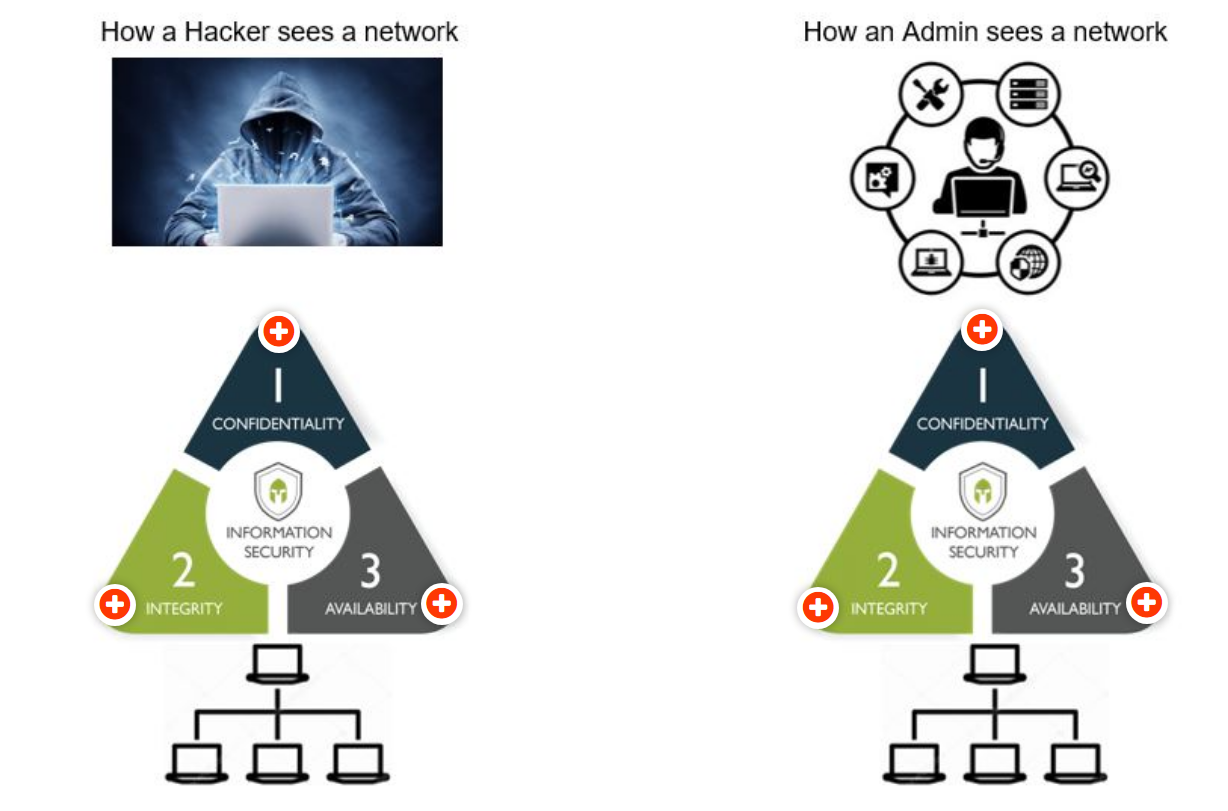
**SECURITY PRINCIPLES**

# WEEK 1: TENETS (PRINCIPLES) OF CYBER SECURITY

## CIA TRIAD



## REFERENCES

UniSA Slides

[WHAT IS CIA TRIAD – F5](https://www.f5.com/labs/articles/education/what-is-the-cia-triad)

## OVERVIEW

CIA TRIAD = CONFIDENTIALITY + INTEGRITY + AVAILABILITY

#### Definition

=> **A SECURITY MODEL**

=> Guide policies for information security in a organization

#### Purpose

To protect a network and its data (information), use security model as CIA TRIAD to design security plan.

## CONFIDENTIALITY

### Definition

*“The property that information is not disclosed to unauthorized individuals, processes, or devices”*

“It’s about ***controlling access to data to prevent unauthorized disclosure***. Typically, this involves ensuring that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access.”

### How will confidentiality be violated?

Confidentiality can be violated in many ways, for example, ***through direct attacks designed to gain unauthorized access to systems, applications, and databases in order to steal or tamper with data.******Network reconnaissance and other types of scans, electronic eavesdropping (via a man-in-the-middle attack), and escalation of system privileges by an attacker*** are just a few examples.

But confidentiality can also ***be violated unintentionally through human error, carelessness, or inadequate security controls***. Examples include failure (by users or IT security) to adequately protect passwords; sharing of user accounts; physical eavesdropping (also known as shoulder surfing); failure to encrypt data (in process, in transit, and when stored); poor, weak, or nonexistent authentication systems; and theft of physical equipment and storage devices.

### To protect

* data classification and labeling
* strong access controls and authentication mechanisms
* encryption of data in process, in transit, and in storage
* steganography
* remote wipe capabilities
* adequate education and training for all individuals with access to data.

### 3 steps

**STEP 1**

Must have **access control** to manage/ authorize person who would be able to access the information/ data in the system The granularity depends on both technical and business requirement.

**STEP 2**

To **limit access** to information/ data to authorized users (AUTHORISATION)

***Authorisation*** *is defined as “access privileges granted to a user, program, or process or the act of granting those privileges*

**STEP 3**

To **validate the indentity** of people requesting access to data ( AUTHENTICATION)

***Authentication*** *is defined as “the process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data* ***Authentication generally prefaces authorisation decisions***

## Integrity

### Definition

*“Integrity commonly refers to* ***maintaining the accuracy of data stored in a computer system****.”*

“Integrity is about ***ensuring that data has not been tampered with and, therefore, can be trusted***. It is ***correct, authentic, and reliable***. Ensuring integrity involves protecting data in use, in transit (such as when sending an email or uploading or downloading a file), and when it is stored, whether on a laptop, a portable storage device, in the data center, or in the cloud.”

Concept ***non-repudiation =*** *the inability to deny something*

***Non-repudiation assists in ensuring integrity.***

*<Term of inability to deny by the source of data in sending action and the recipients in receiving data (via awareness of senders’ identity)>*

### How will Integrity be violated?

Integrity can be compromised directly via ***an attack vector (such as tampering with intrusion detection systems, modifying configuration files during transit, retrieval and at rest, or changing system logs to evade detection)***

***or unintentionally, through human error, lack of care, coding errors, or inadequate policies, procedures, and protection mechanisms.***

### To protect

* Encryption
* Hashing
* Digital signatures
* Digital certificates = Trusted certificate authorities (CAs) issue digital certificates to organizations to verify their identity to website users, similar to the way a passport or driver’s license can be used to verify an individual's identity
* Intrusion detection systems
* Auditing
* Version control
* Strong authentication mechanisms and access controls.

## Availability

### Definition

*“The property of* ***being accessible and useable upon demand by an authorized entity****. Ensures that data is always accessible when and where it is needed.”*

“Availability means that ***networks, systems, and applications are up and running***. It ensures that ***authorized users have timely, reliable access to resources when they are needed***.”

### How will Availability be violated?

By many things, mostly by external factors (not technically jeopardize)

* Hardware or software failure
* Power failure
* Natural disasters
* Human error

Most well-known attack = ***Denial of Service (DoS)*** attack

The performance of a system, website, web-based application, or web-based service is ***intentionally and maliciously degraded***, or the ***system becomes completely unreachable.***

### To protect

* Monitoring of performance, network traffic and network bandwidth
* Maintaining and testing backup systems
* DoS protection systems
* Designing fault-tolerant systems
* Testing access control systems

## Summary

|  |  |  |
| --- | --- | --- |
| CIA Triad | Attackers | Admin |
| Confidentiality | Packet Capturing  Keylogging  Access files  Exfiltrate Data  Delete data | Protect data  Restrict assess |
| Integrity | Encrypt data  Man-in-the-middle attacks  Delete Data  Demand ransom | Backup data  Restore plan  Update |
| Availability | Disrupt services (DoS, DDoS)  Deny access (Account manipulation) | Firewalls  IDS  DDoS Protection Services  Pen Test |

## What is CIA Triad?

### Definition

CIA Triad is a venerable security model, designed as a guidelines policy for information security management that secures an organization’s information system which encompasses both user computer system and data. It is important that each of the elements of a system is designed to achieve one or more of three CIA Triad principles, which makes CIA Triad a fundamental tenet of information security.

### Purpose

CIA Triad is used as a core principle in any organization’s security infrastructure to design a security plan by identifying problem areas and detect appropriate solutions in the arena of information security. In other words, CIA Triad is a standard principle to organizations apply to protect a network and the data within that network.

## What are the three principles of the CIA Triad?

CIA Triad is an abbreviation of its three principles, namely Confidentiality, Integrity and Availability, which each will be explained its definition, how it is damaged and corresponding solutions in this section.

### Confidentiality

#### Definition

Confidentiality is a principle designed to control the access permission to data within a system and prevent unauthorized individuals, processes, or devices disclosure. Confidentiality processes the authentication (validate the identity of data’s requesting) and authorisation (limit data access to authorized users), to ensure the internal data will be accessible by authorized factors only while preventing unauthorized factors from obtaining access.

#### How will confidentiality be violated?

There are multiple actions that compromise Confidentiality whether be intentionally attacked by attackers or unintentionally violated by external factors.

Confidentiality violation involves accessing data or having damaging actions such as steal or tamper with the data of an organization. These attacks can happen in both logical and physical approaches, by computer trespassing or directly attacked by external factors (attackers) trying to compromise the system. A system can be attacked intentionally by designed direct attacks that allow unauthorized personnel to be able to access the system such as failing to encrypt a transmission, accessing malicious code, misconfigured security control or oversight in a security policy.

In addition, Confidentiality can also be jeopardized accidentally by human error and carelessness, oversight or inadequate security controls. This includes failure in protecting or encrypting passwords or data while in process, in transit, and in storage, issues in sharing the same user accounts, poor or lack of authentication systems and even stealing of physical equipment and storage devices.

#### What countermeasures can be employed to strengthen Confidentiality?

* Data classification
* Strong access controls
* Strong authentication mechanisms
* Cryptography
* Training of personnel with access to data
* Avoid the loss of physical devices and lessen human carelessness

### Integrity

#### Definition

Integrity is the concept of maintaining the accuracy, correctness, authenticity, and reliability of data and protect data from unauthorized modifications or being inappropriately tampered with during transit, retrieval and at rest. With the concept of non-repudiation, Integrity is ensured by the process of preventing faking deny of action trading information between sender and recipients.

Perspectives of Integrity:

* Prevent unauthorized users from making modifications
* Prevent authorized users from making changes by mistakes
* Maintain consistency of data

#### How will Integrity be violated?

Similar to Confidentiality, multiple actions compromise Integrity directly by allowing unauthorized networks to access the system or data to launch a cyberattack, aka attack vector. This hazarding factor can be demonstrated in various methods in data system violation, such as modifying configuration files or changing system logs to evade detection.

However, Integrity is also jeopardized by unintentional factors which are human error, viruses, coding errors, malicious modifications, and backdoors. These similarities are a result of a strong dependency between Confidentiality and Integrity.

#### What countermeasures can be employed to strengthen Integrity?

* Encryption
* Hashing
* Input validation
* Intrusion detection systems
* Strong access controls
* Strong authentication mechanisms

### Availability

#### Definition

Availability is the ability to uninterruptedly accessing the data and resources depending on the demand of the authorized entity that a system or organization should respond to and provide the requested information from authorized accesses. Availability depends on Confidentiality and Integrity and will be maintained by the existence of both of them.

#### How will Availability be violated?

By many things, mostly by external factors (not technically jeopardize)

* Hardware or software or device failure
* Power failure
* Communication interruptions
* Environmental issues
* Human error

The most well-known attack that affects availability is Denial of Service (DoS)attack, which is described as overload steam of data flow, flooding the system making it inaccessible to its intended users.

#### What countermeasures can be employed to strengthen Availability?

* Monitoring of performance, network traffic and network bandwidth
* Maintaining and testing backup systems
* DoS protection systems
* Designing fault-tolerant systems
* Testing access control systems

# WEEK 2: CRYTOGRAPHY

## Concepts

### Terminology

* ***Cryptography*** -> the science of secret writing with the goal of hiding the meaning of a message
* ***Cryptanalysis*** -> the science of breaking cryptosystems
* ***Encryption***-> the process of turning plaintext into ciphertext
* ***Decryption*** -> the process of turning ciphertext into plaintext
* ***Cryptology*** -> study of encryption & decryption, including cryptography & cryptanalysis

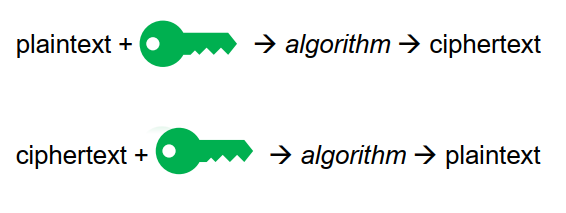
***=> Encryption / decryption*** *requires: an algorithm and a key*

### Types of encryption algorithms

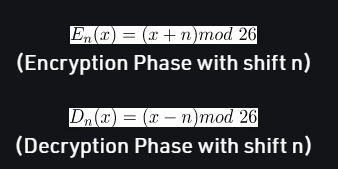
There are **two main types** of encryption algorithms:

• Symmetric algorithms

two parties have an encryption and decryption method for which they ***share a secret key*.**



**Substitution Cipher**

******

**Caesar Cipher**

**(n = 3)**

**Modern Ciphers**

**DES (Data Encryption Standard)**

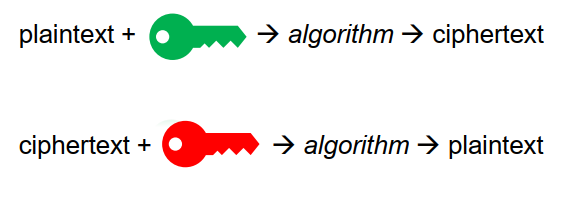
* published by NIST in 1977
* 56bit key length

**AES (Advanced Encryption Standard)**

* NIST replacement for DES published in 2001
* 128-256bit key length

• Asymmetric (or public key) algorithms

a user possesses ***a secret key*** as in symmetric cryptography but also ***a public key***.

****

**Public vs private keys**

– ciphertext encrypted with ***public key*** can be decrypted with ***private key***

– ciphertext encrypted with ***private key*** can be decrypted with ***public key***

• No need to possess a pre-shared secret key

• ***Much slower*** than symmetric cryptography (arithmetically intensive)

• Well suited to ***encrypting small amounts of data***

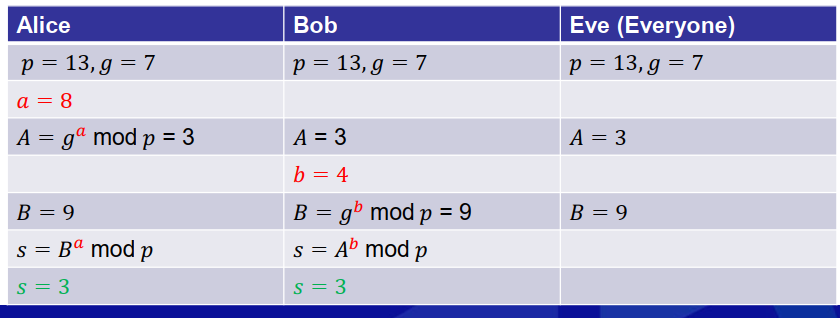
***Example***

Li brx vwxgb kdug brx zloo kdyh d uhzduglqj fduhhu lq LW.

If you study hard you will have a rewarding career in IT

**Diffie-Hellman Key Exchange**

x mod y = z



***Example***

Client p = 5 | Server g = 7

a = 5 => A = 2

b = 2 => B = 4

=> 4 is the shared secret

**STEPS (ASYMMETRIC CRYPTOGRAPHY)**

+ A and B each has their own *Private Key and Public Key*

+ A and B *exchange Public Key* => communicate a message

+ A uses *A’s Private Key -> generate AES key*

+ A *use AES key to encrypt a message* with rules and process used for encryption

+ A *use B’s Public Key to encrypt A’s AES key*

+ A *sends Encrypted message & A’s AES key* to B

+ B *use B’s Private Key to decrypt A’s AES key*

+ B *use A’s AES key and Public key to decrypt the message*

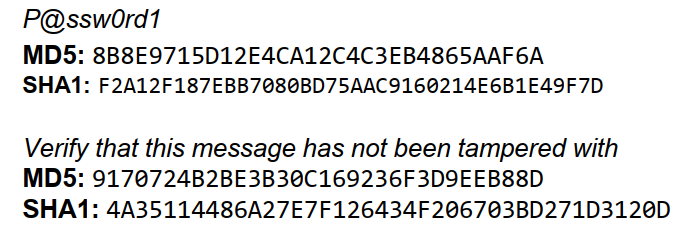
<AES key from A proves the reliability of the message>

## Cryptographic Hash Functions

### Definition

* ***Uses***
* Message integrity
* Digital signatures (more on this later)
* Storing passwords
* ***No key***
* ***One-way calculation***
* It is ***not feasible to modify*** a message without changing its hash value
* ***Strong collision resistance*** – highly unlikely that any two inputs will hash to the same output
* ***Compression*** – usually a fixed size output, smaller than the input
* ***Efficiency***

### Example

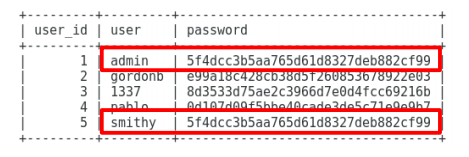
******

***Example - Password Storage***

• **Plaintext** password is ***hashed*** and the **result** is ***stored***

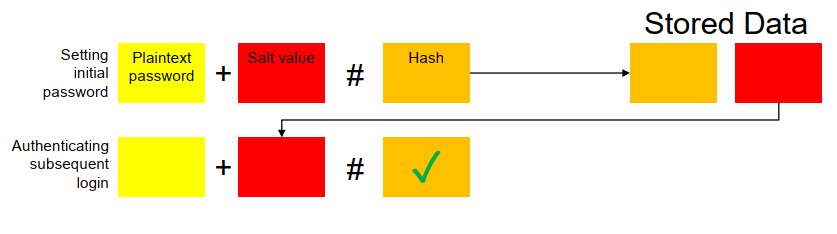
• During authentication, a user ***provides the plaintext*** password, which

is hashed and ***compared to the stored hash value***

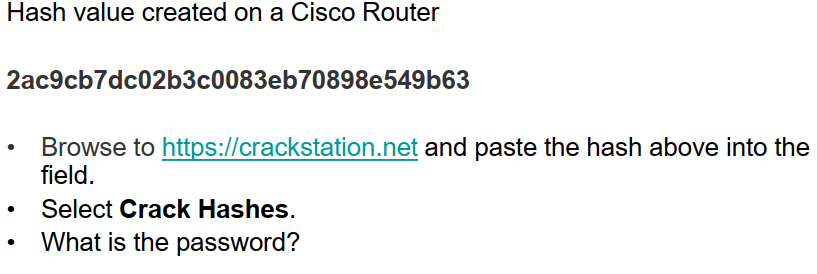


• To **mitigate the damage** that a hash table or a dictionary attack could do, we ***salt the passwords***. A salt makes a hash function look non-deterministic, which is good as we don't want to reveal duplicate passwords through our hashing.

• Let’s say that we have ***password ”password1” and the salt xyz***. We can salt that password by either appending or prepending the salt to it. This will yield ***password1xyz or xyzpassword1***.



***Example – Hash Value***



2ac9cb7dc02b3c0083eb70898e549b63

Password1

## Digital Signatures

• ***Asymmetric encryption + hashing*** can be used to implement **digital signatures**

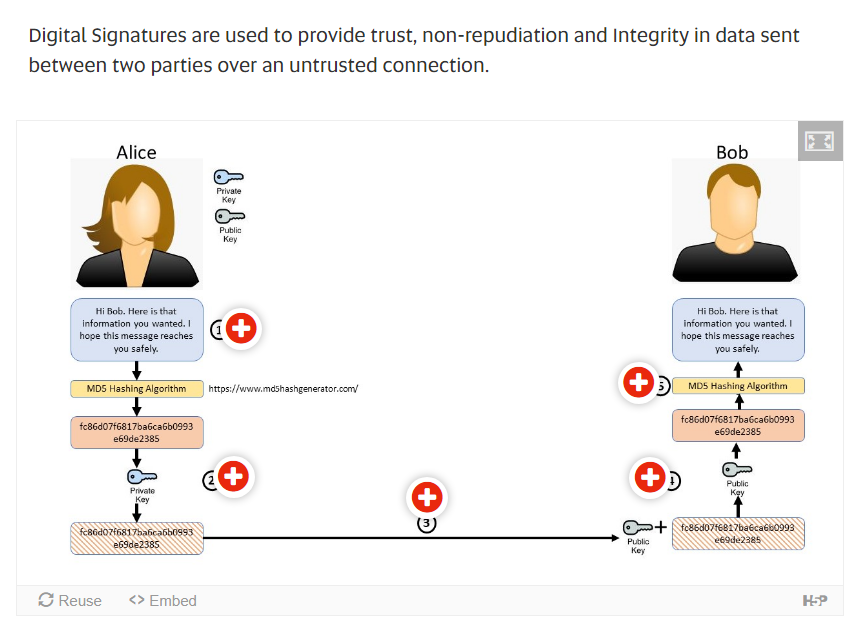
• Provides ***integrity assurance and non-repudiation***

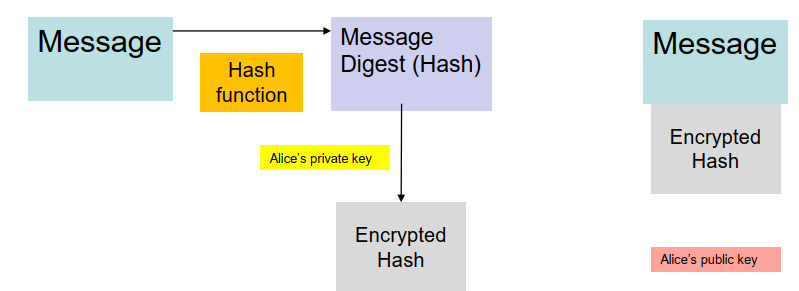
• Commonly achieved by *hashing the message, encrypting the hash using the sender’s private key and ‘attaching’ the encrypted hash to the message*.

• The sender’s public key may also be sent with the message.

**STEPS OF DIGITAL SIGNATURES**

1. Alice applies an MD5 hash function to the cleartext message to create a Message Digest (Hash)
2. Alice uses her Private key to encrypt the message digest. As Alice is the only holder of this private key it proves the message comes from her (trust)
3. Alice now sends the message, the encrypted message digest and her public key to Bob.
4. Bob decrypts the message digest using Alice's public key
5. Bob finally applies the same MD5 hash function to the message. If the resulting message digest (Hash) matches what he was sent from Alice then he knows the original message has not been tampered with and has maintained Integrity.





## Public Key Infrastructure

### Definition

A public key infrastructure (PKI) binds public keys to entities, enables other entities to

verify public key bindings, and provides the services needed for ongoing management of

keys in a distributed system.

### Structure

• **Server**

– generates public and private keys

– requests certificate from CA (certificate will contain server public key and will be encrypted using CA private key)

• **Client**

– decrypts certificate using CA public key

– uses server’s public key to establish secure communications

Week2

Symetric

Asymetric (use case tại sao A gửi file encrypt bằng private key mà B không mở được bằng public key )

phân tích cách hoạt dộng của Asymetric

**Encryption – Hashing – Salting**

Encryption is the process of using a code to stop other parties from accessing information.

Hashing is taking a string of data of any size and always give an output of a predetermined length.

Salting refers to adding random data to a hash function to obtain a unique output which refers to the hash.

**Hashing vs Salting**

Hashing is a one-way function where data is mapped to a fixed-length value. Hashing is primarily used for authentication. Salting is an additional step during hashing, typically seen in association to hashed passwords, that adds an additional value to the end of the password that changes the hash value produced.

phân tích cách đối phó với hash table hoặc dictionary attack – salting

**What is hash table and dictionary attack?**

A **dictionary attack** is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

A rainbow table attack is a type of hacking wherein the perpetrator tries to use a **rainbow hash table** to crack the passwords stored in a database system. A rainbow table is a hash function used in cryptography for storing important data such as passwords in a database. Sensitive data are hashed twice (or more times) with the same or with different keys in order to avoid rainbow table attacks.

**Hash tables** to be exhausted first. Additional results use a rainbow.

Hash tables = fast lookup, but long computation (if you were building one from scratch), more space. Rainbow table = slow lookup because you have to run through the hash algorithms many times, less space.

A hash table is essentially a pre-computed database of hashes. Dictionaries and random strings are run through a selected hash function and the input/hash mapping is stored in a table. The attacker can then simply do a password reverse lookup by using the hashes from a stolen password database.

**pre-computation**. Hash table attacks are fast because the attacker doesn't have to spend any time computing any hashes. The trade-off for the speed gained is the immense amount of space required to host a hash table. We could say that a hash table attack is a pre-computed dictionary and/or brute-force attack.

**How to deal with these attacks?**

Either use sophiticated passwords with uppercase, numbers or special characters (objective solutions, can be protected directly by user)

Or use Salting (subjective), one of the Cryptographic Hash Functions

cách hoạt dộng cùa salting - vì sao nó hiệu quả

**What is salting, how does it work and why is it efficent?**

=> strengthen passwords

A cryptographic salt is made up of random bits added to each password instance before its hashing.

Salts create unique passwords even in the instance of two users choosing the same passwords.

Salts help us mitigate hash table attacks by forcing attackers to re-compute them using the salts for each user.

Creating cryptographically strong random data to use as salts is very complex and it's a job better left to leading security solutions and providers.

Unique + long salt + unpredictable + random generated salt + secret key + reusable + different combination

# WEEK 3 CYBERSECURITY ATTACKS: LIFECYCLE & MOTIVATIONS

## OVERVIEW

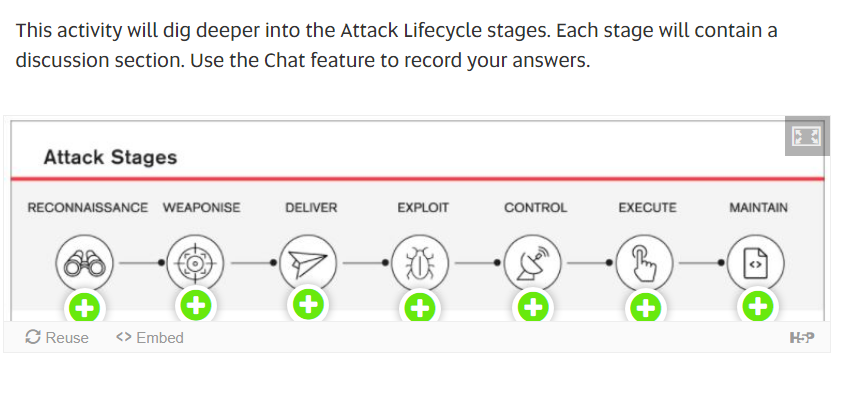
* Sources, methods and reasons for cybersecurity attacks.
* Trends related to Cybersecurity threats.
* Model of attack lifecycles => characterise Cybersecurity attacks.

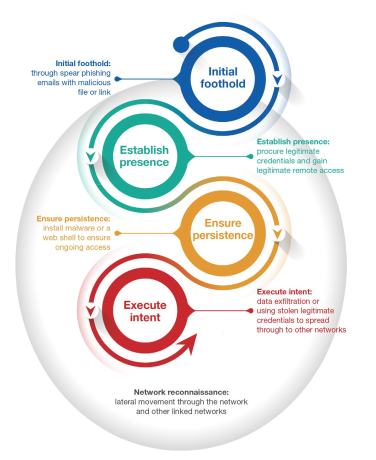
## Cyber Incident

### Definition

One or many (single or a series) of event(s) that threatens one or many of CIA Triad Principle (of Digital Information)

## Attack Lifecycle





**Initial foothold:**

An adversary sends a spear phishing email to their target, relying on trust already

established between users as they repurpose genuine emails or contacts to ensure

success. When the user opens the malicious attachment or link in the spear phishing email,

malware is executed on the user’s workstation creating an entry into the network.

Another method used to gain initial access is the compromise – either targeted or

opportunistic – of vulnerable internet-facing services. Most exploited services have

involved publicly-known vulnerabilities with patches available from application and

operating system vendors.

**Network reconnaissance** is continually performed by the adversary once they

have access to the network. Moving laterally, the adversary will study the network

infrastructure, search for domain administration credentials and possibly propagate

through other linked networks. Adversaries will typically build-up knowledge of the

compromised network that rivals, and sometimes exceeds, the organisation’s own

administrators. In some cases, ASD has observed adversaries actively monitoring

administrators to identify upcoming changes within the environment or to determine if

the compromise has been detected. As an example, an adversary will regularly access

the network to gain updated user credentials, thus avoiding losing access because of

password changes.

**Establish presence:**

Once in the network, the adversary will attempt to procure legitimate user credentials with

the goal of gaining legitimate remote administrative access.

Adversaries will typically obtain legitimate privileged credentials by dumping them from

administrator workstations, domain controllers, or other key hosts within the network.

After legitimate credentials are obtained, the adversary will transition from malwaredependant tradecraft to the use of Virtual Private Network (VPN), Virtual Desktop

Infrastructure (VDI), or other corporate remote-access solutions combined with software

native to the organisation.

**Ensure persistence:**

In the types of compromises responded to by the ACSC, adversaries typically want to

establish persistence. To do this, adversaries strive to install malware or a web shell to

ensure ongoing access should their legitimate accesses cease to function. Malware is

typically configured with a limited “beacon rate” to minimise network traffic and evade

network defenders. However, web shells are increasingly being used as they generate

zero network traffic and are difficult to detect unless the adversary is actively interacting

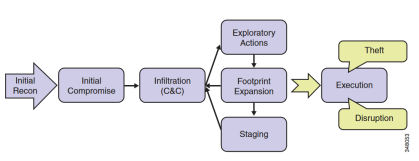
with them.

**Execute intent:**

Once persistent access is gained, the adversary will execute their intent. This intent could

be anything from data exfiltration to enabling lateral movement to the real targeted

organisation, exploiting circle of trust relationships between the organisations.



## MITRE ATT&CK Matrix and Techniques

<https://attack.mitre.org/>

# WEEK 4 ESSENTIAL 8

## Cyber Intrusions

An intrusion is any activity that is designed to compromise your data security. This can be through more menacing and pervasive formats like ransomware or unintentional data breaches by employees or others connected to your network.

An intrusion may include any of the following:

* Malware or ransomware
* Attempts to gain unauthorized access to a system
* DDOS attacks
* Cyber-enabled equipment destruction
* Accidental employee security breaches (like moving a secure file into a shared folder)
* Untrustworthy users –– both team members and those outside of your organization
* Social engineering attacks –– such as phishing campaigns and other ways of tricking users with seemingly legitimate communication

week4

## The essential 8

## The following is a summarized version of the Essential Eight strategies (Australian Cyber Security Centre):-

## Application whitelisting – to control the execution of unauthorized software

## Patching applications – to remediate known security vulnerabilities

## Configuring Microsoft Office macro settings – to block untrusted macros

## Application hardening – to protect against vulnerable functionality

## Restricting administrative privileges – to limit powerful access to systems

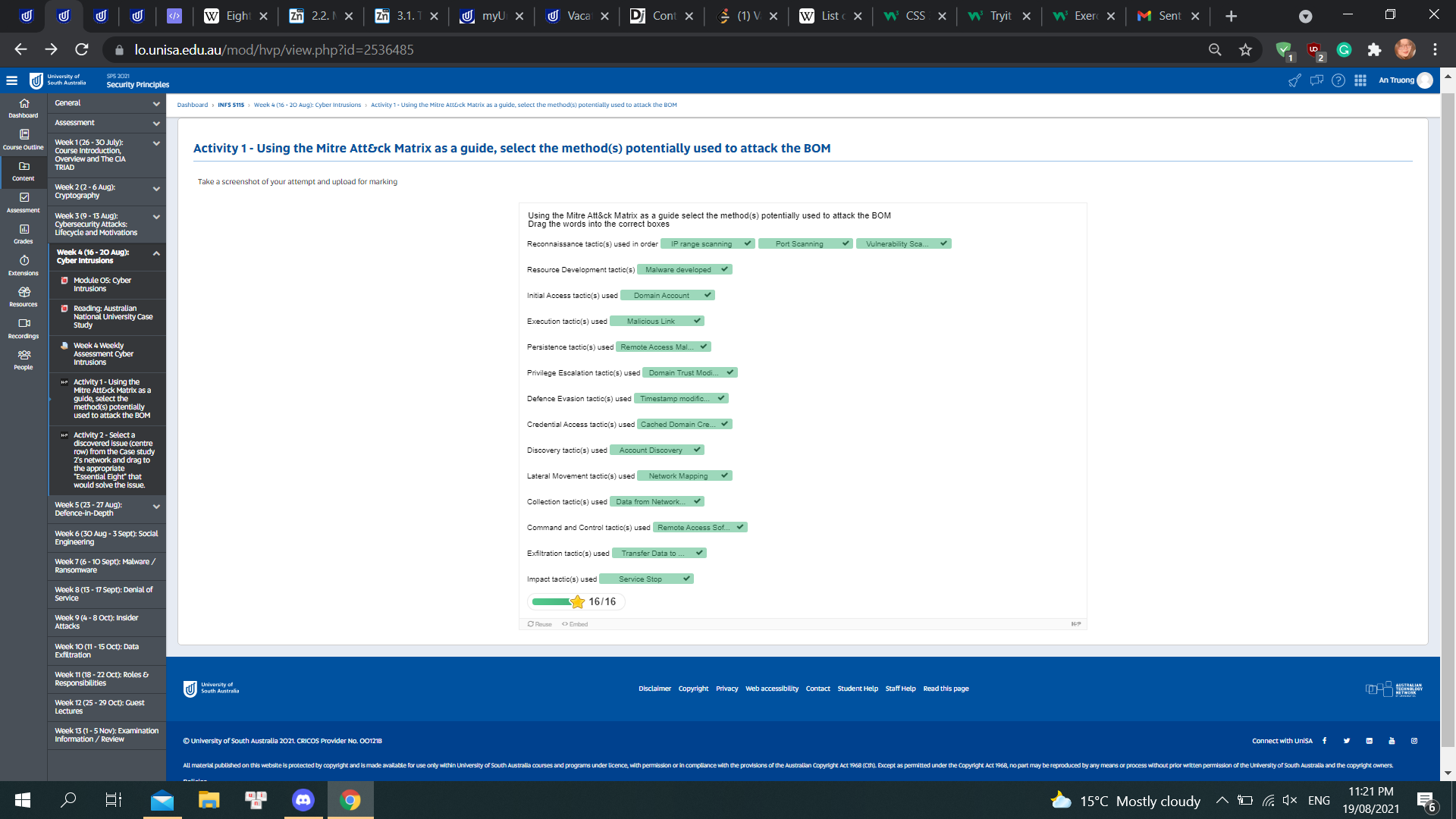
## Patching operating systems – to remediate known security vulnerabilities

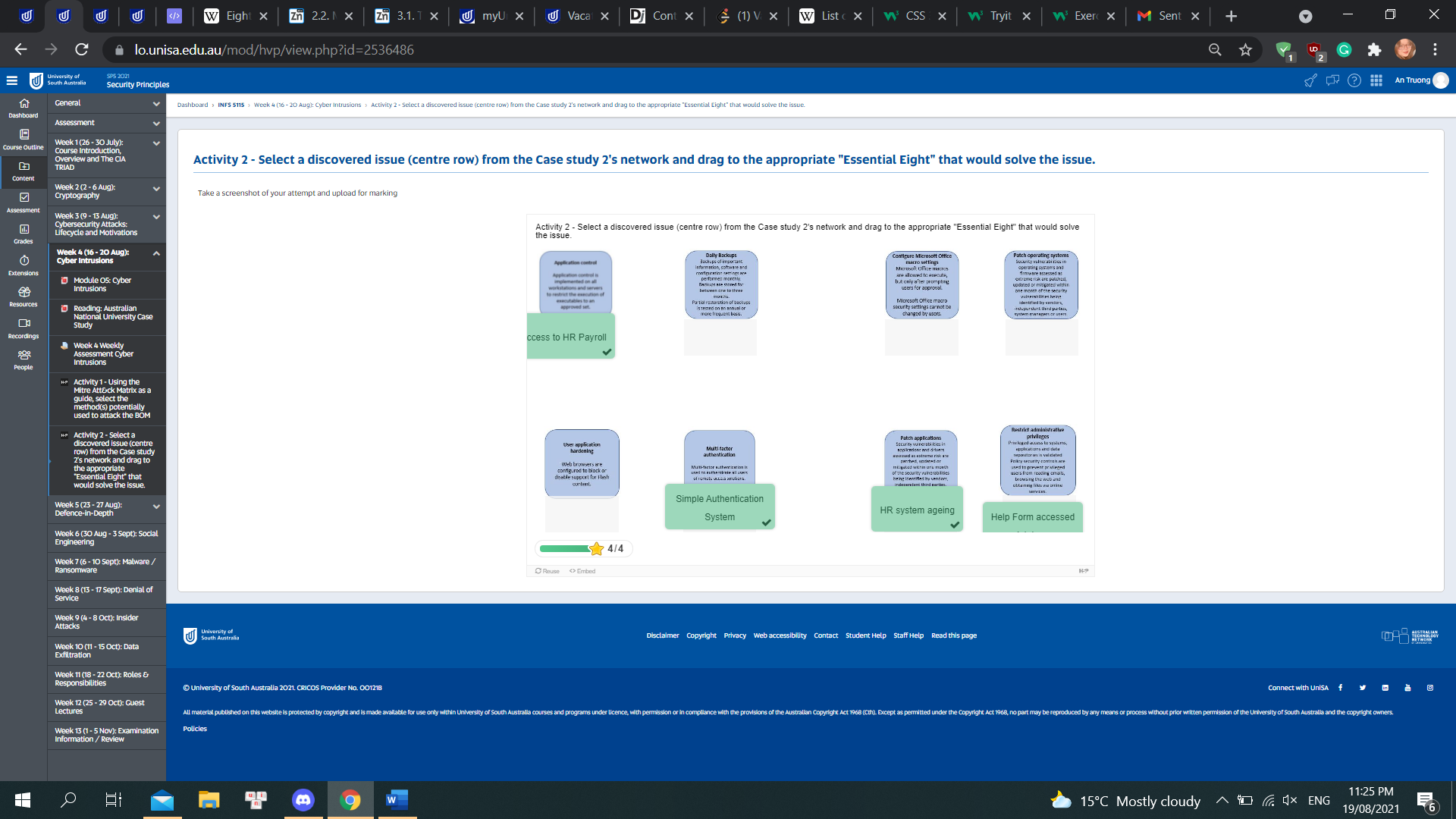
## Multi-factor authentication – to protect against risky activities

* Daily backups – to maintain the availability of critical data.

<https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents>

<https://www.data3.com/solutions/security/acsc-essential-eight/>





**ESSENTIAL EIGHT MATURITY MODEL FOR CYBER SECURIT**

**1. APPLICATION CONTROL:**

To prevent the execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell, and HTA), and installers.

Why? This control is for all non-approved applications (including malicious code) are prevented from executing.

**2. PATCH APPLICATIONS**

Flash, web browsers, Microsoft Office, Java, and PDF viewers. Patch/mitigate computers with ‘extreme risk’ vulnerabilities within 48 hours. Use the latest version of applications.

Why? Security vulnerabilities in applications can be used to execute malicious code on systems.

**3. CONFIGURE MICROSOFT OFFICE MACRO SETTINGS**

To block macros from the internet, and only allow vetted macros either in ‘trusted locations’ with limited write access or digitally signed with a trusted certificate.

Why? Microsoft Office macros, for example, can be used to deliver and execute malicious code on systems.

**4. USER APPLICATION HARDENING.**

Configure web browsers to block Flash (ideally uninstall it), ads, and Java on the internet. Disable unnecessary features in Microsoft Office (e.g. OLE), web browsers, and PDF viewers.

Why? Flash, ads, and Java are popular ways to deliver and execute malicious code on systems.

person writing bucket list on book

**5. RESTRICT ADMINISTRATIVE PRIVILEGES**

Operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don’t use privileged accounts for reading email and web browsing.

Why? Admin accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems.

**6. PATCH OPERATING SYSTEMS.**

Patch/mitigate computers (including network devices) with ‘extreme risk’ vulnerabilities within 48 hours. Use the latest operating system version. Don’t use unsupported versions.

Why? Security vulnerabilities in operating systems can be used to further the compromise of systems.

**7. MULTI-FACTOR AUTHENTICATION**

It includes VPNs, RDP, SSH, and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

Why? Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

**8. DAILY BACKUPS**

Daily back-ups of important new/changed data, software, and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.

Why? To ensure information can be accessed following a cybersecurity incident (e.g. a ransomware incident).

1 số câu hỏi về essential eight, 1 công ty gặp trường hợp a thì nên áp dụng technique nào trong 8 cái

định nghĩa 1 trong 8 cái là gì và cách áp dụng nó

# WEEK 5 DEFENCCE-IN-DEPTH

week 5 defence in depth

## Definition

**Defence-in-Depth**

– Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

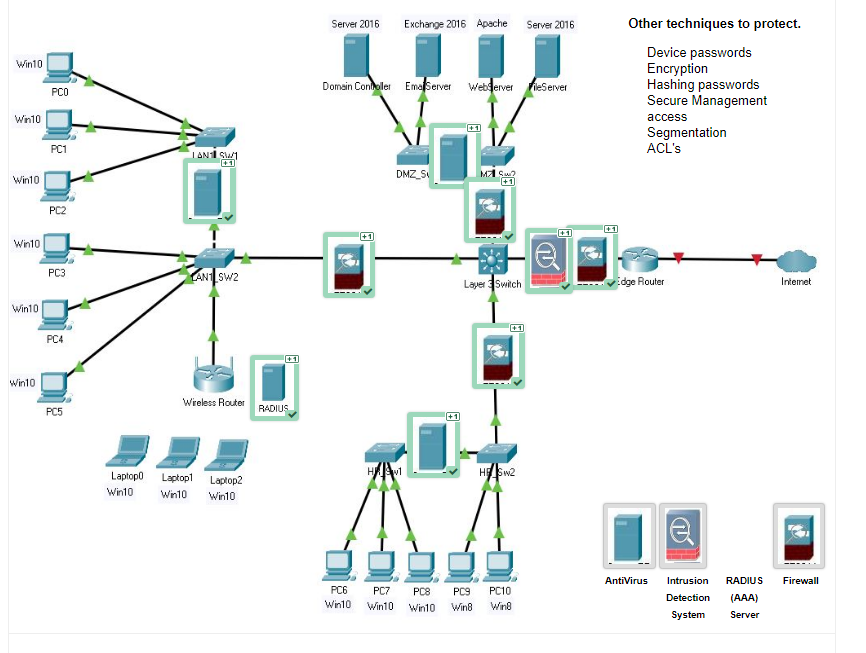
**In contrast to: Defence-in-Breadth**

– A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

*có 1 câu use case về defence indepth mà hỏi chung chung lắm nên anh không nhớ phần nào trong week6 :>*

*à, devices nào giúp manage information truyền từ ngoài vào trong mạng nội bộ và devices đó nên được đặt ở đâu trong network*

**fire wall + secured router**

****

## Maturity Levels

**ACSC Mitigation Strategies**

To assist organisations in determining the maturity of their

implementation of the Essential Eight, three maturity levels have been

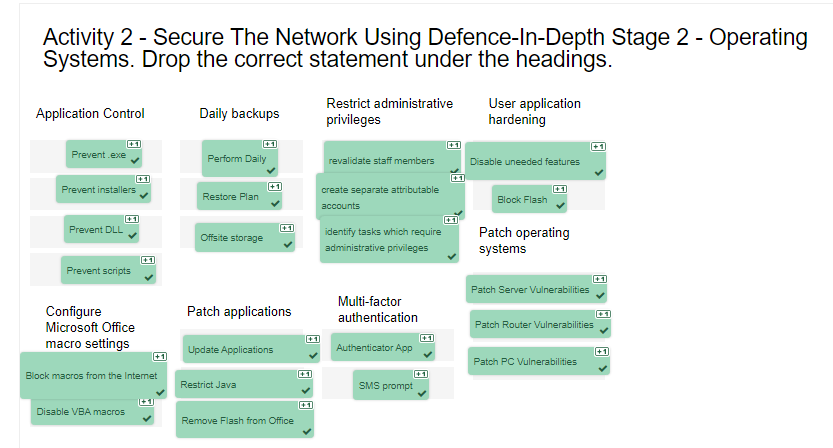
defined for each mitigation strategy. The maturity levels are defined as:

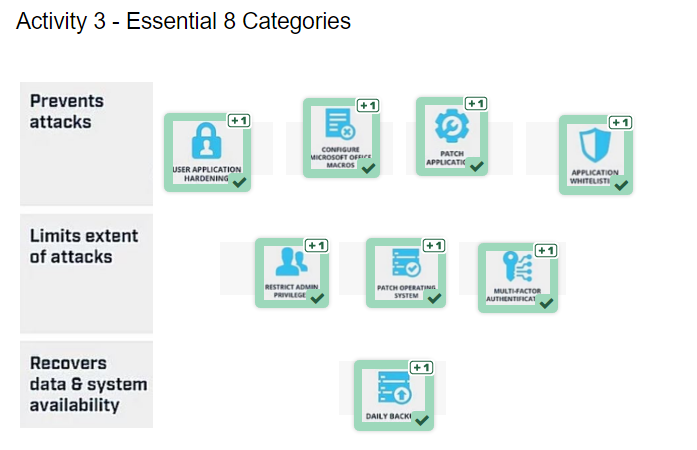
– **Maturity Level One**: Partly aligned with the intent of the mitigation strategy

– **Maturity Level Two**: Mostly aligned with the intent of the mitigation strategy

– **Maturity Level Three**: Fully aligned with the intent of the mitigation strategy

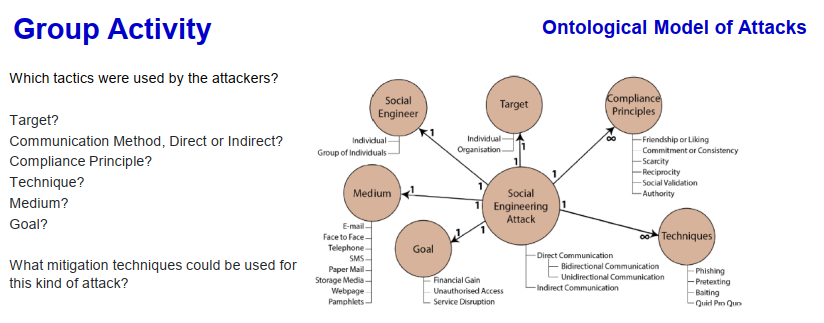
<https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>

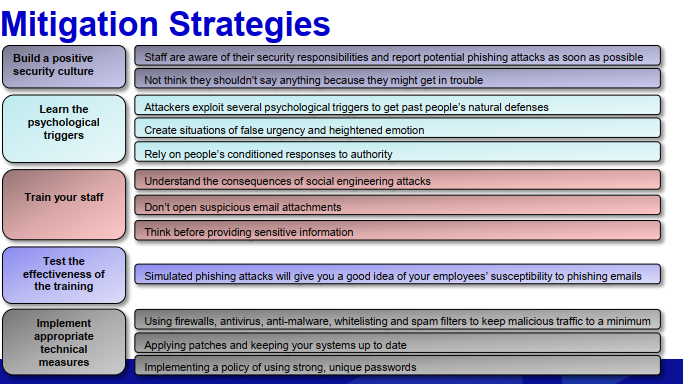


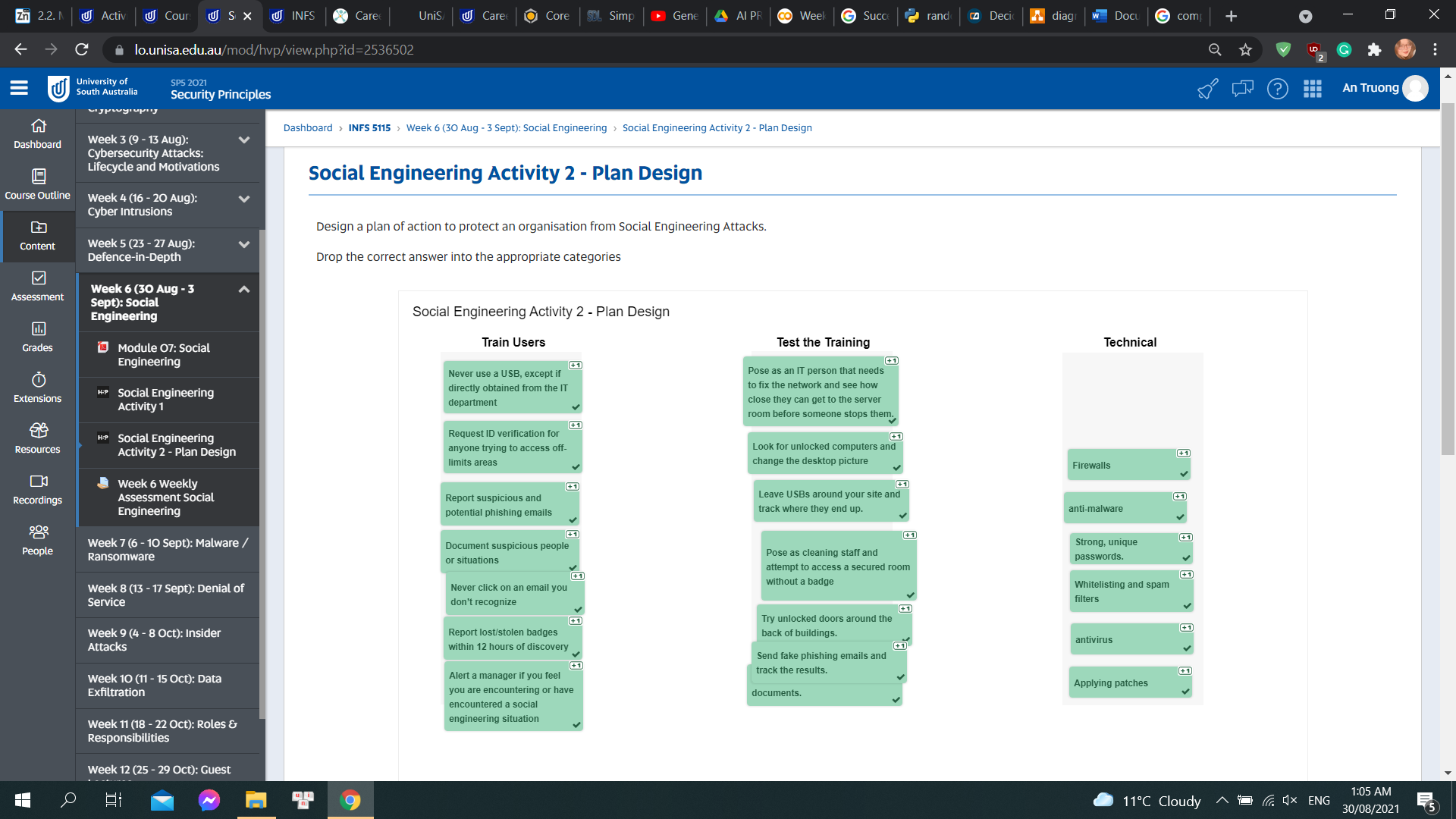


week6 - ontological model of attacks - figure1 ấy

use case phân tích 1 người bị đánh cắp thông tin xong hỏi phân tích thành từng section trong figure







maturity level

hình như không có định nghĩ nhưng có thể xem qua cho chắc :>

xem bảng maturity patch application a - có 1 câu hỏi la khi maturity level náo nên dc áp dụng khi cần được update within 48 hours (level 3)

# WEEK 8 DDOS

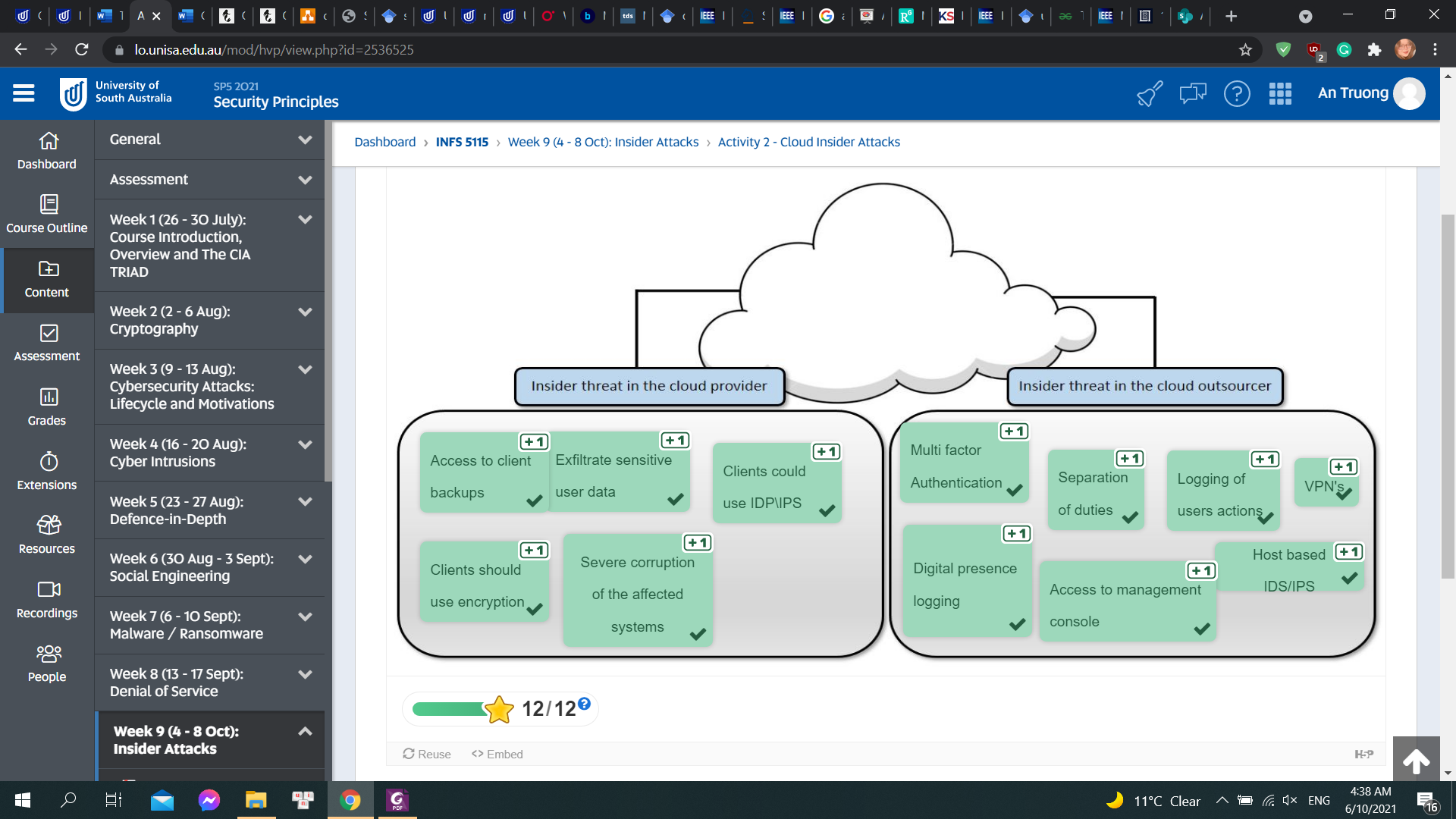
week8 - attack nào đượng biết đến qua việc sử dụng nhiều botnet trong lúc execute - DDoS

tại sao bạn chọn đáp án đêí

# WEEK 9 INSIDER ATTACKS

week9

use case phân tích insider attacks - không nhớ lắm câu hỏi là gì :>



chủ yếu là chừng này phần khác có thể xem qua đề phòng :>

# Mock Exam

