**1. Use John the Ripper tool to crack the passwords for the three different user accounts you have created by using the three different methods: single, wordlist and incremental. Explain your findings and include screenshots.**

```
root@kali:~# john password1
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
user123          (user1)
Orange           (user2)
2g 0:00:00:37 6.67% 2/3 (ETA: 12:31:54) 0.05389g/s 466.6p/s 821.9c/s 821.9C/s ninas..fishings
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@kali:~#
```

Single – utilizes the GECOS fields as candidate passwords, and a wordlist.
The password User123 was cracked very quickly as it is a combination of the username and room number. The password Orange was also easily cracked as it is a typical word.

```
root@kali:~# john -wordlist=/usr/share/john/password.lst password1
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 DONE (2019-03-11 12:29) 0g/s 457.5p/s 915.0c/s 915.0C/s paagal..sss
Session completed
root@kali:~#
```

Wordlist - utilizes a specified wordlist.
Orange had already been cracked by single mode but would have been otherwise by wordlist. The other two accounts use a mix of number and letters, so wordlist was no help in cracking those passwords.

```
root@kali:~# john -incremental:lanman password1
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:40  0g/s 467.8p/s 936.1c/s 936.1C/s MILDEE1..MINANDS
0g 0:00:02:41  0g/s 467.8p/s 936.0c/s 936.0C/s MEGIENE..METHOPO
0g 0:00:02:46  0g/s 467.5p/s 935.5c/s 935.5C/s ALANCIS..ALB1120
0g 0:00:03:32  0g/s 468.1p/s 936.2c/s 936.2C/s BUDELA1..BUNNEY0
0g 0:00:05:56  0g/s 467.3p/s 934.9c/s 934.9C/s MANIO11..MATAMEL
0g 0:00:09:13  0g/s 469.2p/s 938.5c/s 938.5C/s JINTYA..JIGUEN
0g 0:00:09:14  0g/s 469.2p/s 938.4c/s 938.4C/s JILEST..JILALE
0g 0:00:13:05  0g/s 471.6p/s 943.2c/s 943.2C/s PASHULA..PASTIAL
0g 0:00:16:00  0g/s 471.2p/s 942.4c/s 942.4C/s PUPATOR..PUMBRUC
0g 0:00:24:08  0g/s 469.6p/s 939.2c/s 939.2C/s A8I..IA)
0g 0:00:39:46  0g/s 468.5p/s 937.0c/s 937.0C/s LAMBELO..LAMBAMI
0g 0:00:47:19  0g/s 468.9p/s 937.9c/s 937.9C/s SASARDI..SASALLO
0g 0:00:52:15  0g/s 469.3p/s 938.7c/s 938.7C/s JCRES..JCRY1
0g 0:00:57:06  0g/s 457.3p/s 914.7c/s 914.7C/s CONTUPI..CONGKOR
0g 0:00:57:19  0g/s 456.7p/s 913.4c/s 913.4C/s CR19424..CR13610
Session aborted
root@kali:~#
```

Incremental – tries all possible character combinations
The downside of trying every possible character combination is the resources required. I ran it for an hour and aborted the session. I would have liked to have gotten one of the two remaining accounts cracked but incremental mode is time consuming.

**2. Inquire about tools to brute force Microsoft Windows systems. Write a report with technical information i.e. name of the tool, required steps for the attack, Microsoft Windows version affected, etc.**

L0phtCrack is a password auditing and recovery tool designed to test password strength. It is sometimes used to retrieve lost Unix and Microsoft Windows passwords through brute-force, dictionary, rainbow tables and hybrid attacks. The most recent version L0phtCrack 7 works on Windows XP up to Windows 10. Simply choose a target operating system, choose the source machine, enter source machine credentials, choose the audit type, and finally select your preferences for the report.

**3. Using mkpasswd tool generate the same hash for one of your user accounts. Include screenshots to demonstrate you succeed.**


**4. What is Key stretching technique and how it is related to Salt and Pepper?**

Key stretching is used to make a weak key more secure against brute-force attacks. Salt and pepper is a method key stretching may utilize in order to secure a key.

**5. Mention two differences and two similarities between Salt and Pepper.**

Salt and pepper are both utilized in cryptographic hash functions and append random data to some other data. However, salt is appended to the front of the string and may be stored alongside the hash value while pepper is appended to the end of the string and stored in a separate location or not at all.