

Forum:[Hack Forums](#)

Thread: [Steal password using mimikatz as it happened in the movie Mr. Robot](#)

Mr8n - March 31, 2018, 6:10 am

Mr.Robot has shown us that it is the best series that lists the reality of penetration in the form of a film on some films that use programs or penetration tools that do not exist in health. But in Mr.Robot, specifically in episode 6 of season 2, Angela was the best Friend of Elliott, is now an executive at E Corp looking for information about poisonous chemical leakage by E Corp that killed her mother and father Elliott. We also used USB Rubby to extract company passwords (the password is not encrypted)

This information can be given by toxic chemical leakage in Washington.

As it turns out in episode 6 of season 2 Angela made his supporters that it was easy to get the password for her boss, and actually be right if the hacker knew what he was doing.

In this post we will add some games using the computer and the victim's operating intent is windows passwords without encryption.

Rubber Ducky

Let's get to know what is Rubber Ducky so that things do not mix up. Rubber Ducky is a USB device that simulates a keyboard through which we can extract input on your printer, mouse, keyboard, etc., you can buy one from Hackaday's store

<https://hakshop.com/products/usb-rubber-ducky-deluxe>

As we urged in the episode, Angela assured us that you do not need high hacking skills to extract passwords.

Also do not forget that you can use mimikatz to extract passwords instead of Rubber Ducky.

What is Mimikatz !!!

We must first get to know Mimikatz !!

A Mimikatz is a self-contained program used by Angela to extract her boss's password It was developed by Benjamin Delpy, also known as gentilkiwi and is probably developed in C, and Mimikatz's main mission in the victim's device is to steal data from the Windows operating system in memory.

Mimikatz has proven to be a very powerful tool, so much so that Rapid7 has developed a copy of Mimikatz and developed it within the Metasploit project.

Download link Mimikatz

<https://github.com/gentilkiwi/mimikatz>

Now let's talk and we'll go to the application explanation and we'll learn how to extract passwords from any device just like Angela did.

Install mimikatz

After uploading to mimikatz, open the cmd.exe file, but you must have the "Open as Administrator"

As you will follow in the picture below, a session will open at Mimikatz

Note :

Before proceeding to work on Mimikatz

```
mimikatz # privilegegegege :: debug
```

Before embarking on the next step you should know what is the release of the operating stream

And this is the case

```
mimikatz # version
```

As we look at the picture above, the mimikatz was able to know what the OS version was, and the version was Windows NT 6.1 build 7601 (Windows 7) 64-bit.

Now we have reached the task stage and are extracting passwords

We first need to explain to you how Mimikatz can extract the passwords on your device !!

Mimikatz injects the .dll files on the device.

But to be more clear he is injecting a file named sekurlsa.dll.

For passwords, type;

```
mimikatz # sekurlsa :: logonpasswords
```

As we can see in the picture above, the operating platform has responded to us and we have been

able to get the password and some information. As we can see in the picture, the user name is Angela's Boss and also domain (E Corp). The most important of all is The password is (pa \$\$ w0rd).

Now Angela can get the secret files of E-Corp's and find evidence of the toxic substances that killed her mother and Elliott's father and bring the perpetrators to justice !

Mr.Mr8n ?

Translate google was used