**Information Security Technologies COMP607**  
**Assignment Part 2 (20%)**

**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)

PowerShell-based attacks are a type of fileless virus attack that exploit the PowerShell scripting language in Windows operating systems. These attacks allow malicious commands to be executed directly in memory, leaving no traces on the disk. It can be difficult to differentiate between legitimate and malicious PowerShell activities, making detection challenging for individuals, businesses, and organizations using Windows-based systems.

To mitigate these attacks, robust security measures should be implemented. This includes using endpoint detection and response solutions, network monitoring, and access controls to limit PowerShell usage to authorized personnel. Regular security awareness training can also help users identify suspicious PowerShell activities.

Countermeasures against PowerShell-based attacks involve monitoring for unusual or unauthorized commands, restricting PowerShell script execution to trusted sources, implementing application whitelisting, and keeping PowerShell versions up to date to take advantage of built-in security enhancements. Advanced threat detection tools that can identify anomalous behavior patterns can also aid in the early detection and prevention of these attacks.

**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: simple12

password3: s@mp1e12

**b**. For each one generate the MD5 hash (use online tool or Linux), e.g.  
$ echo -n simple | md5sum  
8dbdda48fb8748d6746f1965824e966a -

* For password1:



* For password2:



* For password3:



**c**. For each one generate the SHA1 hash, e.g. in Linux  
$ echo -n password | shasum  
0f7d0d088b6ea936fb25b477722d734706fe8b40 -

* For password1:



* For password2:

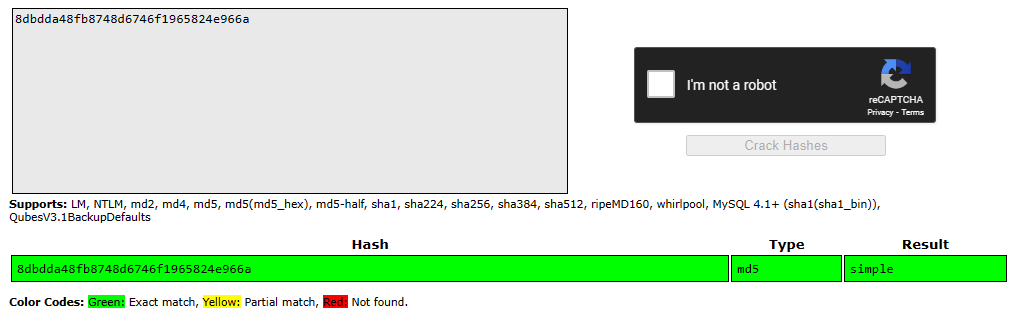


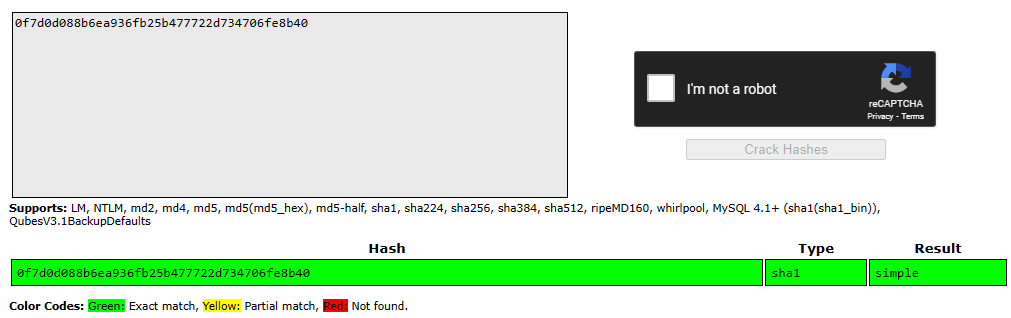
* For password3:



**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]

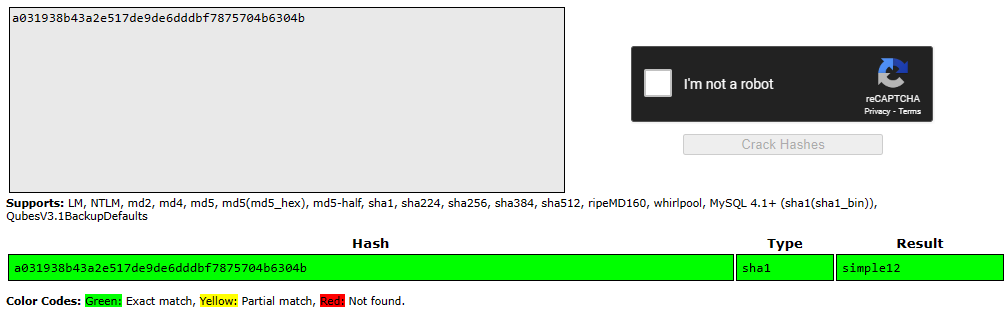
* For password1:



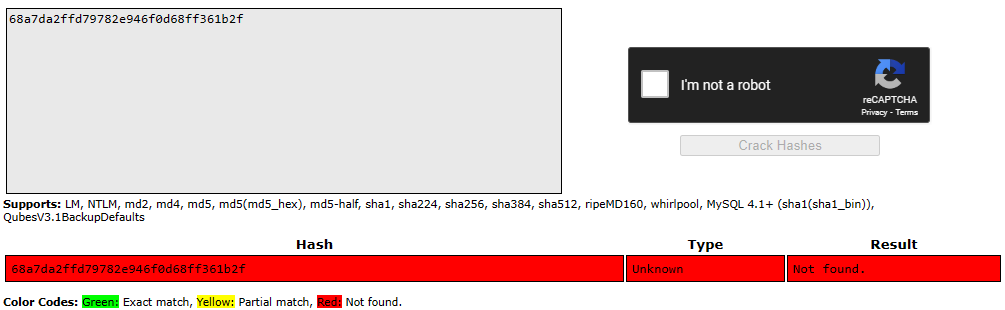


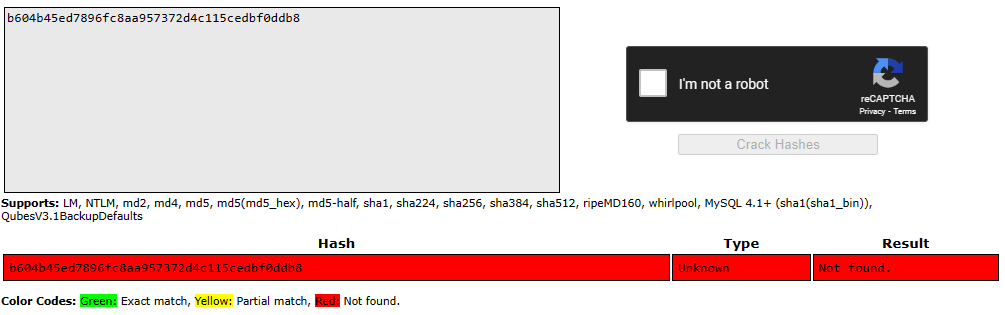
* For password2:



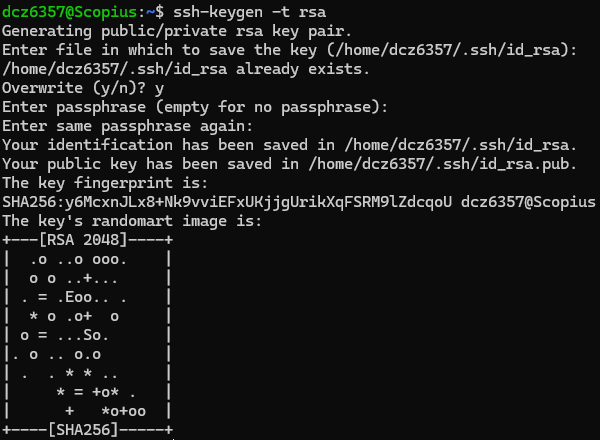


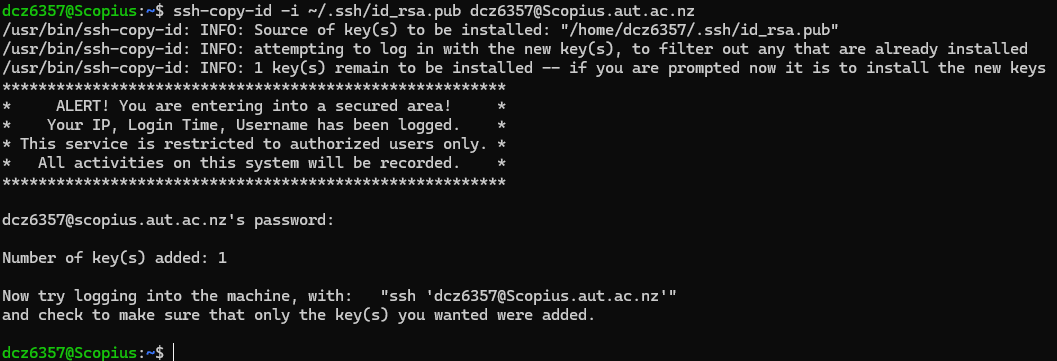
* For password3:

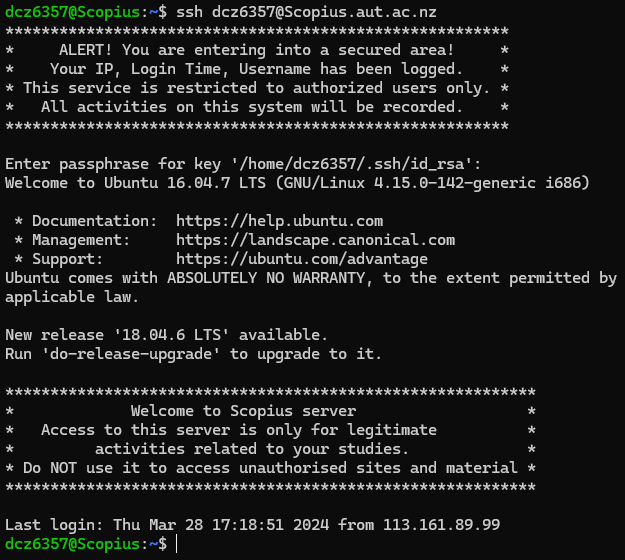




**Question 3: Identification and AAA**  
Research the Internet to implement login to the SSH server at scopius.aut.ac.nz using your public key (what you have) -- i.e. passwordless login. The exact commands may be different if you use Linux, Windows, or Mac, but it will consist of the following steps:  
 (i) Create your rsa ssh private and public key pair in your local PC. (Eg. in Linux using ssh-keygen).

  
 (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)

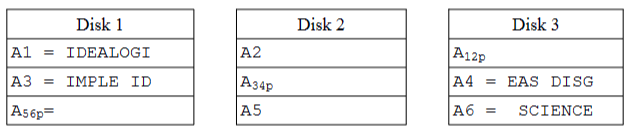
**Question 4: Wireless Security**  
Research and write using not less than 200 words describing and explaining the various security risks involved with public and home WiFi networks. You should describe the risks, how they can occur and suggest how they can be mitigated. (10 marks)

Public and home WiFi networks pose numerous security risks due to their vulnerabilities, making them easy targets for malicious actors. These risks can lead to the exposure of sensitive data, personal information, and even the security of connected devices. It is essential to understand these risks and take appropriate measures to protect against potential threats.

Eavesdropping on public WiFi networks is a significant risk, as hackers can intercept unencrypted data transmissions to steal sensitive information like login credentials and financial details. Users should be cautious when using unsecured connections and opt for encryption protocols like HTTPS to enhance security. Rogue access points are another threat, where attackers create fake hotspots to deceive users and launch attacks. Verifying network legitimacy and using VPNs can help prevent falling victim to such attacks.

Home WiFi networks are also at risk from unauthorized access and weak password security. Default or easily guessable passwords can be exploited by attackers to compromise the network and connected devices. To mitigate this risk, users should change default passwords to strong ones and enable encryption protocols on their routers. Both public and home WiFi networks are vulnerable to phishing attacks, emphasizing the importance of staying vigilant and cautious while using these 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 A12p, A34p and A56p for the respective blocks, e.g. A12p for A1 and A2, etc., as follows:



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  
A56p= 01110101,00011010,00010000,00001100,00000001,01101110,00000010,00010110

Disk 3  
A12p = 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"