

**Name:** Lakhani Ritesh Shaileshbhai

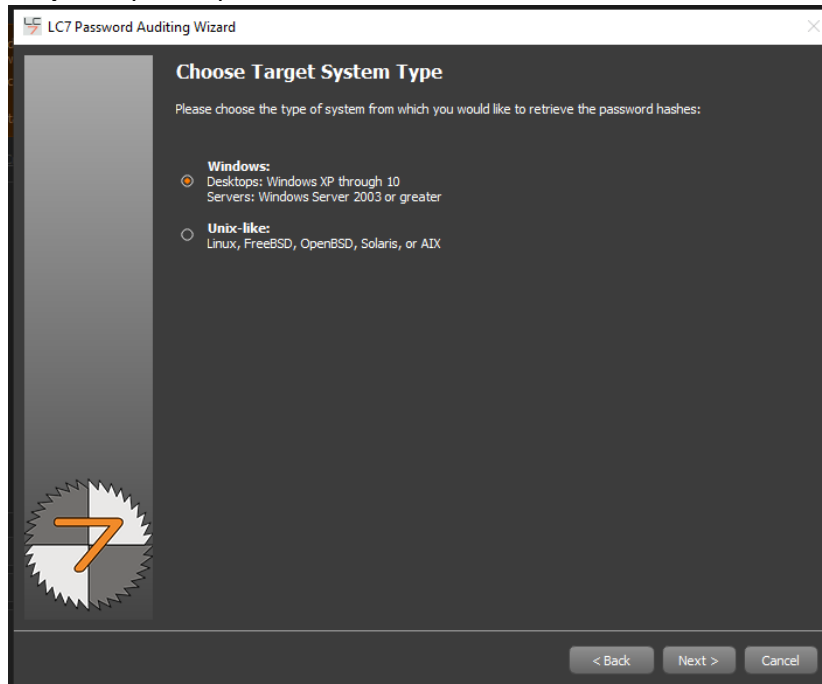
**Enrollment No:** 22010101099

**Date:** 15/02/2025

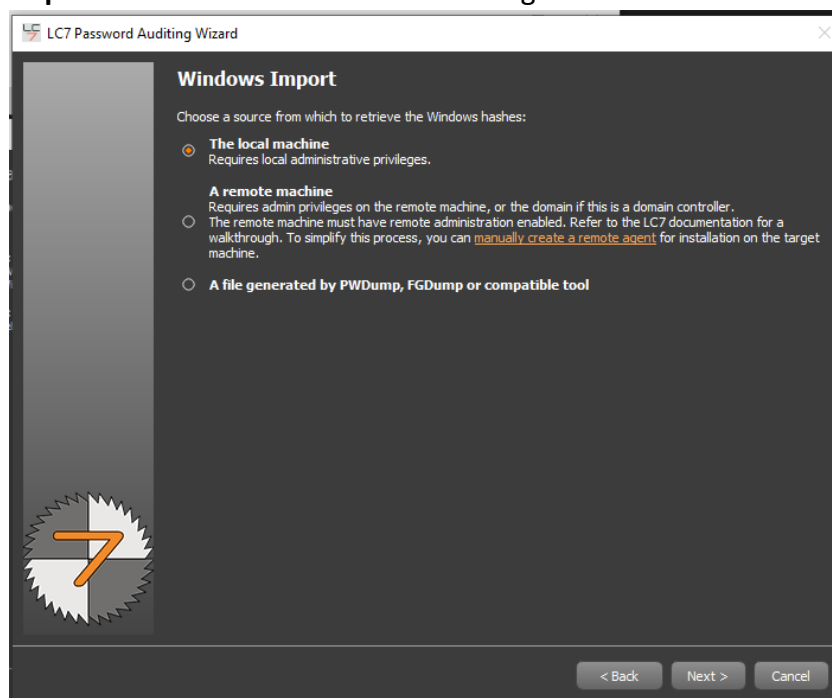
**Lab 10. Perform password cracking concept using brute force tools- L0phtCrack and John the ripper.**

## 1. Steps to Perform Password Cracking using L0phtCrack 7:

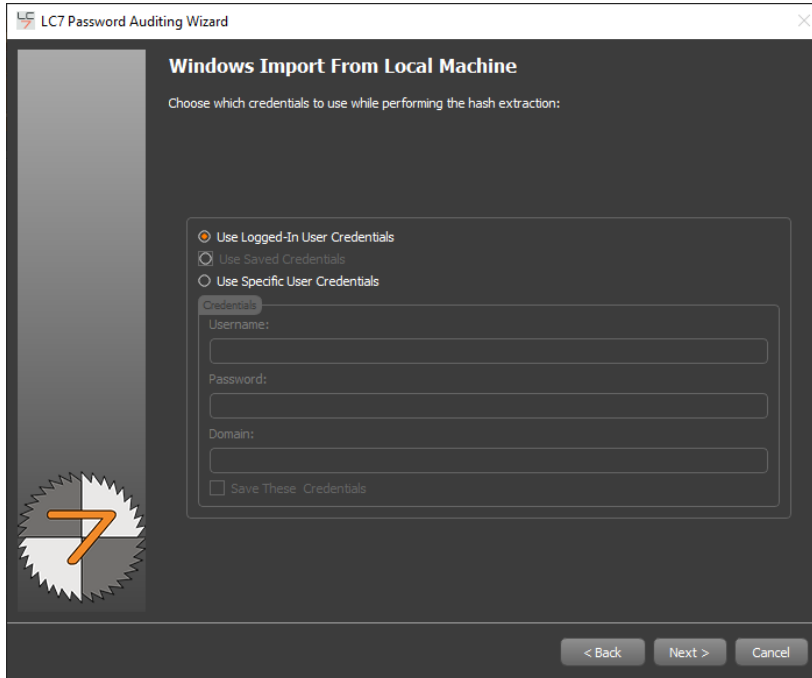
**Step-1:** Open L0phtCrack 7 and select Windows.



**Step 2:** Choose Local Machine as the target.



**Step 3: Enter User Credentials if required.**



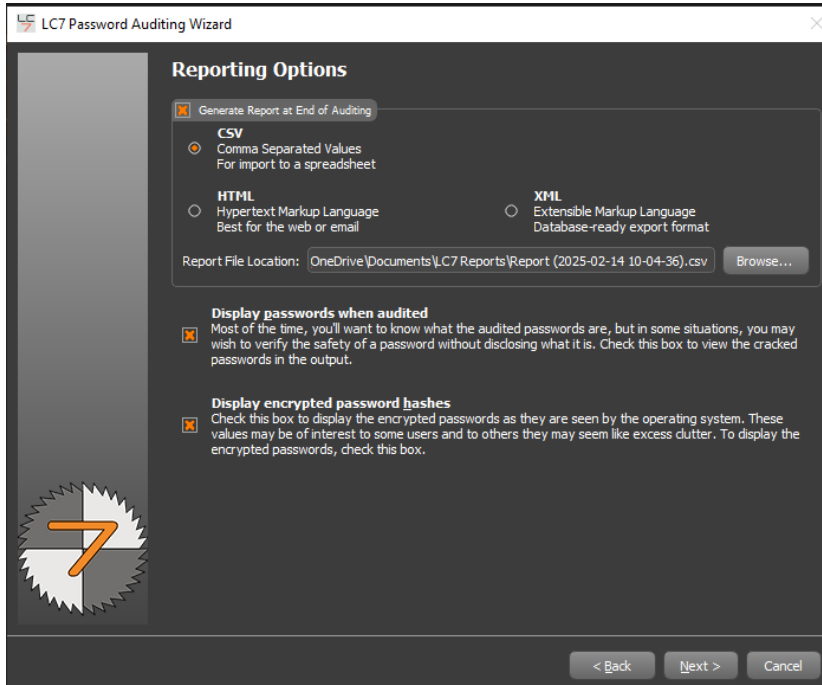
The screenshot shows the 'LC7 Password Auditing Wizard' window with the title 'Windows Import From Local Machine'. The instruction says 'Choose which credentials to use while performing the hash extraction:'. There are three radio button options: 'Use Logged-In User Credentials' (selected), 'Use Saved Credentials', and 'Use Specific User Credentials'. Below these is a 'Credentials' section with input fields for 'Username:', 'Password:', and 'Domain:'. There is also a checkbox for 'Save These Credentials'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'. On the left side of the window, there is a circular icon with a white background, a black border, and a large orange number '7'.

**Step 4: Select Quick Password Audit to initiate the attack.**



The screenshot shows the 'LC7 Password Auditing Wizard' window with the title 'Choose Audit Type'. The instruction says 'Choose the type of audit you would like to perform:'. There are four radio button options: 'Quick Password Audit' (selected), 'Common Password Audit', 'Thorough Password Audit', and 'Strong Password Audit'. Each option has a brief description. Below these is a 'Dictionary' section with the text: 'wordlist-medium.txt, 253525 words. No length limit, 1 hour maximum. 'Jumbo Plus' permutations set.' At the bottom are buttons for '< Back', 'Next >', and 'Cancel'. On the left side of the window, there is a circular icon with a white background, a black border, and a large orange number '7'.

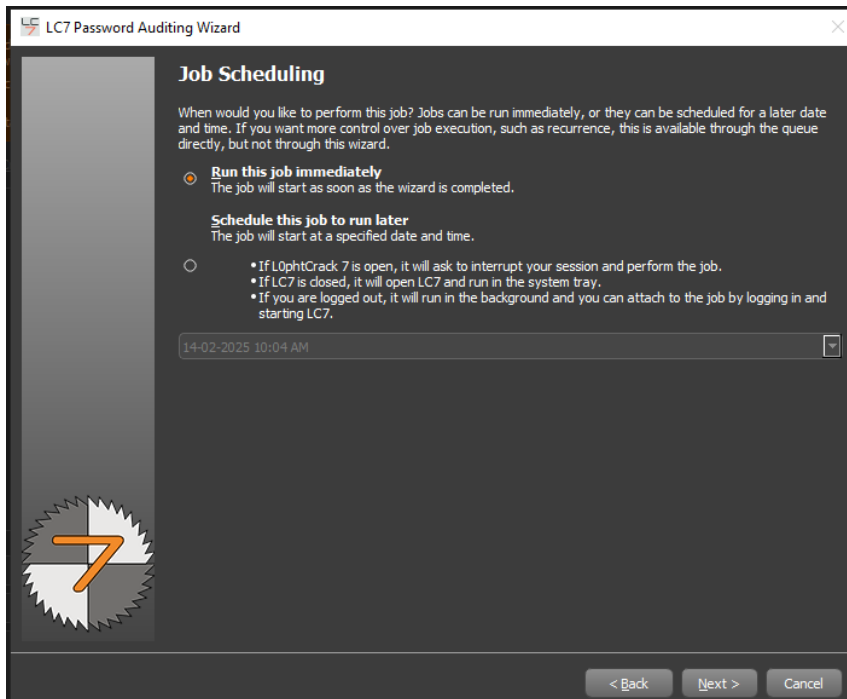
**Step 5:** If you want to generate Report , choose the desired file format.



The screenshot shows the 'Reporting Options' window of the LC7 Password Auditing Wizard. The window has a dark theme and a sidebar on the left with a circular icon containing a stylized '7'. The main content area is titled 'Reporting Options' and contains the following elements:

- A checkbox labeled 'Generate Report at End of Auditing' which is checked.
- Two radio button options for the report format:
  - CSV** (selected): Comma Separated Values. For import to a spreadsheet.
  - HTML**: Hypertext Markup Language. Best for the web or email.
  - XML**: Extensible Markup Language. Database-ready export format.
- A text field for 'Report File Location' showing 'OneDrive\Documents\LC7 Reports\Report (2025-02-14 10-04-36).csv' and a 'Browse...' button.
- A checkbox labeled 'Display passwords when audited' which is checked. Below it is explanatory text: 'Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.'
- A checkbox labeled 'Display encrypted password hashes' which is checked. Below it is explanatory text: 'Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.'
- At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

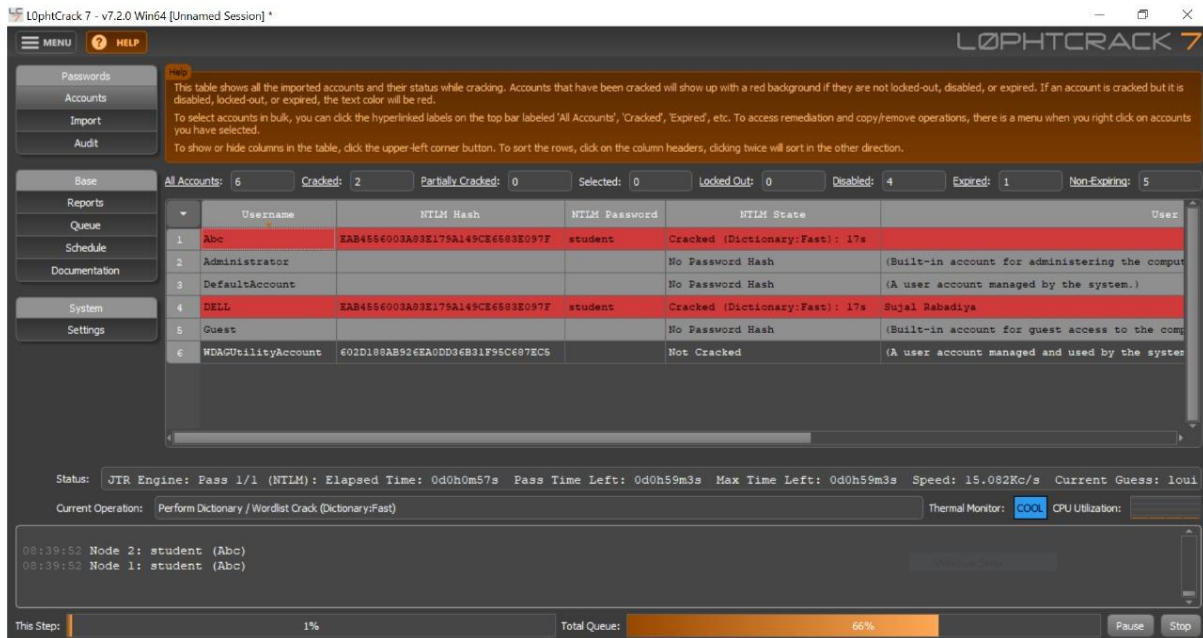
**Step 6:** Configure Job Scheduling (default: immediate execution).



The screenshot shows the 'Job Scheduling' window of the LC7 Password Auditing Wizard. The window has a dark theme and a sidebar on the left with a circular icon containing a stylized '7'. The main content area is titled 'Job Scheduling' and contains the following elements:

- Introductory text: 'When would you like to perform this job? Jobs can be run immediately, or they can be scheduled for a later date and time. If you want more control over job execution, such as recurrence, this is available through the queue directly, but not through this wizard.'
- Two radio button options:
  - Run this job immediately** (selected): The job will start as soon as the wizard is completed.
  - Schedule this job to run later**: The job will start at a specified date and time. Below this are three bullet points:
    - If L0phtCrack 7 is open, it will ask to interrupt your session and perform the job.
    - If LC7 is closed, it will open LC7 and run in the system tray.
    - If you are logged out, it will run in the background and you can attach to the job by logging in and starting LC7.
- A date and time selector showing '14-02-2025 10:04 AM' with a dropdown arrow.
- At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 7:** Click Run to start the password-cracking process.



## Output:

You can see in that Passwords is cracking after some time and its **student**.

## 2. Steps to Perform Password Cracking using John the Ripper:

**Step-1:** Install John the Ripper (if not installed) using `sudo apt install john` (Linux) or download it from the official site.

-use **Sudo apt install john**

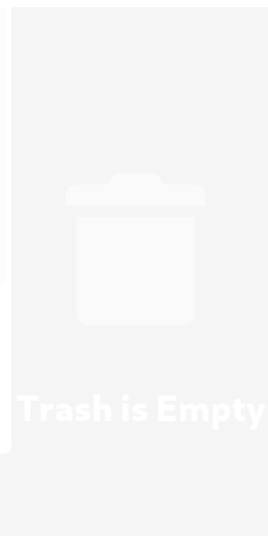
**Name:** Lakhani Ritesh Shaileshbhai

**Enrollment No:** 22010101099

**Date:** 15/02/2025

Step-2: Gather the password hash file from the target system.

```
(root@student)-[~] 65 (delta 1), reused 2 (delta 0), pack-reused 2458 (from 1)
# adduser testk
info: Adding user `testk' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testk' (1003) ...
info: Adding new user `testk' (1003) with group `testk (1003)' ...
info: Creating home directory `/home/testk' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testk
Enter the new value, or press ENTER for the default
  Full Name []: 0
  Room Number []: 0
  Work Phone []: 0
  Home Phone []: 0
  Other []: 0
Is the information correct? [Y/n] y
info: Adding new user `testk' to supplemental / extra groups `users' ...
info: Adding user `testk' to group `users' ...
```



```
_gvm:::20050:::
speech-dispatcher:::20050:::
fwupd-refresh:::20050:::
inetsim:::20050:::
geoclue:::20050:::
lightdm:::20050:::
gnome-remote-desktop:::20050:::
statd:::20050:::
saned:::20050:::
polkitd:::20050:::
rtkit:::20050:::
colord:::20050:::
Debian-gdm:::20050:::
nm-openvpn:::20050:::
nm-openconnect:::20050:::
student:$y$j9T$VkrIKywJM7yzdtOwYEGBB1$JFH1rBQqYXCxWogK0Mf7zV3aV3rKJuOCLW5n7urnmtC:20050:0:99999:7::
_dvwa:::20084:::
cups-pk-helper:::20118:::
test01:$y$j9T$0yBWoovBv/hXRFKRa3D/E/$ovhJeNjZarUoTRMOFj3krmezAiOP3NVzKig1rhp/8G8:20131:0:99999:7:::
test02:$y$j9T$JlF2JtsJsgPDkY8UcyQth.$kMBq9AFr.0kAD0W/yD1/PZxkLQ7nIwuhub7A9I5Iu35:20131:0:99999:7:::
testk:$y$j9T$A0Ma.K78358fj9kCDqbQx/$9qsam2VtQ7P5C4EA7p0jKQVn57KPIsU9939JR1xHYPC:20133:0:99999:7:::
testp:$y$j9T$Na0DhEIWLp1LFei0VM1gd.$qlFjB67Bnw6bb5zRMxxhDuwaVt9Y//SU3lpV38Sa4qC:20133:0:99999:7:::
```



**Name:** Lakhani Ritesh Shaileshbhai

**Enrollment No:** 22010101099

**Date:** 15/02/2025

```
# cat pass1.txt
root::!20050:0:99999:7:::
daemon:*:20050:0:99999:7:::
bin:*:20050:0:99999:7:::
sys:*:20050:0:99999:7:::
sync:*:20050:0:99999:7:::
games:*:20050:0:99999:7:::
man:*:20050:0:99999:7:::
lp:*:20050:0:99999:7:::
mail:*:20050:0:99999:7:::
news:*:20050:0:99999:7:::
uucp:*:20050:0:99999:7:::
proxy:*:20050:0:99999:7:::
www-data:*:20050:0:99999:7:::
backup:*:20050:0:99999:7:::
list:*:20050:0:99999:7:::
irc:*:20050:0:99999:7:::
_apt:*:20050:0:99999:7:::
nobody:*:20050:0:99999:7:::
systemd-networkd:*:20050:0:99999:7:::
_galera:*:20050:0:99999:7:::
mysql:*:20050:0:99999:7:::
tss:*:20050:0:99999:7:::
strongswan:*:20050:0:99999:7:::
systemd-timesyncd:*:20050:0:99999:7:::
rwhod:*:20050:0:99999:7:::
_gophish:*:20050:0:99999:7:::
iodine:*:20050:0:99999:7:::
messagebus:*:20050:0:99999:7:::
tcpdump:*:20050:0:99999:7:::
miredo:*:20050:0:99999:7:::
_rpc:*:20050:0:99999:7:::
Debian-snmpp:*:20050:0:99999:7:::
```

```
(student@student)-[~]
$ sudo adduser abc
info: Adding user `abc' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `abc' (1006) ...
info: Adding new user `abc' (1006) with group `abc (1006)' ...
info: Creating home directory `/home/abc' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for abc
Enter the new value, or press ENTER for the default
  Full Name []: ki
  Room Number []: 0
  Work Phone []: 0
  Home Phone []: 0
  Other []: 0
Is the information correct? [Y/n] y
info: Adding new user `abc' to supplemental / extra groups `users' ...
info: Adding user `abc' to group `users' ...
```

Screenshot captured

You can paste the image from the clipboard.

Step-3: Run john --format=<hash-type> <hash-file> to start cracking.

```
(root@student)-[~]
# nano pass1.txt
(root@student)-[~]
# nano pass1.txt
(root@student)-[~]
# cat pass1.txt
estk:$y$j9T$A0Ma.K78358fj9kCDqbQx/$9qsam2VtQ7P5C4EA7p0jKQVn57KPIsU9939JR1xHYPC:20133:0:99999:7:::
estp:$y$j9T$Na0DhEIWlp1LFei0VM1gd.$qLFjB67Bnw6bb5zRMxxhDuwaVt9Y//SU3lpV38Sa4qC:20133:0:99999:7:::
(root@student)-[~]
# john --format=crypt pass1.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descript 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 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Learning: Only 16 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
2345 (testk)
isdf (testp)
g 0:00:00:43 DONE 2/3 (2025-02-14 08:25) 0.04601g/s 144.6p/s 147.2c/s 147.2C/s lacrosse..pumpkin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
(student@student)-[~]
$ ls
1.pcap Demo Downloads Pictures data1.html data4.html pass.txt scan.xml test_db.db wordlist
1016 Desktop Music darshan.txt data2.html get-pip.py passlist.txt second.html vh.html wordlist.txt
DVWA Documents Nessus-10.8.3-ubuntu1604_amd64.deb data.html data3.html m.pcap pwdump1 sniffed.pcap w3af

(student@student)-[~]
$ sudo cat wordlist.txt
[sudo] password for student:
12345
123
Ritesh

(student@student)-[~]
$ sudo adduser abc
info: Adding user 'abc' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'abc' (1006) ...
```