

Forum:[Hack Forums](#)

Thread: [get passwords out of MacBook Keychain and Safari files](#)

Bierfreund_bw - March 9, 2017, 4:04 am

Dear All,

i have a question, i managed to get access to an macbook over SSH.

I took keychain and Safari Folders. (because i could not prepare and did not know about the OS).

Now im on windows OS, how can i decrypt the files so i can get bookmarks, history and passwords?

If some one can help me, i would be very thankful.

MR - X - March 9, 2017, 6:07 am

One very easy way would be to install a virtual machine and put a mac OS on there with the same version of safari they had installed.

Replace the safari files you downloaded with yours in VM and load up safari. With any luck and give the right files were copied it should load the bookmarks/history/passwords

As for decrypting the keyfile and passwords

Apple provides a tool called 'plutil.exe' for playing with these keylist

Here is the command to covert cryptic 'keychain.plist' file to easily readable 'keychain.xml' file

```
Code plutil.exe -convert xml1 -s -o c:\keychain.xml "c:\users\administrator\appdata\roaming\apple computer\preferences\keychain.plist"
```

The generated XML file contains encrypted password data along with website URL and username information. This stored password data is encoded using BASE64 algorithm.

So at this point its down to cracking the base64 encryption of the strings

Once you decode the password using BASE64 you will see original encrypted password data

Bierfreund_bw - March 9, 2017, 7:31 am

Thank you for your high quallity reply.

one further question, if i have the possibility again, what files should i download too? any further interesting thinks to do?

Or pearhaps files to upload?

Thank you

MR - X - March 9, 2017, 7:46 am

(Mar 9, 2017 08:31 AM)Bierfreund_bw Wrote: [CITE](#) Thank you for your high quallity reply.

one further question, if i have the possibility again, what files should i download too? any further interesting thinks to do?

Or perhaps files to upload?

Thank you

This would be a nice path to rip

/Users/USERNAME/Library/Application Support/

As this directory would contain the programs appdata or temp data/files

Would be the like "C:\Users\userName\AppData\Roaming\" with windows

This could contain login info for other software they might have installed or stored cookies for other software.

/System/Library/StartupItems

Might be a good upload path if you wanted to make the system run a file you upload on next startup.

vaiperboy - March 10, 2017, 8:09 am

(Mar 9, 2017 07:07 AM)MR - X Wrote: [\[CITE\]](#) This stored password data is encoded using BASE64 algorithm.

So at this point its down to cracking the base64 encryption of the strings
Once you decode the password using BASE64 you will see original encrypted password data wait what, apple stores passwords in base64? wow, what a shitty company :|

Bierfreund_bw - March 13, 2017, 7:40 am

Thank you for all the informations.

can you tell me, i only have the following files inside the Keychains folder:

login.keychain

login.keychain-db

metadata.keychain

metadata.keychain-db

keychain-2.db

keychain-2.db-shm

keychain-2.db-wal

ocspcache.sqlite...

sadly no keychain.plist, i didn't find it anywhere.

tnt_time - March 13, 2017, 7:46 am

you can buy a usb rubber ducky and automate the process so when you have the opportunity it goes fast and smooth

mulcahy911 - June 26, 2017, 10:10 pm

(Mar 13, 2017 07:46 AM)tnt_time Wrote: [\[CITE\]](#) you can buy a usb rubber ducky and automate the process so when you have the opportunity it goes fast and smooth

Do you have a link to that payload? I've seen it somewhere and have been searching for hours and I just can not find it.

imaketools - February 23, 2018, 3:18 am

keychaindumpPro

<https://hackforums.net/showthread.php?tid=5803486>