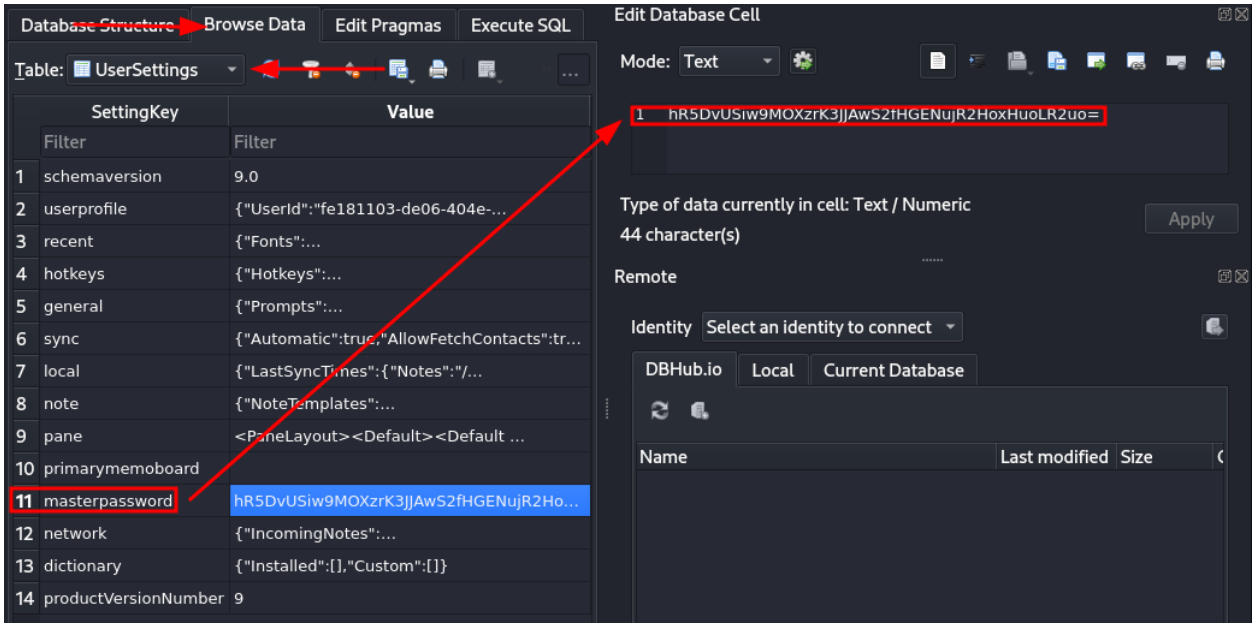


3. Encrypt the note with a password “flash”



4. Grab the hash of master password from “**Notes9.db**” in *C:\Users\<username>\AppData\Roaming\Conceptworld\Notezilla*





Exploitation

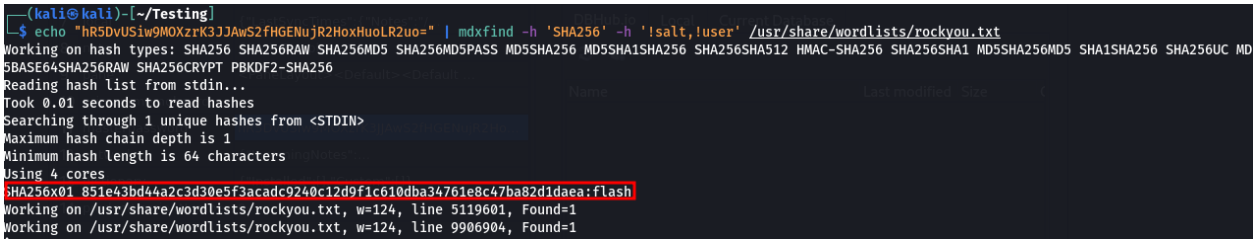
1. The master password hash is “hR5DvUSiw9MOXzrK3JJAwS2fHGENujR2HoxHuoLR2uo=”
2. Create a new note and encrypt it with password “test”, grab the master password hash “n4bQgYhMfWWaL+qgxVrQFaO/TxsrC4Is0V1sFbDwCgg=” searching for this would lead to https://stackoverflow.com/questions/37128276/how-to-compute-an-sha256-hash-and-base64-string-encoding-in-javascript-node which says that it is SHA256 encryption with BASE64 encoding

3. Download mdxfind from here.

```
wget https://www.techsolvency.com/pub/bin/mdxfind/mdxfind.static -O mdxfind && chmod +x mdxfind
```

4. Generate all SHA-256 hashes (non-salted) from the wordlist rockyou.txt and grep out the required hash.

```
echo
"hR5DvUSiw9MOXzrK3JJAwS2fHGENujR2HoxHuoLR2uo="
| mdxfind -h 'SHA256' -h '!salt,!user'
/usr/share/wordlists/rockyou.txt
```



5. We have successfully cracked notezilla's master password hash.

References

- https://www.techsolvency.com/pub/bin/mdxfind/
- https://0xln.pw/MDXfindbible
- https://github.com/pi-hole/pi-hole/issues/2521
- https://stackoverflow.com/questions/37128276/how-to-compute-an-sha256-hash-and-base64-string-encoding-in-javascript-node