PART A – John the Ripper

Open the INFO6001 **Windows 7** VMware image (Login as Administrator password: Windows1).
Create a folder named **pwd** off the root of drive C.
From the **c:\security\PwdCrackers** folder, copy the **john-17** folder and the **pwdump7** folder to the **c:\pwd** folder .

Preparing the password files

Delete any users created in previous labs .
Open start menu – right click on computer and select **Manage.**
Under **System Tools** go to Local Users and Groups \ users
Create 5 new ***standard*** users in Windows with names ***user1, user2, user3 & user4*** (make sure the password option: ***user must change the password at next logon*** is not checked!).

Give ***user1*** a simple password **longer** than 7 characters. **eg. elephant**
Give ***user2*** a simple password less than 7 characters. **eg. horse**
Give ***user3*** a password with at least 15 characters. **eg. myscreencaptures**
Give ***user4*** a complex password of 6 characters. **eg. Pa$$Me**
Create a 5th user with your ***FOLusername*** and password. **Fanshawe1 (do not use the _ in your name)**

Extract the password hash from the SAM

Generate the password files using the pwdump7 utility.
Open a command prompt and change to the **c:\pwd\pwdump7** directory and type: c:\pwd\pwdump7>
pwdump7 > pwdcrack
The output of the pwdump7 command is redirected into a new file named **pwdcrack** which is a text file that now contains the password hashes.

View the password hashes

C:\pwd\ pwdump7> **type pwdcrack**

1. ***Take a screen capture of the list of username and password hashes***

Move or copy the file **pwdcrack** into the **c:\pwd\john-17\run** folder.
The **john-386.exe** program must be run from the command prompt C:\pwd\john-17\run>
john-386.exe pwdcrack

The program could take considerable time to try all the combinations. To see the current combinations being compared press the enter key. To break out of the session press Crtl + C. In the space below record the first password cracked. First password cracked: _____
Note the program output shows the password as each group of 7 characters.

2. ***Take a screen capture of the list of passwords that have been cracked***

To view a summary of the passwords which have been cracked:
C:\pwd\john-17\run> **john-386 –show pwdcrack**
The result has been saved to a file. To view the file enter the command below C:\pwd\john-17\run>
type john.pot
Delete john.pot before running the john-386 file a second time.

For brute force cracking

Type: **john-386 –i pwdcrack**
Press the enter key to have the current password guess displayed.
Brute force cracking of password Windows1 may take over 20 minutes- **do this later to save time.**
Press **CTRL + C** to break out of the program.

PART B – LC6

LC6 is trial evaluation copy of a password auditing tool that is used for testing the strength of Windows passwords.

From FOL course content Lab Content/**Week 13**, download **lc6setup_V6.0.20.zip**
Move the compressed installer to Windows 7 VM, extract the executable and Install it. If asked to install WinPcap 4.1.3, click Next and finish installation.

Go to start menu and run L0phtCrack 6 This
is an evaluation version. Click OK.
Choose the following options:
Select Next
Retrieve from local machine → Next
Strong Password Audit → Next
Select all reporting styles → Next
Finish

The program will now begin to crack the passwords on the system.
View the results displayed from the password audit.

Note the display shows both the LM and NTLM passwords being cracked.

3. Take a screen capture of the list of passwords that have been cracked

LC6 has the capability of doing a dictionary, hybrid or brute force cracking of passwords.
Under **Session (Auditing)**, **Session Options** check out the options that are available.
You can set options for the Dictionary list to be used, the number of characters to prepend and append to the dictionary word file and the special characters that can be used in brute force cracking passwords.

4. Take a screen capture of the passwords cracking options

The dictionary can be viewed in Wordpad.
Open C:\Program Files\L0phtCrack 6\words-english.dic
You could add your own dictionary list to be used by the program.

PART C - Local Security Policy

Start → Control Panel→ Administrative Tools → Local Security Policy
Expand Local Policy select → Security Options
In the right-hand panel
Select → **Network Security: Do not store LAN Manager HASH values**
Right click and select properties → Enabled
Exit from Local Security Policy
Change password for ***user1*** to **laptop**
Note: this password (laptop) should be as easy to crack as elephant if LAN Manager HASH is stored.
Close LC6 if opens and re-lunch the application.
View the password **hash** for the user account ***user1***
Expand LC6 window so LM Hash and NTLM Hash are visible.
How is this password crack different from the previous attempts passwords?

5. Take a screen capture of the list of passwords cracked