Password hashes

1. Extracting hashes from Windows system

The LM hash is the old style hash used in Microsoft OS before NT 3.1. Then, NTLM was introduced and supports password length greater than 14.
On Vista, 7, 8 and 10 LM hash is supported for backward compatibility but is disabled by default. The goal is to extract LM and/or NTLM hashes from the system, either live or dead. These hashes are stored in memory (RAM) and in flat files (registry hives).

If LM hashes are **enabled** on your system (Win XP and lower), a hash dump will look like:

```
Administrator:500:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537::
:
```

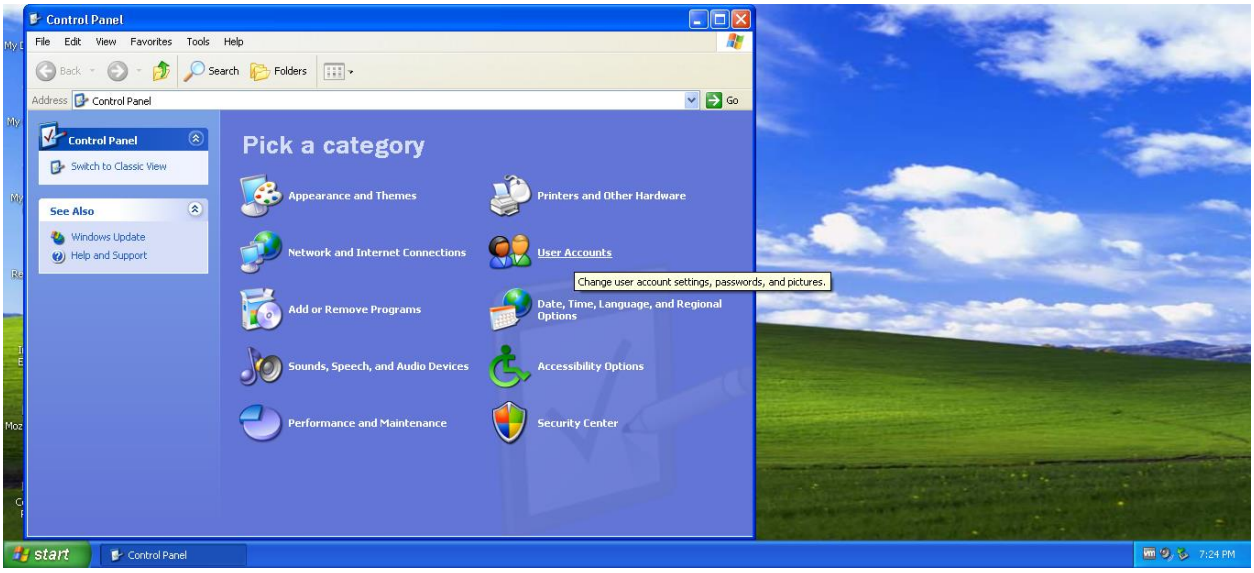
If LM hashes are **disabled** on your system (Win Vista, 7, 8+), a hash dump will look like:

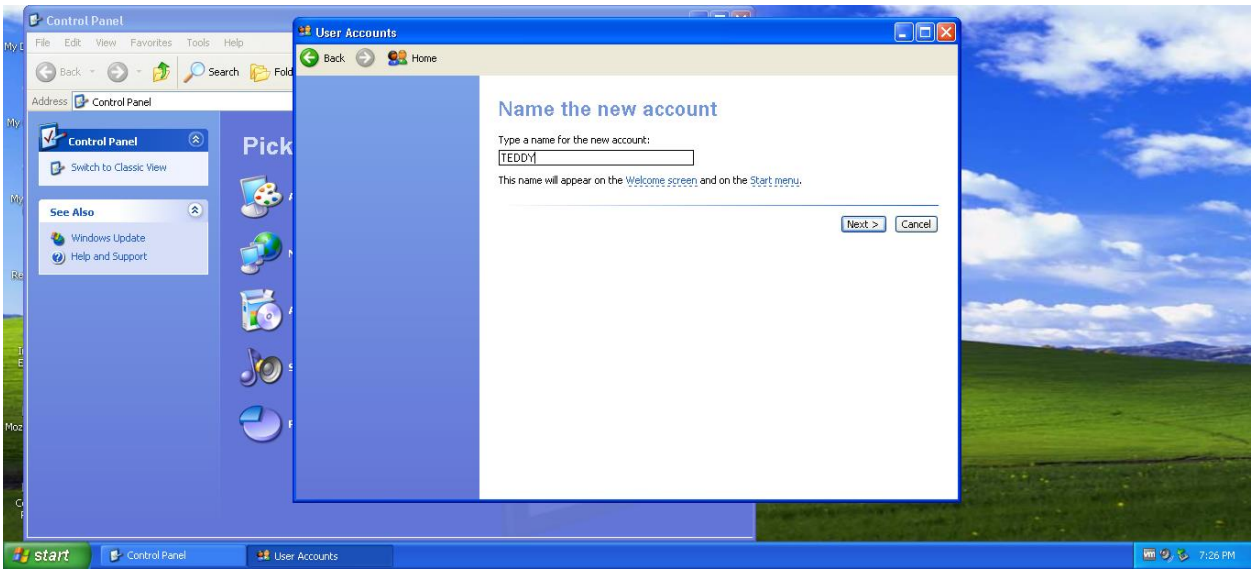
```
Administrator:500:NO PASSWORD*********************:0CB6948805F797BF2A82807973B89537::
:
```

Let`s begin.

1. Start your Windows XP virtual machine and open up the control panel.

2. Create 2 new user accounts, give them a username and provide password for each one.

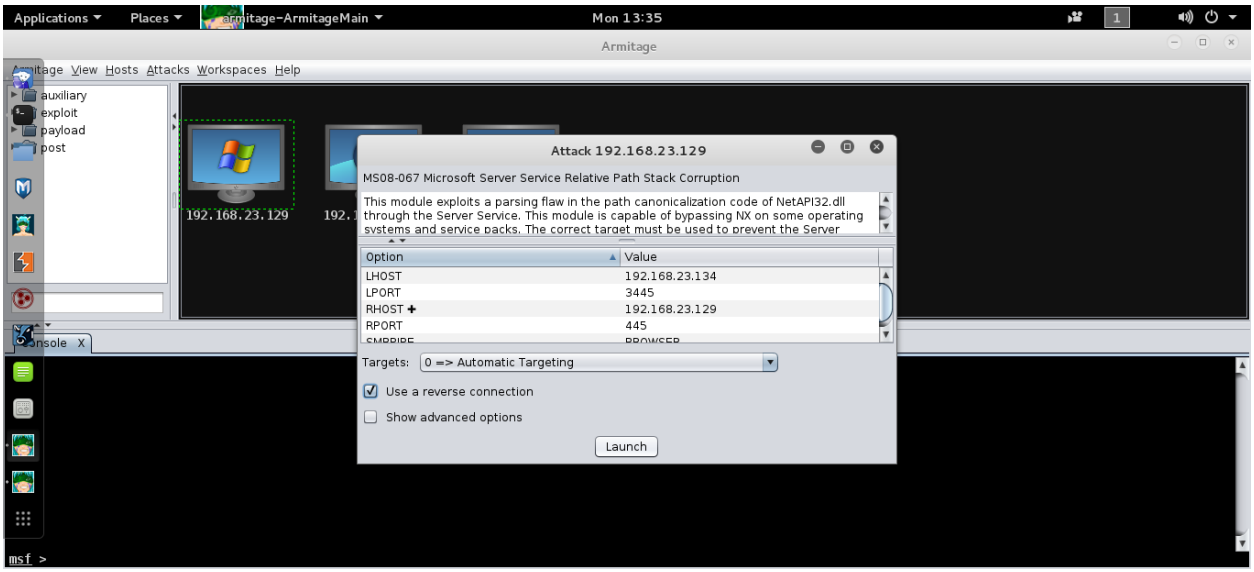




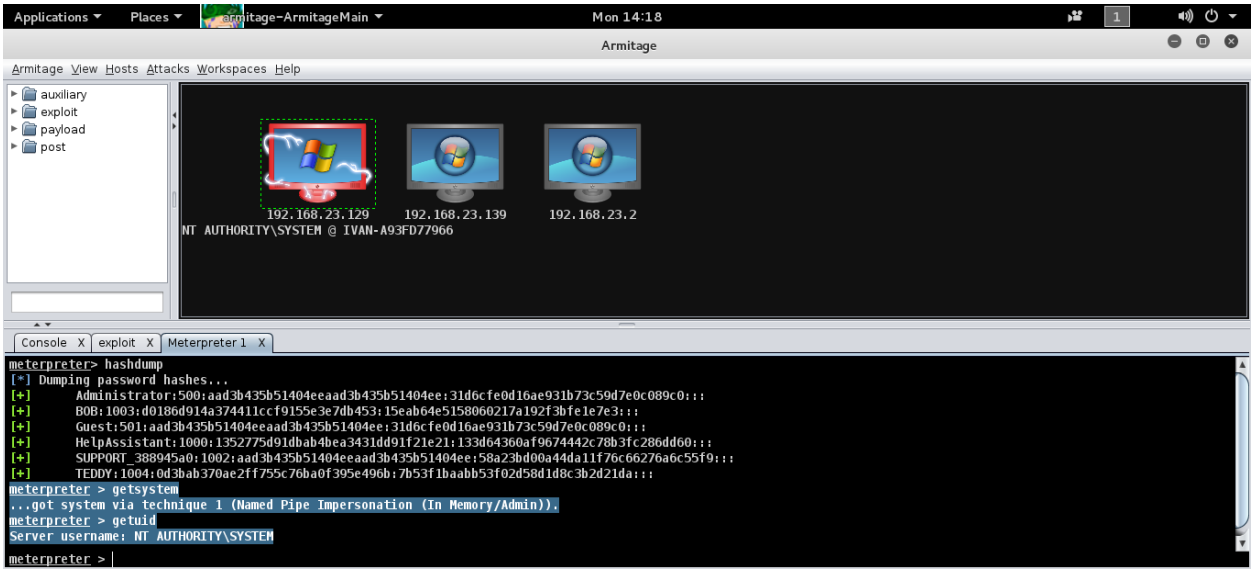
For example I am creating 2 users : TEDDY and BOB with usernames

3.Next , start you kali machine and open up Armitage (Please review Metasploit lab if you have issues)

From the Armitage panel attack and take over the Windows XP machine , using the netapi exploit (or one of your choice.

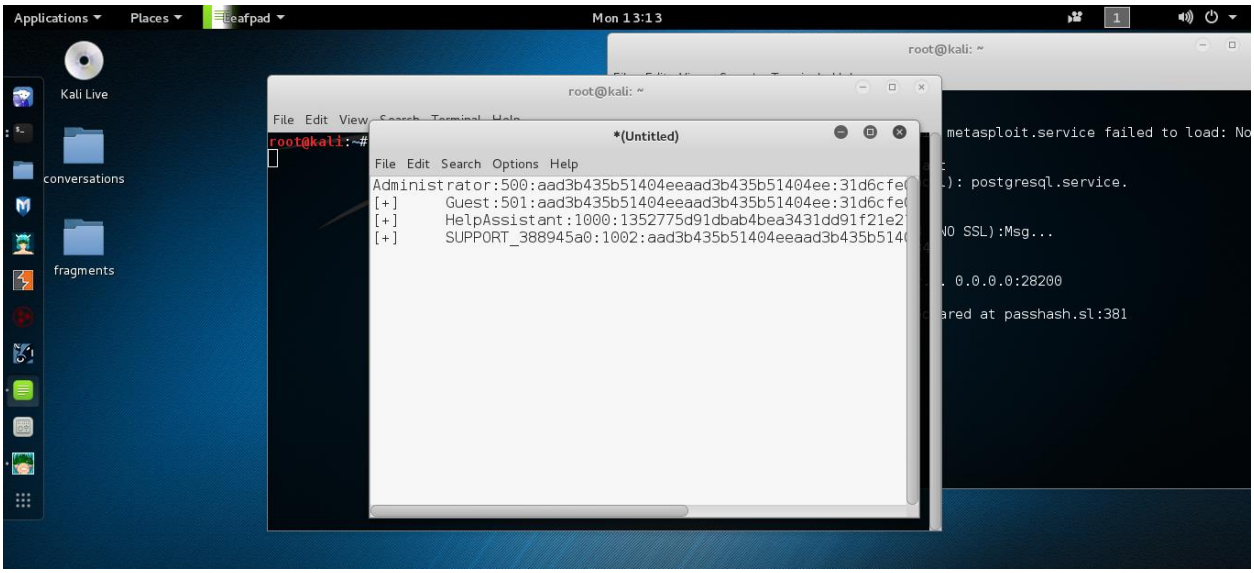


Once you open up a meterpreter session ,navigate and select to extract the hashes.Another option to get the hashes is if you simply type in the meterpreter session : hashdump



4. Copy the hashes that appear.

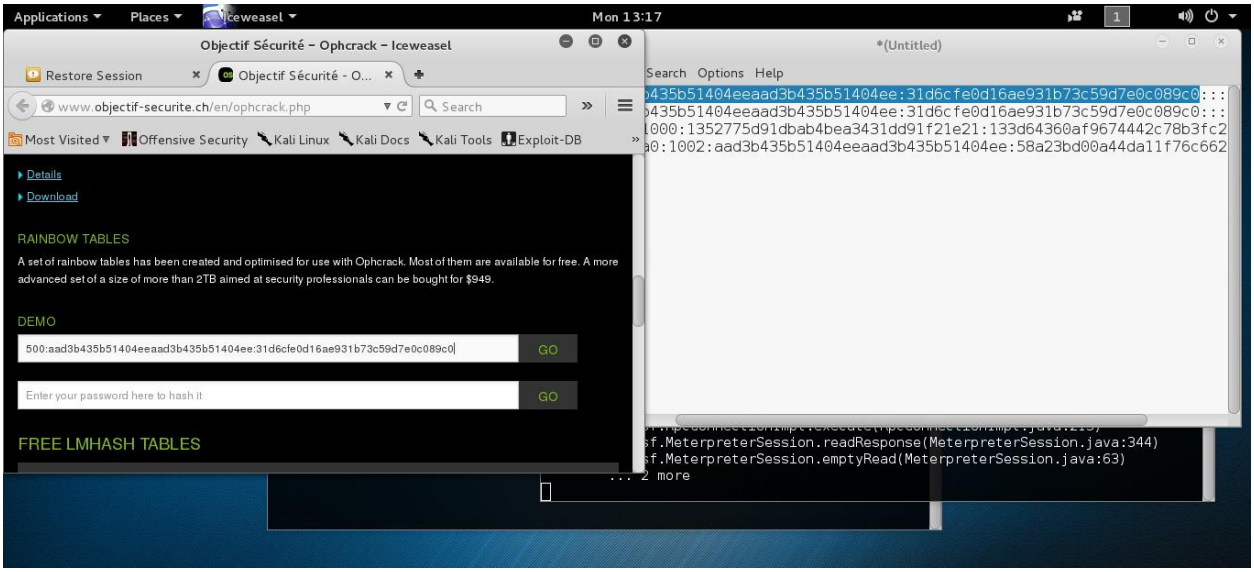
5. Open up another terminal and type in leafpad. Paste the hashes here. After this save the file as default on your desktop.

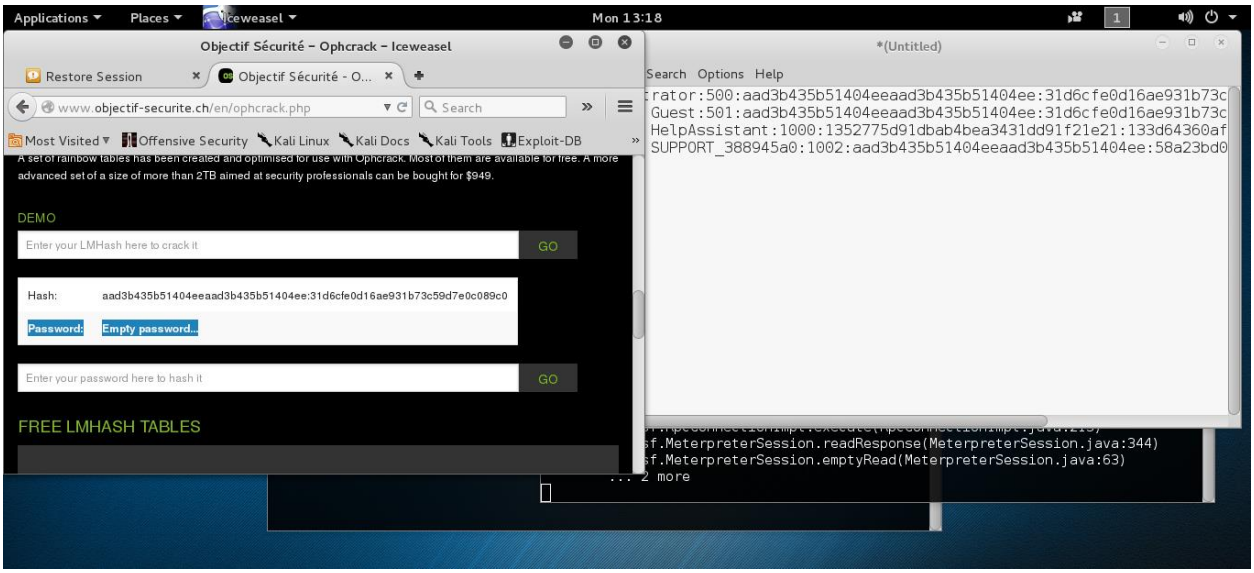


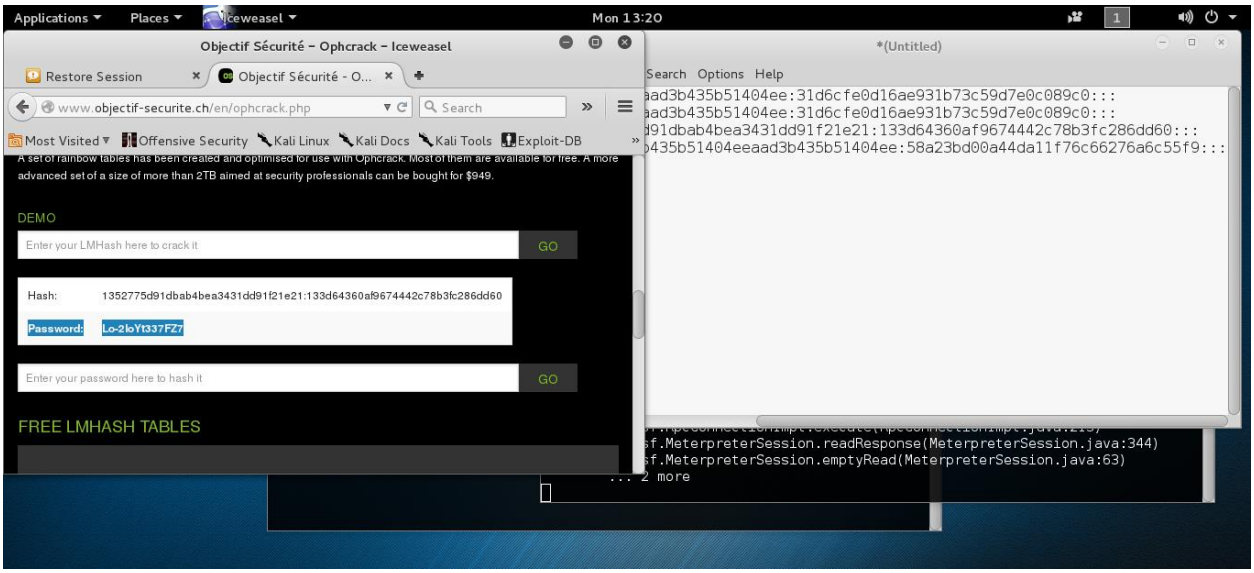
6.Next open up Iceweasel browser and navigate to following website:

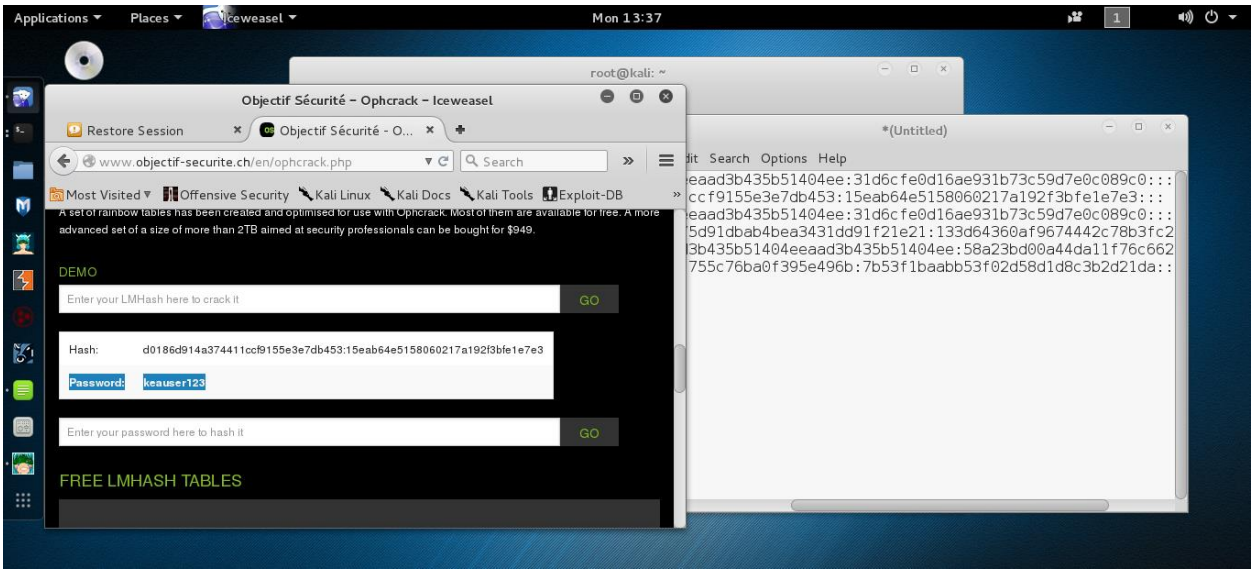
http://www.objectif-securite.ch/en/ophcrack.php

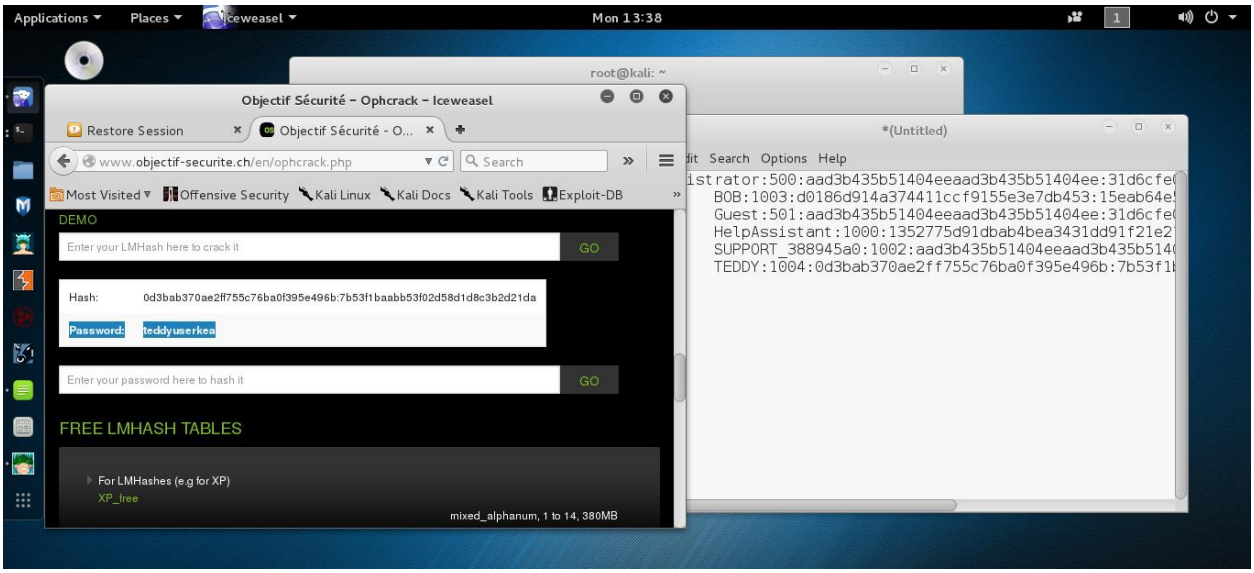
7.Copy and paste the different hashes here.See the results.



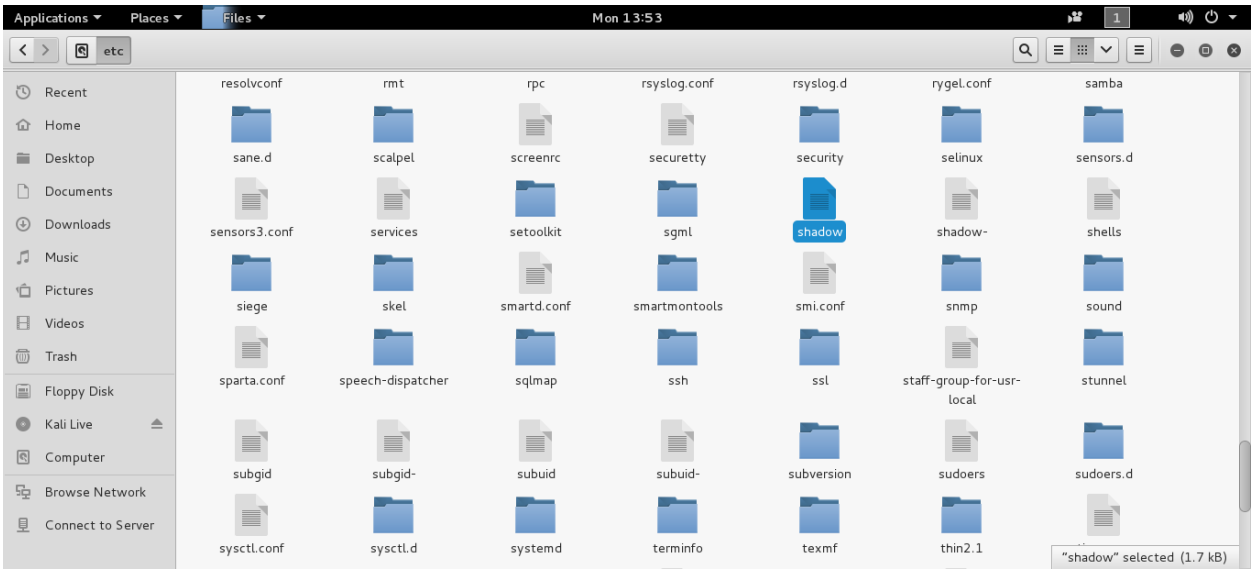

Applications
Places
Iceweasel
Mon 13:18
Objectif Sécurité – Ophcrack – Iceweasel
Restore Session
Objectif Sécurité - O...
www.objectif-securite.ch/en/ophcrack.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
A set of rainbow tables has been created and optimised for use with Ophcrack. Most of them are available for free. A more advanced set of a size of more than 2TB aimed at security professionals can be bought for $949.
DEMO
Enter your LMHash here to crack it
GO
Hash:
aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Password:
Empty password...
Enter your password here to hash it
GO
FREE LMHASH TABLES
*(Untitled)
Search
Options
Help
rator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c
HelpAssistant:1000:1352775d91dbab4bea3431dd91f21e21:133d64360af
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:58a23bd0
sf.MeterpreterSession.readResponse(MeterpreterSession.java:344)
sf.MeterpreterSession.emptyRead(MeterpreterSession.java:63)
... 2 more


Applications
Places
Iceweasel
Mon 13:20
Objectif Sécurité – Ophcrack – Iceweasel
Restore Session
Objectif Sécurité - O...
www.objectif-securite.ch/en/ophcrack.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
A set of rainbow tables has been created and optimised for use with Ophcrack. Most of them are available for free. A more advanced set of a size of more than 2TB aimed at security professionals can be bought for $949.
DEMO
Enter your LMHash here to crack it
GO
Hash:
1352775d91dbab4bea3431dd91f21e21:133d64360af9674442c78b3fc286dd60
Password:
Lo-2loYt337FZ7
Enter your password here to hash it
GO
FREE LMHASH TABLES
*(Untitled)
Search
Options
Help
aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
d91dbab4bea3431dd91f21e21:133d64360af9674442c78b3fc286dd60:::
b435b51404eeaad3b435b51404ee:58a23bd00a44da11f76c66276a6c55f9:::
sf.MeterpreterSession.readResponse(MeterpreterSession.java:344)
sf.MeterpreterSession.emptyRead(MeterpreterSession.java:63)
... 2 more



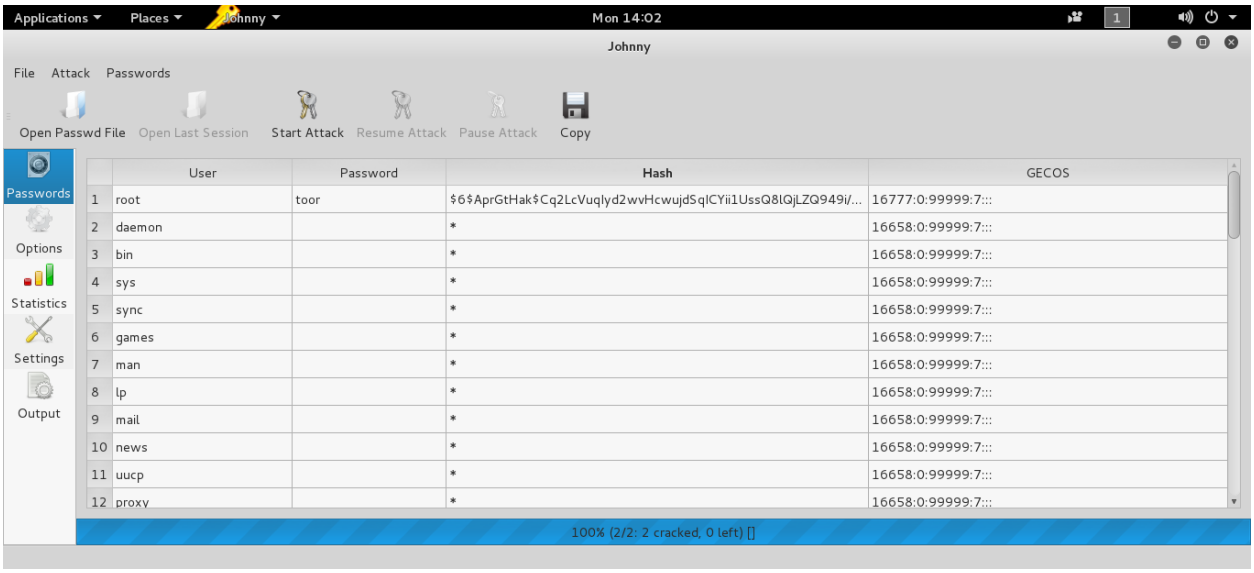


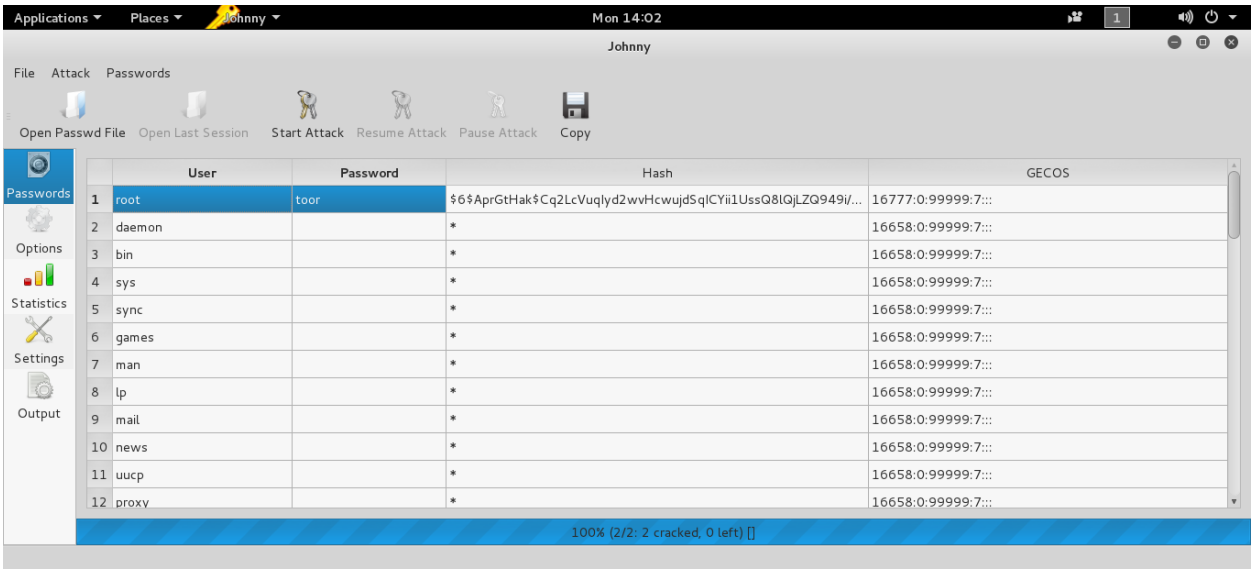
8.In you Kali machine go to Places>Computer > etc and find the shadow file. Here is where Linux is keeping the hashed values for passwords of its users.Open up the file , then copy and paste the values into a newly opened leafpad .Then save the file on your desktop.



9. Open up Johnny (John the reaper tool)

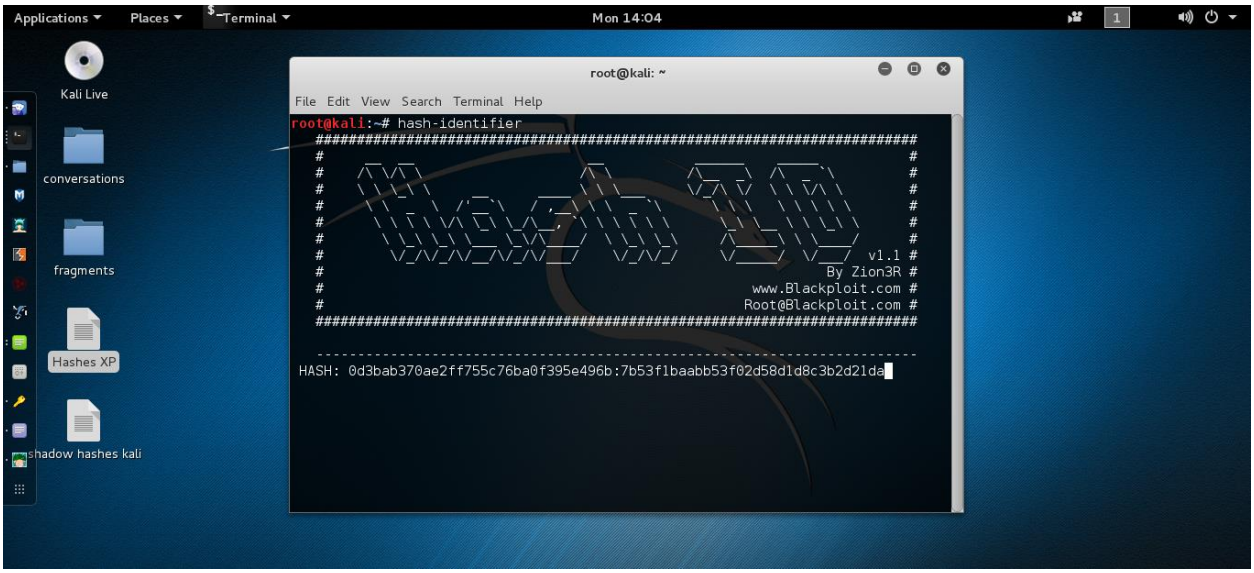
10.Upload the file you saved into Johnny. Then click on start the attack.

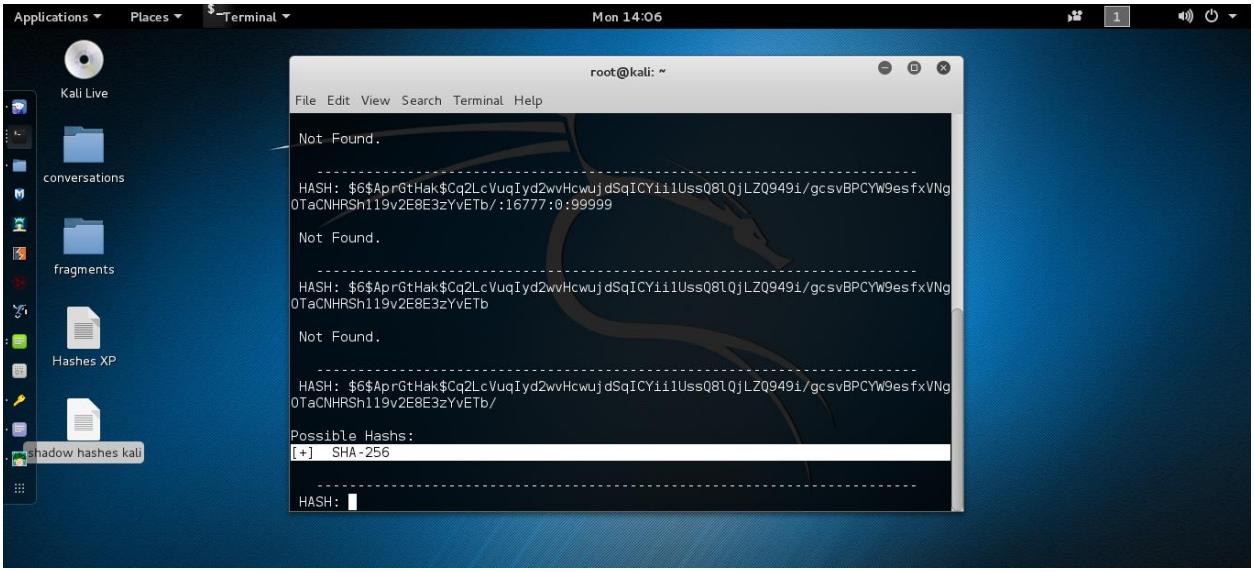




11. Another great tool to recognize the type of hash is: hash-identifier

Simply type in the command in Kali .Then copy and paste the hash and the tool will try to tell you which type is it.

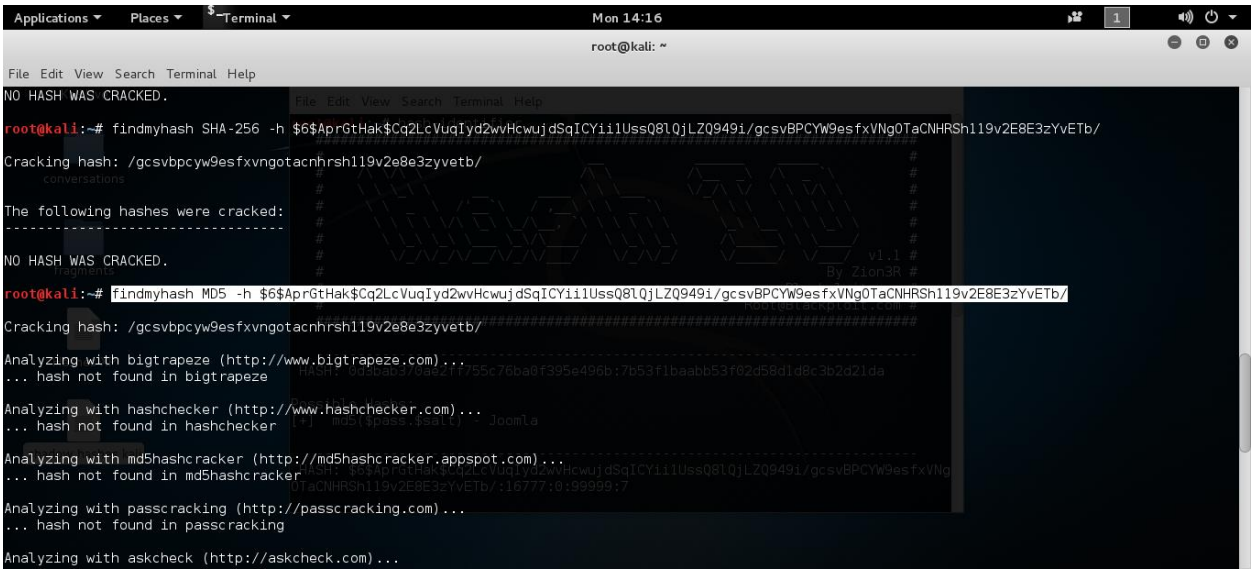




12. Another great tool to use is findmyhash

Usage: findmyhash <Encryption > -h < hash>

For example: findmyhash –MD5 –h *6AprGtHak$Cq2LcVuqIyd2wvHcwujdSqICYii1UssQ8lQjLZQ949i/gcsvBPCYW9esfxVNgOTaCNHRSh119v2E8E3zYvETb/*



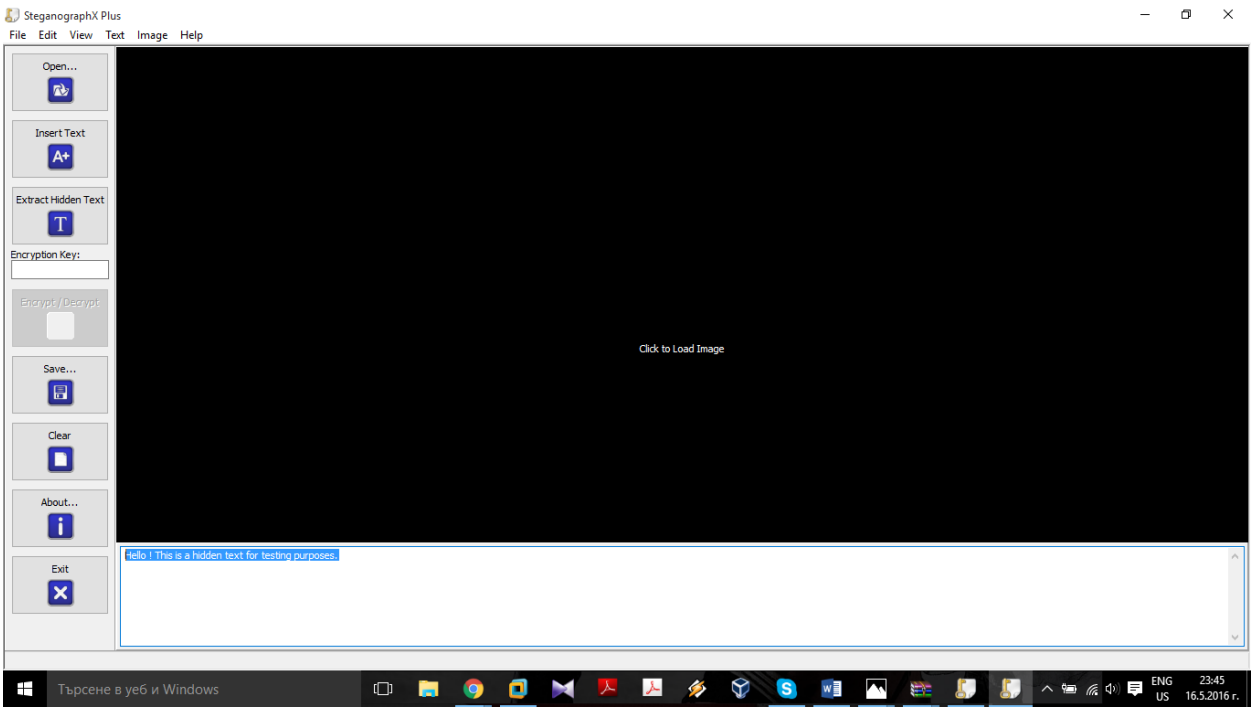
Steganography

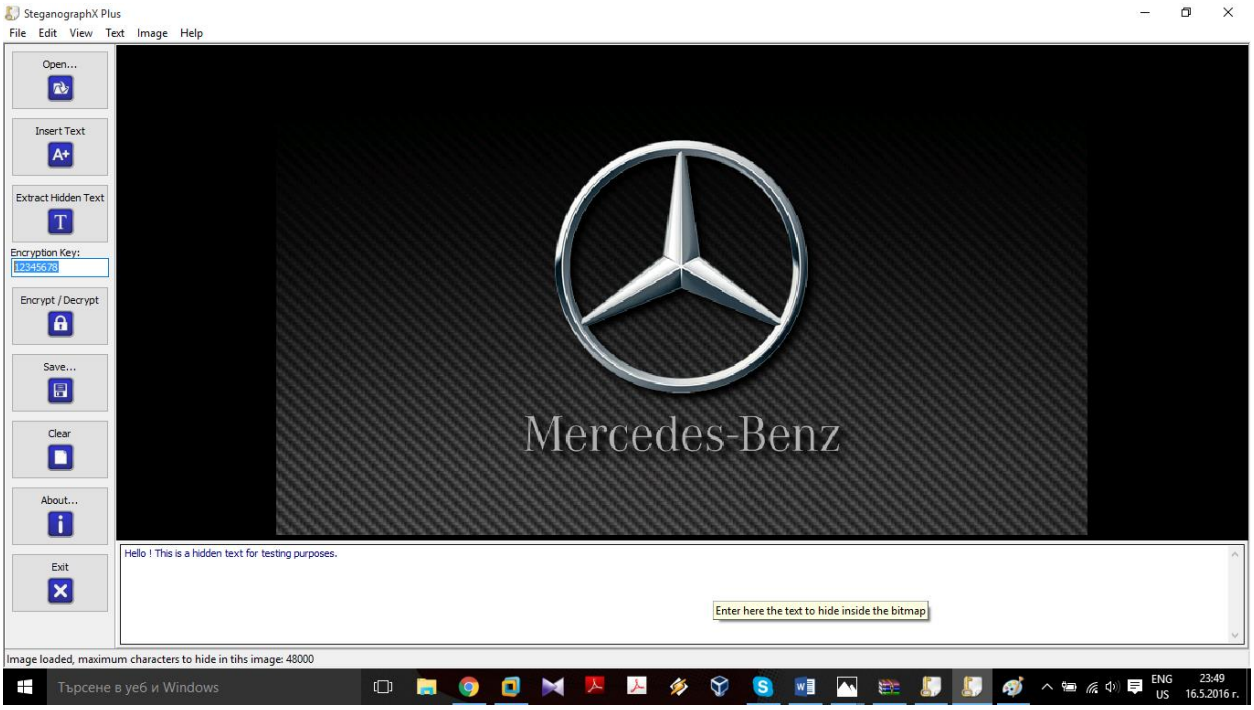
Steganography is the art of hiding a secret message behind the normal message. This is used to transfer some secret message to other person and no interim person will be able to know what the real message which you wanted to convey was. This art of hiding secret messages has been used for years in real life communications. Since the evolvement of digital communication, it has also been used in digital conversations. In computer, it is achieved by replacing the unused or useless data of a regular computer file with the bit of your secret message. This secret hidden information can be a plain text message, cipher text, or image. One can hide information in any kind of file. Usually image, video and audio files are used to hide plain text message or image message. Few tools now allow one to hide files inside an image or audio file.

Many tools available. Here is an example one - Steganography Pro

Download from here:

http://www.mediafire.com/download/nwmqjnim22o/StgP.zip





Hidden file looks like this:

Another great and easy tool is Open Puff: Download from here:

http://embeddedsw.net/OpenPuff_Steganography_Home.html