Information Security Technologies COMP607
Assignment Part 2 (20%)

Instructions:

1. Type your answers on A4 size paper.
2. The assignment must be completed in English.
3. Some of the questions are intentionally general and you are encouraged to research and write about some aspects of the questions that interest you.
4. It must be your own work. Do not copy material from anywhere as it will be penalised. Canvas has a pliagarism detection mechanism.
5. Submission: Convert your document to pdf format and submit in AUT Canvas before the deadline. Do not zip your files, submit multiple files is necessary.

Question 1: Vulnerabilities and Attacks

Research on attacks on fileless virus attacks. Choose one attack. Describe and discuss in not less than 100 words, how the attack works, who are affected, how it can be mitigated, what counter measures are available, etc. (10 marks)

1. The "Kovter" trojan, which rose to popularity due to its fileless persistence mechanism, is a prominent example of a fileless viral infection. Kovter spreads largely through malicious email attachments and drive-by downloads. Once performed, it remains in the system's registry, leaving no files on the disk, making it impossible for typical antivirus software to identify and uninstall.
2. Kovter functions by injecting malicious code into normal programs running in memory, such as PowerShell or Windows Management Instrumentation (WMI), allowing it to carry out its actions undetected. It frequently functions as click-fraud malware or a ransomware downloader.
3. The assault primarily targets Windows users, particularly those with out-of-date computers or poor security measures. Enterprises may be particularly affected owing to the possibility of extensive harm across networked systems.
4. Mitigation strategies include:
   - **Behavior-based detection:** Utilizing security solutions that analyze system behavior to detect anomalies, instead of depending only on signature-based detection methods.
   - **Regular updates:** Updating operating systems and applications to address vulnerabilities that might be exploited by fileless malware.
   - **Application whitelisting:** Allowing only approved programs to run can prevent unauthorized scripts or executables from executing.
   - **User education:** Training users to recognize and avoid phishing attempts and suspicious links that could lead to a fileless malware infection.
   - **Enhanced monitoring:** Implementing advanced threat detection tools that can identify and alert on suspicious registry or memory changes.
   - **Privilege restriction:** Limiting user privileges to reduce the potential impact of an attack and prevent malware from making significant system changes.
5. Organizations can enhance their defense against fileless malware by utilizing endpoint detection and response (EDR) platforms. These platforms analyze system behavior to identify patterns and anomalies associated with fileless malware. Moreover, implementing a

comprehensive cybersecurity framework that encompasses network segmentation, intrusion detection systems, and regular security audits can proactively safeguard organizations against these threats.

Question 2: Authentication Technologies

Cracking password using online rainbow table cracker at https://crackstation.net/
For the following, you need to take a screenshots of your work and results, and paste them into your assignment to show you have done them.

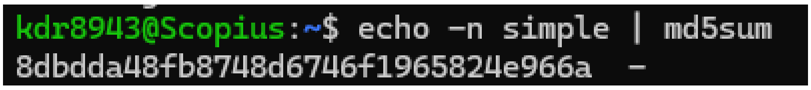
a. Choose 3 passwords of the following types:

password1: simple 6 character password from common English words,
password2: using password1 above, add 2 numbers to the end,
password3: using password 1 above, substitute some characters with symbols and numers.

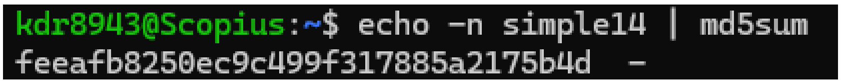
password1: simple
password2: simple14
password3: s@mpl@14

b. For each one generate the MD5 hash (use online tool or Linux), e.g.

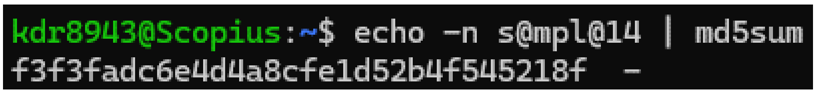
```
$ echo -n simple | md5sum
8dbdda48fb8748d6746f1965824e966a  -
```



```
kdr8943@Scopius:~$ echo -n simple | md5sum
8dbdda48fb8748d6746f1965824e966a  -
```



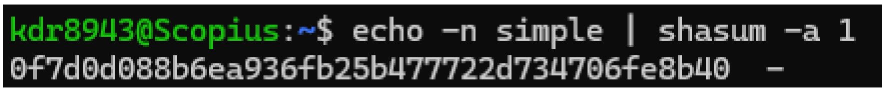
```
kdr8943@Scopius:~$ echo -n simple14 | md5sum
feeafb8250ec9c499f317885a2175b4d  -
```



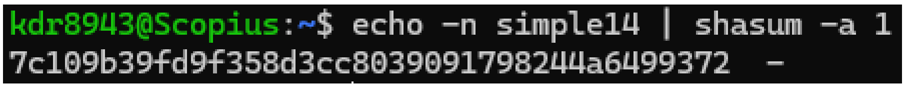
```
kdr8943@Scopius:~$ echo -n s@mpl@14 | md5sum
f3f3fadc6e4d4a8cfe1d52b4f545218f  -
```

c. For each one generate the SHA1 hash, e.g. in Linux

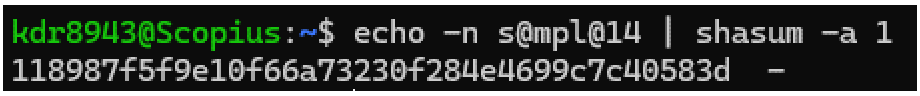
```
$ echo -n password | shasum
0f7d0d088b6ea936fb25b477722d734706fe8b40  -
```



```
kdr8943@Scopius:~$ echo -n simple | shasum -a 1
0f7d0d088b6ea936fb25b477722d734706fe8b40  -
```



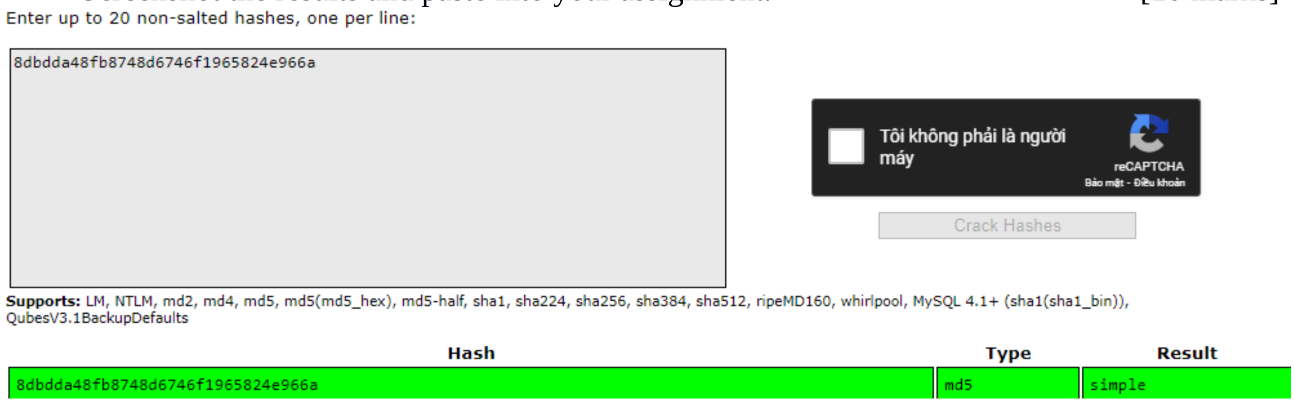
```
kdr8943@Scopius:~$ echo -n simple14 | shasum -a 1
7c109b39fd9f358d3cc8039091798244a6499372  -
```



```
kdr8943@Scopius:~$ echo -n s@mpl@14 | shasum -a 1
118987f5f9e10f66a73230f284e4699c7c40583d  -
```

d. Copy each hash and paste into https://crackstation.net/ to obtain the plaintext password. You should choose passwords such that password1 and password2 are successful, password3 is unsuccessful.

Screenshot the results and paste into your assignment. [10 marks]

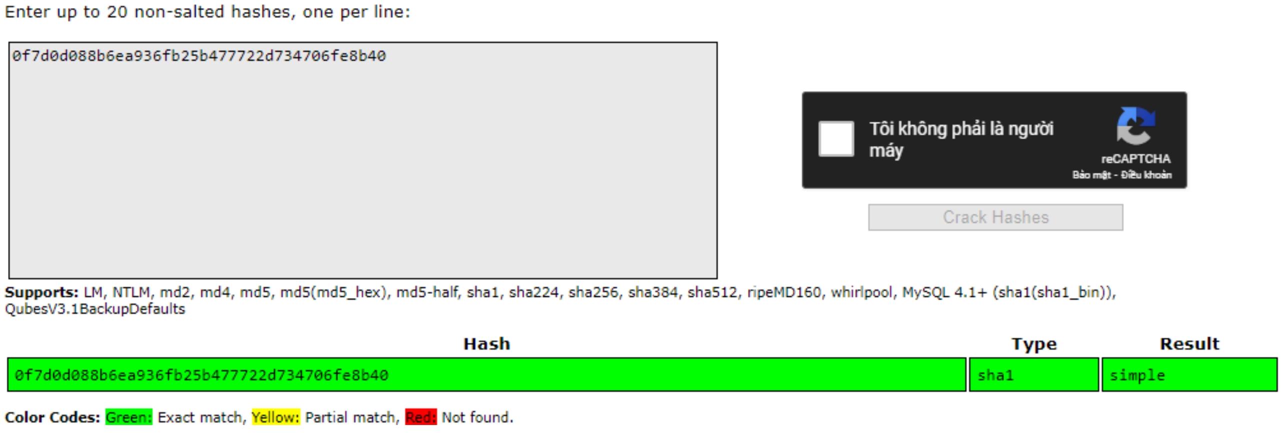


Enter up to 20 non-salted hashes, one per line:

```
8dbdda48fb8748d6746f1965824e966a
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8dbdda48fb8748d6746f1965824e966a	md5	simple



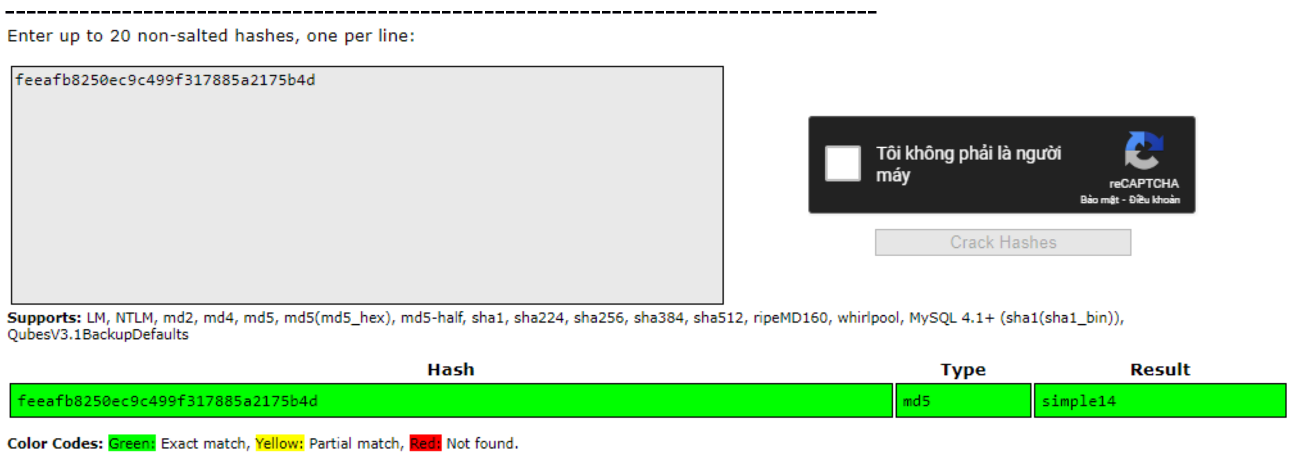
Enter up to 20 non-salted hashes, one per line:

```
0f7d0d088b6ea936fb25b477722d734706fe8b40
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0f7d0d088b6ea936fb25b477722d734706fe8b40	sha1	simple

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



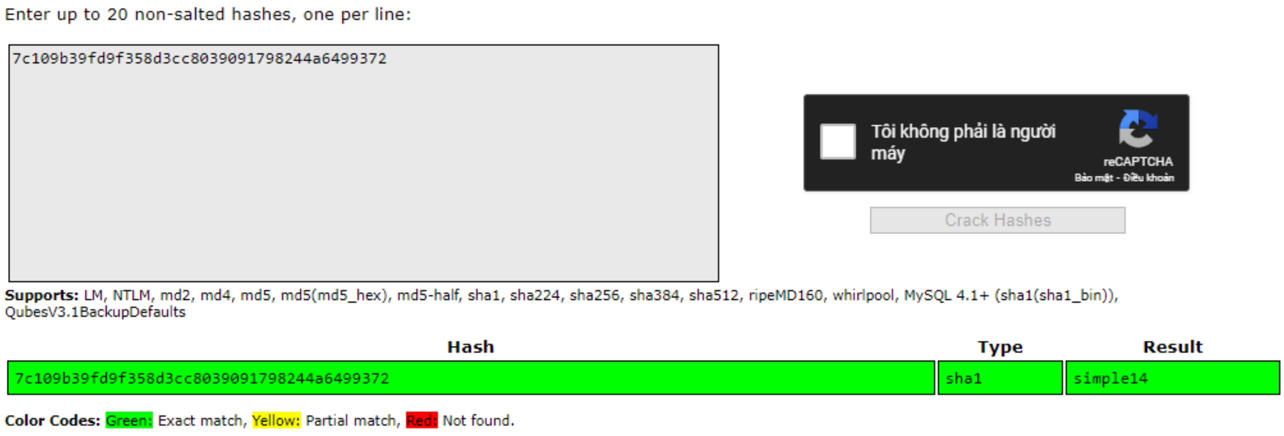
Enter up to 20 non-salted hashes, one per line:

```
feeafb8250ec9c499f317885a2175b4d
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
feeafb8250ec9c499f317885a2175b4d	md5	simple14

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



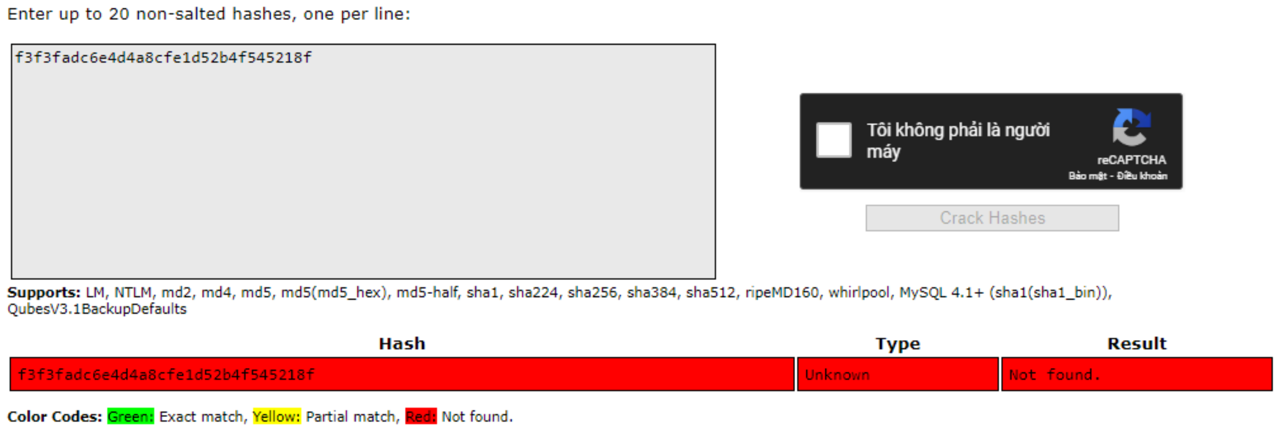
Enter up to 20 non-salted hashes, one per line:

```
7c109b39fd9f358d3cc8039091798244a6499372
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
7c109b39fd9f358d3cc8039091798244a6499372	sha1	simple14

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



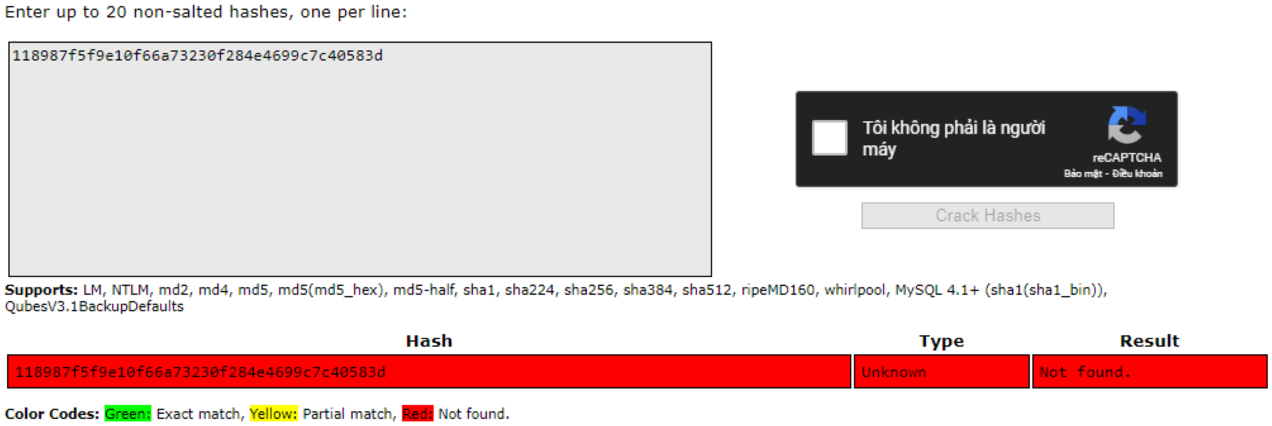
Enter up to 20 non-salted hashes, one per line:

```
f3f3fadc6e4d4a8cfe1d52b4f545218f
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f3f3fadc6e4d4a8cfe1d52b4f545218f	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



Enter up to 20 non-salted hashes, one per line:

```
118987f5f9e10f66a73230f284e4699c7c40583d
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

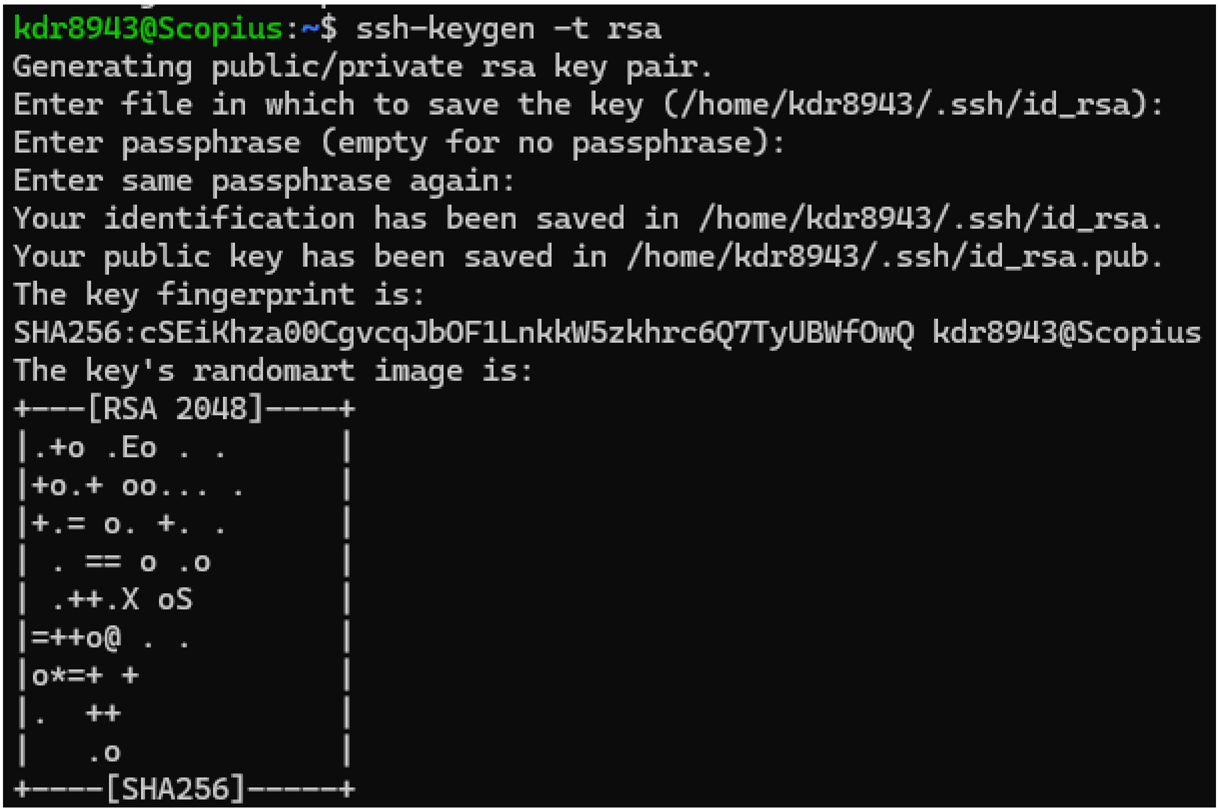
Hash	Type	Result
118987f5f9e10f66a73230f284e4699c7c40583d	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Question 3: Identification and AAA

Research the Internet to implement login to the SSH server at *scopius.aut.ac.nz* using your public key (what you have) -- i.e. passwordless login. The exact commands may be different if you use Linux, Windows, or Mac, but it will consist of the following steps:

(i) Create your *rsa* ssh private and public key pair in your local PC. (Eg. in Linux using *ssh-keygen*).



```
kdr8943@Scopius:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kdr8943/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kdr8943/.ssh/id_rsa.
Your public key has been saved in /home/kdr8943/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:cSEiKhza00CgvcqJbOF1LnkkW5zkhrc6Q7TyUBWfOwQ kdr8943@Scopius
The key's randomart image is:
+---[RSA 2048]----+
|.+o .Eo . .      |
|+o.+ oo... .     |
|+.= o. +. .      |
| . == o .o       |
| .++.X oS        |
|=++o@ . .        |
|o*=+ +           |
|.  ++            |
|    .o           |
+----[SHA256]-----+
```

(ii) Insert/copy your public key to the Linux server in the *authorized_keys* file in the .ssh/ folder under your *home* folder. You may need to first create there the .ssh folder and *authorized_keys* file, e.g.

In your home directory in the Linux server :

```
$ mkdir .ssh
$ cd .ssh
$ touch authorized_keys
```

Submission: Capture the screenshots of the steps and login results and paste into you assignment. (10 marks)

Question 4: Wireless Security

Research and write using not less than 200 words describing and explaining the various security risks involved with public and home WiFi networks. You should describe the risks, how they can occur and suggest how they can be mitigated. (10 marks)

Users should be cautious of security risks associated with both public WiFi networks and home WiFi networks to safeguard their sensitive information. Public WiFi networks, like those in cafes, airports, and hotels, are especially susceptible to attacks due to their lack of encryption and open nature. One prevalent threat is the man-in-the-middle attack, where hackers can intercept data exchanged between a user's device and the network, potentially resulting in the compromise of personal information, login details, and financial data.

Cybercriminals often create malicious hotspots on public WiFi networks to deceive users into connecting to them, posing a significant risk. These hackers can then carry out a range of attacks, such as installing malware and intercepting data. Moreover, unsecured public WiFi networks are vulnerable to eavesdropping, enabling attackers to monitor network traffic and capture sensitive information.

Security risks are a concern for home WiFi networks, as hackers or neighbors can gain unauthorized access. Attackers can exploit weak passwords, outdated firmware, and unsecured network configurations to compromise devices and launch various attacks like ransomware infections and data theft.

To improve the security of both public and home WiFi networks, users can take precautions. For public networks, it is recommended to use a virtual private network (VPN) to encrypt data traffic and protect against eavesdropping and man-in-the-middle attacks. Additionally, users should refrain from accessing sensitive information or logging into accounts with personal or financial data while connected to public WiFi.

It is recommended for users of home WiFi networks to modify default router passwords to strong, unique ones, activate WPA2 or WPA3 encryption, and consistently update router firmware to address security weaknesses. Creating separate guest networks and IoT networks through network segmentation can aid in containing potential security risks. Furthermore, activating firewall protection and installing antivirus software on all connected devices can offer an additional level of protection against cyberattacks.

Users may lessen their vulnerability to cyber attacks and protect their privacy and sensitive information by taking proactive steps to secure both public and residential WiFi networks.

Question 5: Business continuity

The following diagram shows implementation of RAID-5 with 3 disks. The data is writen on the disks in blocks. Each block consists of 8 ASCII characters (8 bits).

A file consisting of 6 blocks A1, A2, .., A6 are striped across the 3 disks with parity blocks A_{12p}, A_{34p} and A_{56p} for the respective blocks, e.g. A_{12p} for A1 and A2, etc., as follows:

Disk 1	Disk 2	Disk 3
A1 = IDEALOGI	A2	A_{12p}
A3 = IMPLE ID	A_{34p}	A4 = EAS DISG
A_{56p}=	A5	A6 = SCIENCE

The binary bits for each character in the block are as follows. The commas (,) are separators only for display.

Disk 1

A1 = 01001001,01000100,01000101,01000001,01001100,01001111,01000111,01001001
A3 = 01001001,01001101,01010000,01001100,01000101,00100000,01001001,01000100
A_{56p}= 01110101,00011010,00010000,00001100,00000001,01101110,00000010,00010110

Disk 3

A_{12p} = 00001100,00010111,01100101,00000000,00011110,00001010,01100111,00011010
A4 = 01000101,01000001,01010011,00100000,01000100,01001001,01010011,01000111
A6 = 00100000,01010011,01000011,01001001,01000101,01001110,01000011,01000101

Disk 2 suffered a catastrophic failure. You are required to recover the data blocks A2 and A5. What is the content of the recovered file? [10 marks]

Hint: You can use Genius to convert binary to ASCII characters, for example:

```
genius> IntegerOutputBase=2
genius> x=[2\1001001, 2\1000100, 2\1000101, 2\1000001, 2\1001100, 2\1001111,
2\1000111, 2\1001001]
genius> ASCIIToString(x)
= "IDEALOGI"
```