Client Side Attacks (Contd)

Tools in Kali Linux

Module #26

Kali Linux: Johnny?

Johnny is a GUI for the very popular John the Ripper password cracking tool.

Johnny has several engines that allows it to crack different types of passwords, including encrypted and hashed passwords.

Can auto-detect most hashes and encrypted passwords, making the process easier for Penetration Testers. Very easily customizable and can be configured in different ways to speedup password cracking.

Available in Password Attacks | Offline Attacks and select Johnny. Click on Open Password File and select the password file you want to crack.

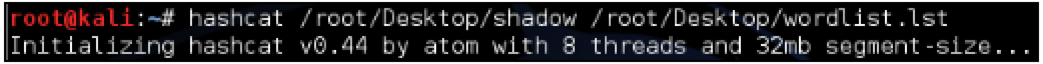
Kali Linux: hashcat?

hashcat and oclHashcat are password cracker utilities.

These are multithread tools that can handle multiple hashes and password lists during a single attack session. Offers many attack options: brute-force, combinator,dictionary, hybrid, mask, and rule-based attacks.

Available in Password Attacks → Offline Attacks

To use hashcat on a document, type hashcat [options] hashfile [wordfiles|directories . The following example shows hashcat running a wordlist against a shadow file:



```
root@kali:~# hashcat /root/Desktop/shadow /root/Desktop/wordlist.lst
Initializing hashcat v0.44 by atom with 8 threads and 32mb segment-size...
```

Kali Linux: samdump2?

Utility that dumps the Microsoft Windows password hashes from a SAM file so that they can be cracked by an offline tool.
For newer versions of Windows, you will need another tool to capture the SYSKEY (boot key) file to access the hashes stored in the SAM database.

samdump2 can be found under “Offline Attacks”. When you open samdump , a Terminal window will pop up.

You must mount your target Windows system so that samdump can access the SAM file.
Next, copy the SAM and SYSTEM files into your attack directory.

```
cp SAM SYSTEM /root/AttackDirectory
```

Kali Linux: samdump2?

Navigate to the attack directory and issue bkhive SYSTEM bootkey to obtain the bootkey. Copy the bootkey into a text file so that samdump has the SAM file with bootkey

```
cd /root/AttackDirectory > windowshashfiles.txt
```

Execute samdump using the samdump SAM bootkey command. Copy the output into a second text file.

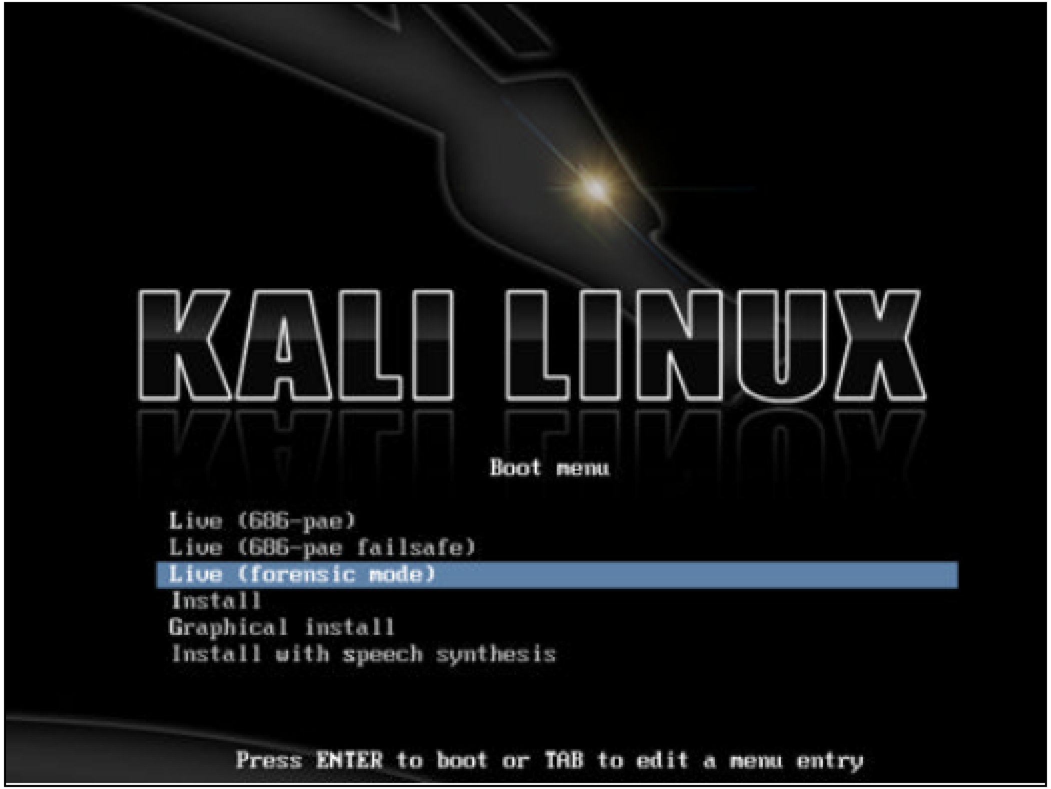
```
Samdump2 SAM bootkey > windowshashfiles2.txt
```

Now use a password cracking tool such as John the Ripper to crack the hashes!

Kali Linux: chntpw?

chntpw is a tool that resets local passwords on Windows 8 and earlier versions of Windows.
It modifies the Windows password database. This tool is primarily used for getting into Windows boxes when you do not know the password.
To use chntpw , boot up the Windows machine with the Kali Live CD.

On the boot menu for Kali, select Forensics option.

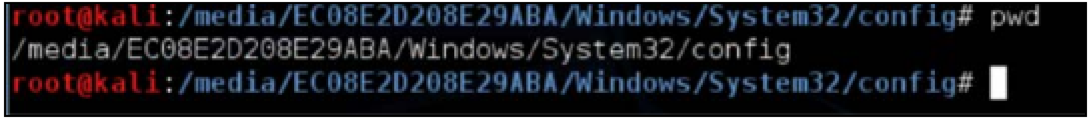


Press ENTER to boot or TAB to edit a menu entry

Kali Linux: chntpw?

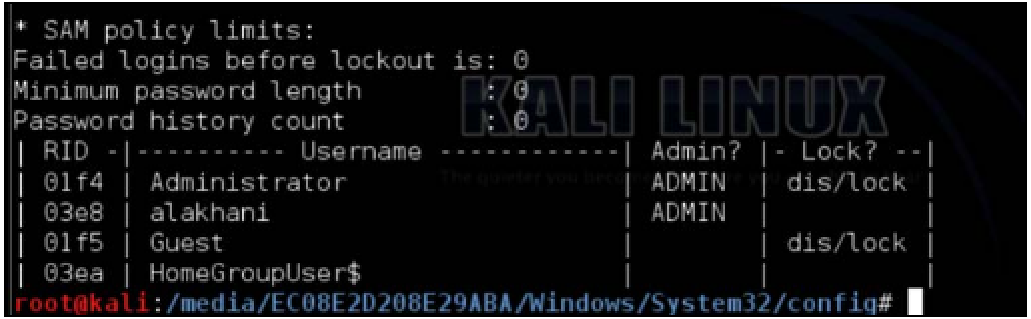
The SAM file is usually located under /Windows/System32/config .

The SAM database is usually in the /media/name_of_hard_drive/Windows/System32/config.



```
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config# pwd
/media/EC08E2D208E29ABA/Windows/System32/config
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config# 
```

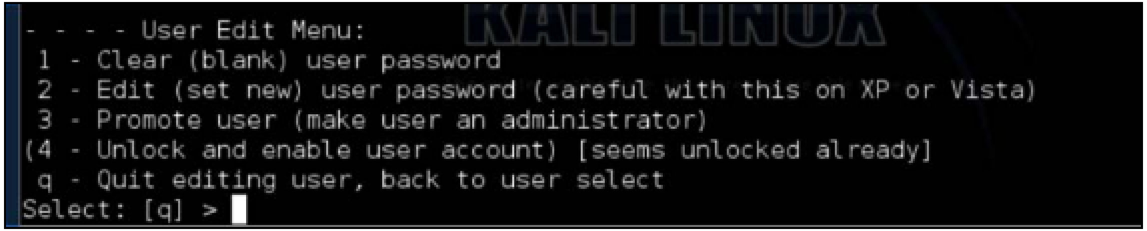
The command chntpw -l SAM will list out all the usernames that are contained on the Windows system.



```
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length         : 0
Password history count          : 0
| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 03e8 | alakhani                       | ADMIN  |          |
| 01f5 | Guest                          |        | dis/lock |
| 03ea | HomeGroupUser$                 |        |          |
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config# 
```

Kali Linux: chntpw?

chntpw -u "Administrator" SAM, and we got the following menu:



```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] >
```

We now have the option of clearing the password, changing the password, or promoting the user to administrator. Recommendation is to clear the password. By doing this, you will be able to log into the target system with a blank password.

Thank You