This challenge is supposed to be trivial, but getting the right conditions for it is pretty difficult on modern machines. I decided to solve it via volatility2 and mimikatz.

Step 1: Getting volatility 2 on the linux machine. For this part I used https://seanthegeek.net/1172/how-to-install-volatility-2-and-volatility-3-on-debian-ubuntu-or-kali-linux/ to install volatility2.

Step 2: Finding the profile. For this step, we simply need to run **vol.py -f crashdump.elf imageinfo** . We soon find out a suitable profile is **Win7SP1x64**. We will need this information later.

Step 3: To actually solve the challenge, we need to use mimikatz, more specifically the volatility2 plugin mimikatz. It can be found at https://github.com/volatilityfoundation/community/blob/master/FrancescoPicasso/mimikatz.py.

That plugin needs to be inserted into the plugins directory of the volatility installations. For that, I used **find /home/<username>/.local/lib/python2.7/site-packages/ -type d -name 'volatility' 2>/dev/null** . This command located the volatility folder in your system, as long as <username> is the username under which volatility was installed at Step 1. After that, we simply insert the contents at mimikatz.py, and we are good to go! Well, almost

Step 4: Fixing mimikatz. Turns out, there are some issues with mimikatz. For me, the issue I had is at https://github.com/volatilityfoundation/community/issues/15. Other issues may arise, so make sure to solve them properly before you run mimikatz. You are good to go when you get:

```
vol.py --info | grep "mimikatz"

Volatility Foundation Volatility Framework 2.6.1

mimikatz                    - mimikatz offline
```

Step 5: Putting everything togheter. The actual step that involved solving the chall. Simply run **vol.py -f crashdump.elf --profile=Win7SP1x64 mimikatz**.

Made with love by: AndreiCat