**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 plagiarism 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)

Fileless virus attacks, also known as fileless malware attacks. Unlike a traditional virus, the code for the fileless virus is not stored in a file or be installed in victim computer. Alternatively, it loads directly into memory disk and run immediately.

One of the largest and most notable files malware attacks in history is the “Power Ghost” malware attacks, which was discovered in 2018. It’s a crypto-miner malware designed to stealthily mine crypto-currency on infected system. First, it’s enter the system through various ways, including phishing mails, malicious attachments, exploit kits. Then it’s operated itself in the memory disk, launch its malicious code into PowerShell or Window Management. Next, Power Ghost infiltrates systems to mine cryptocurrency, leveraging PowerShell for stealth. It exploits vulnerabilities or uses phishing to gain access, then deploys PowerShell scripts to download and run malware. These scripts establish persistence, disable security measures, and initiate cryptocurrency mining.

To mitigate, organizations should monitor PowerShell usage, restrict script execution, and employ application whitelisting. Regular updates and phishing awareness training are also essential defences. To mitigate Power Ghost attacks, organizations should prioritize patch management, deploying endpoint protection with behaviour-based detection, and network segmentation. Access control measures should restrict user permissions, while email and web filtering solutions block malicious content. Security awareness training helps employees recognize and report suspicious activity. An incident response plan outlines procedures for detecting, containing, and mitigating attacks. Network monitoring and logging are essential for detecting unusual activity. By implementing these measures, organizations can effectively reduce the risk posed by Power Ghost malware and enhance their overall cybersecurity posture.

**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: expert

-password2: expert32

-password3:$xper132

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]

Password1:

A screenshot of a computer

Description automatically generated

Password2:

A screenshot of a computer

Description automatically generated

Password3:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**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:

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

A screenshot of a computer program

Description automatically generated

(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)

A blue screen with white text

Description automatically generated

**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 Wi-Fi networks. You should describe the risks, how they can occur and suggest how they can be mitigated. (10 marks)

First, both public and home Wi-Fi networks are at risk of being compromised by various security threats due to their inherent vulnerabilities. One of the most significant dangers is eavesdropping, where cyber attackers can intercept network data, potentially gaining access to sensitive information such as login credentials and personal details.

Secondly, unauthorized access is another major concern, often made possible by weak passwords or outdated router firmware, which can allow attackers to exploit vulnerabilities or engage in malicious activities. Man-in-the-middle attacks are also a prevalent threat, enabling hackers to intercept and manipulate data exchanges between users, leading to potential data breaches and privacy violations.

Thirdly, to address these security risks effectively, it is crucial to implement protective measures such as enabling encryption protocols like WPA3, utilizing VPNs for secure connections, setting up strong and unique passwords, regularly updating router firmware, and deploying firewalls to block unauthorized access attempts. Furthermore, utilizing secure protocols like HTTPS and implementing two-factor authentication can significantly enhance protection against potential attacks.

Finally, in addition to technical safeguards, regular monitoring of network traffic and educating users about best practices for Wi-Fi security are essential steps to ensure a secure network environment. By taking proactive measures and staying informed about the latest security threats, both individuals and organizations can better protect themselves against potential cyber threats and safeguard their sensitive information.

**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:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Disk 1 |  | Disk 2 |  | Disk 3 |
| A1 = IDEALOGI | A2 |  | A12p |
| A3 = IMPLE ID | A34p |  | A4 = EAS DISG |
| A56p= | 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

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"

A blue screen with white text

Description automatically generated

A2:

A blue screen with white text

Description automatically generated

A5:

A blue screen with white text

Description automatically generated