

 HyperSine /
how-does-MobaXterm-encrypt-password

Public

 Notifications

 Fork 94

 Star 289

<> Code

 Issues 4

 Pull requests 1

 Actions

 Projects

 Security

 Insights


 master ▾


 


Go to file


<> Code ▾



About



 doc

 python3

 README.md

 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.

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

-  Readme
-  Activity
-  289 stars
-  6 watching
-  94 forks

Report repository



Releases

No releases published

Packages

No packages published

Contributors 2

-  HyperSine
-  DoubleLabyrinth Double Sine

Usage:



```
MobaXtermCipher.py <enc|dec> [-sysh sys_hostname]
                                <-h conn_hostname>
                                <plaintext|ciphertext>
```

```
MobaXtermCipher.py <enc|dec> <-sp SessionP>
```

```
MobaXtermCipher.py <enc|dec> <-p master_password>
```

<enc dec>	"enc" for encryption This parameter
-----------	--

[-sysh sys_hostname]	Hostname of system This parameter
----------------------	--------------------------------------

[-sysu sys_username]	Username of system This parameter
----------------------	--------------------------------------

<-h conn_hostname>	Hostname of MobaXterm This parameter
--------------------	---

<-u conn_username>	Username of MobaXterm This parameter
--------------------	---

<-sp SessionP>	The value `SessionP` This parameter
----------------	--

<-p master_password>	The master password This parameter
----------------------	---------------------------------------

<plaintext ciphertext>	Plaintext string This parameter
------------------------	------------------------------------

Usage:



```
ShowMobaXterm.py [master_password]
```

[master_password]	The master password This parameter but must be specified
-------------------	--

Languages

● Python 100.0%

3. Example:

MobaXterm will save passwords and credentials in:

Type	Registry Path
Credentials	HKEY_CURRENT_USER\Software\Mobatek\MobaXterm
Passwords	HKEY_CURRENT_USER\Software\Mobatek\MobaXterm

If you have NOT set a master password in MobaXterm:

1. Credentials would look like:


Name	Type	Data	
example.com	REG_SZ	root:bSj4VWbHe:	

You can reveal credential by:

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

You can reveal password by:

```
$ ./MobaXtermCipher.py dec -sysh ShadowSurface 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:0XR0pGmLA'

You can reveal credential by:

```
$ ./MobaXtermCipher.py dec -p 12345678 0XR0pGmLA'
HyperSine
```

where `12345678` is the master password you set.

2. Password would look like:

Name	Type	Da	
ssh22:root@45.32.110.171	REG_SZ	1di	

You can reveal password by:

```
$ ./MobaXtermCipher.py dec -p 12345678 1du1: 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
```