Product ∨   Solutions ∨   Resources ∨   Open Source ∨   Enterprise ∨   Pricing

Sign in   Sign up

HyperSine / **how-does-MobaXterm-encrypt-password**   Public

🔔 Notifications   Fork **95**   ☆ Star **290**

<> Code   ⊙ Issues **4**   ⅋ Pull requests **1**   ▷ Actions   ▢ Projects   ⊘ Security   📈 Insights

⅋ master ∨   ⅋   🏷

🔍 Go to file   <> Code ∨

HyperSine Update readme   462cd00 · 5 years ago   ⏱ **3 Commits**

📁 doc   Update readme   5 years ago

📁 python3   Refactor code   5 years ago

📄 README.md   Update readme   5 years ago

📖 **README**   ☰

Reveal password encrypted by MobaXterm

1. How does it work?

See [here](#)

2. How to use?

- Make sure you have Python3 and have `pycryptodome` installed.

```
Usage:
    MobaXtermCipher.py <enc|dec> [-sysh sys_hostname] [-sysu sys_user
                                 <-h conn_hostname> <-u conn_usernam
                                 <plaintext|ciphertext>

    MobaXtermCipher.py <enc|dec> <-sp SessionP> <plaintext|ciphertext

    MobaXtermCipher.py <enc|dec> <-p master_password> <plaintext|cip

        <enc|dec>              "enc" for encryption, "dec" for dec
                              This parameter must be specified.

        [-sysh sys_hostname]  Hostname of system where MobaXterm
                              This parameter is optional. If not

        [-sysu sys_username]  Username of system where MobaXterm
                              This parameter is optional. If not

        <-h conn_hostname>    Hostname of MobaXterm connection co
                              This parameter must be specified.

        <-u conn_username>    Username of MobaXterm connection co
                              This parameter must be specified.

        <-sp SessionP>        The value `SessionP` stored in key
                              This parameter must be specified.

        <-p master_password>  The master password set in MobaXter
                              This parameter must be specified.
```

About

This repo offers a tool to reveal password encrypted by MobaXterm.

📖 Readme

〰 Activity

☆ 290 stars

👁 6 watching

⅋ 95 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 2

👤 HyperSine

👤 DoubleLabyrinth Double Sine

Languages

● Python 100.0%

```
        <plaintext|ciphertext>    Plaintext string or ciphertext strin
                                  This parameter must be specified.
```

```
Usage:
    ShowMobaXterm.py [master_password]

        [master_password]        The master password set in MobaXtern
                                 This parameter is optional,
                                 but must be specified if you set a n
```

3. Example:

MobaXterm will save passwords and credentials in:

Type	Registry Path
Credentials	`HKEY_CURRENT_USER\Software\Mobatek\MobaXterm\C`
Passwords	`HKEY_CURRENT_USER\Software\Mobatek\MobaXterm\P`

If you have NOT set a master password in MobaXterm:

1. Credentials would look like:

```
Name              Type         Data
example.com       REG_SZ       root:bSj4VWbHezNH3tTY9Nil2RzJX57p7/!
```

You can reveal credential by:

```
$ ./MobaXtermCipher.py dec -sp 165821882556840 bSj4VWbHezNH3tTY9l
HyperSine
```

where `165821882556840` is the value `SessionP` stored in `HKCU\Software\Mobatek\MobaXterm`. Please modify it based on you environment.

2. Password would look like:

```
Name                        Type         Data
ssh22:root@45.32.110.171    REG_SZ       F0+wuBvbe9qPW6ypiOeYHTHl
```

You can reveal password by:

```
$ ./MobaXtermCipher.py dec -sysh ShadowSurface -sysu DoubleSine
Lw3+cZ2s.w@U@f]U
```

where `ShadowSurface` is my computer hostname and `DoubleSine` is my computer username.

If the password is stored on your computer, `-sysh` and `-sysu` can be omitted.

By the way, the example I give is a real SSH connection. But don't be happy too early, I've already delete that server.

3. All credentials and passwords can be revealed by `ShowMobaXterm.py`:

```
$ ShowMobaXterm.py 12345678
------------------Credentials-------------------
[*] Name:     example.com
[*] Username: root
[*] Password: HyperSine

------------------Passwords--------------------
[*] Name:     ssh22:root@45.32.110.171
[*] Password: Lw3+cZ2s.w@U@f]U
```

```
[*] Name:     root@45.32.110.171
[*] Password: Lw3+cZ2s.w@U@f]U
```

If you have set a master password in MobaXterm:

1. Credentials would look like:

```
Name            Type        Data
example.com     REG_SZ      root:0XROpGmLAYVx
```

You can reveal credential by:

```
$ ./MobaXtermCipher.py dec -p 12345678 0XROpGmLAYVx
HyperSine
```

where `12345678` is the master password you set.

2. Password would look like:

```
Name                        Type        Data
ssh22:root@45.32.110.171    REG_SZ      1du11XKQBOxud/FWh4ouWA=
```

You can reveal password by:

```
$ ./MobaXtermCipher.py dec -p 12345678 1du11XKQBOxud/FWh4ouWA==
Lw3+cZ2s.w@U@f]U
```

where `12345678` is the master password you set.

3. All credentials and passwords can be revealed by `ShowMobaXterm.py` :

```
$ ShowMobaXterm.py 12345678
-----------------Credentials-------------------
[*] Name:     example.com
[*] Username: root
[*] Password: HyperSine

------------------Passwords--------------------
[*] Name:     ssh22:root@45.32.110.171
[*] Password: Lw3+cZ2s.w@U@f]U

[*] Name:     root@45.32.110.171
[*] Password: Lw3+cZ2s.w@U@f]U
```

where `12345678` is the master password you set.