

SECURITY PRINCIPLES

WEEK 1: TENETS (PRINCIPLES) OF CYBER SECURITY

CIA TRIAD

How a Hacker sees a network



How an Admin sees a network



REFERENCES

UniSA Slides

[WHAT IS CIA TRIAD – F5](#)

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 identity** 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 access
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 stream 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: CRYPTOGRAPHY

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**.

plaintext +  → algorithm → ciphertext

ciphertext +  → algorithm → plaintext

Substitution Cipher

$$E_n(x) = (x + n) \bmod 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) \bmod 26$$

(Decryption Phase with shift n)

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**.

plaintext +  \rightarrow algorithm \rightarrow ciphertext

ciphertext +  \rightarrow algorithm \rightarrow plaintext

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 vwxbg 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

$$x \bmod y = z$$

Alice	Bob	Eve (Everyone)
$p = 13, g = 7$	$p = 13, g = 7$	$p = 13, g = 7$
$a = 8$		
$A = g^a \bmod p = 3$	$A = 3$	$A = 3$
	$b = 4$	
$B = 9$	$B = g^b \bmod p = 9$	$B = 9$
$s = B^a \bmod p$	$s = A^b \bmod p$	
$s = 3$	$s = 3$	

Example

Client $p = 5$ | Server $g = 7$

$a = 5 \Rightarrow A = 2$

$b = 2 \Rightarrow B = 4$

$\Rightarrow 4$ 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* \Rightarrow communicate a message

+ A uses *A's Private Key* \rightarrow 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

P@ssw0rd1

MD5: 8B8E9715D12E4CA12C4C3EB4865AAF6A

SHA1: F2A12F187EBB7080BD75AAC9160214E6B1E49F7D

Verify that this message has not been tampered with

MD5: 9170724B2BE3B30C169236F3D9EEB88D

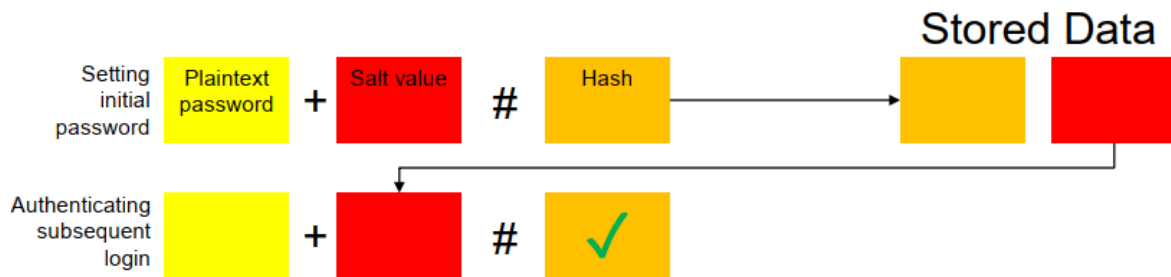
SHA1: 4A35114486A27E7F126434F206703BD271D3120D

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**

user_id	user	password
1	admin	5f4dcc3b5aa765d61d8327deb882cf99
2	gordonb	e99a18c428cb38d5f260853678922e03
3	1337	8d3533d75ae2c3966d7e0d4fcc69216b
4	pablo	0d107d00f5bbe40cade3de5c71e9e9b7
5	smithy	5f4dcc3b5aa765d61d8327deb882cf99

- 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

Hash value created on a Cisco Router

2ac9cb7dc02b3c0083eb70898e549b63

- Browse to <https://crackstation.net> and paste the hash above into the field.
- Select **Crack Hashes**.
- What is the password?

2ac9cb7dc02b3c0083eb70898e549b63

Password1

Digital Signatures

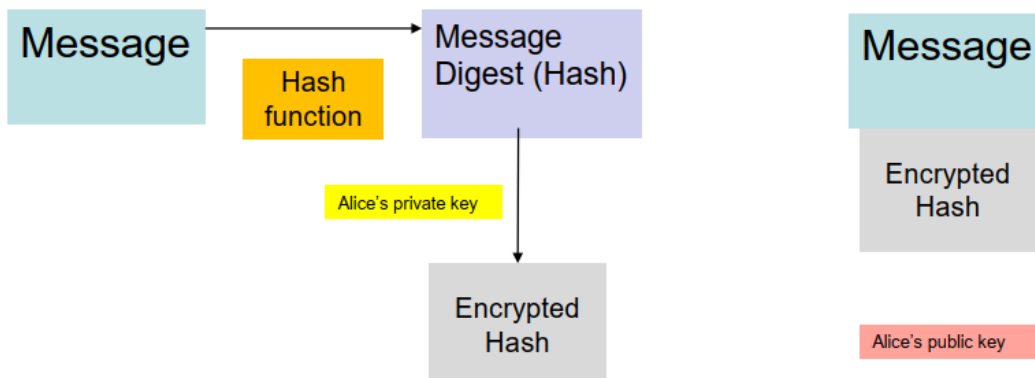
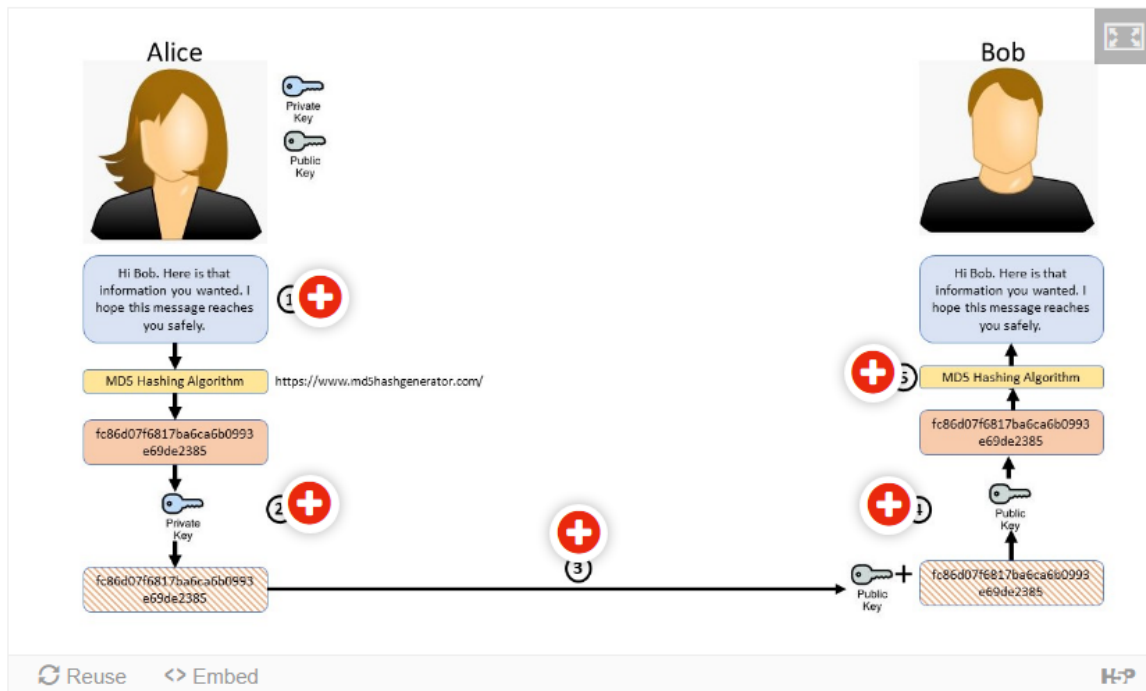
- **Asymmetric encryption + hashing** can be used to implement **digital signatures**
- Provides **integrity assurance and non-repudiation**
- Commonly achieved by *hashing the message, encrypting the hash using the sender's private key and 'attaching' the encrypted hash to the message.*
- The sender's 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

- 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.

Digital Signatures are used to provide trust, non-repudiation and Integrity in data sent between two parties over an untrusted connection.



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 động 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 sophisticated 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 động của salting - vì sao nó hiệu quả

What is salting, how does it work and why is it efficient?

=> 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.

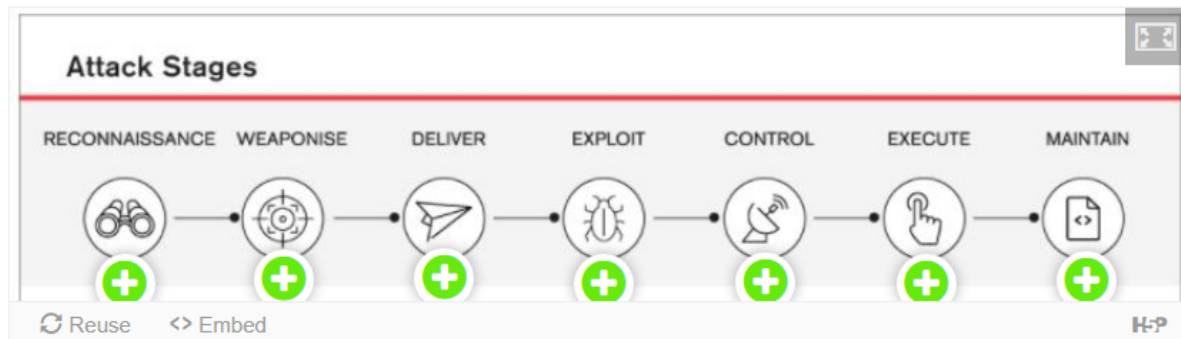
Cyber Incident

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

This activity will dig deeper into the Attack Lifecycle stages. Each stage will contain a discussion section. Use the Chat feature to record your answers.



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 malware dependant 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.

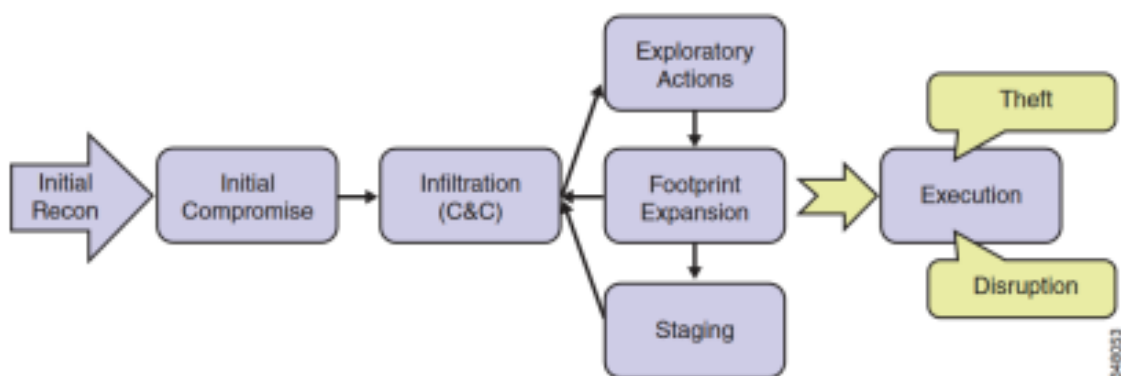
Ensure persistence:

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/>

Using the Mitre Att&ck Matrix as a guide select the method(s) potentially used to attack the BOM
Drag the words into the correct boxes

Reconnaissance tactic(s) used in order IP range scanning ✓ Port Scanning ✓ Vulnerability Sca... ✓

Resource Development tactic(s) Malware developed ✓

Initial Access tactic(s) used Domain Account ✓

Execution tactic(s) used Malicious Link ✓

Persistence tactic(s) used Remote Access Mal... ✓

Privilege Escalation tactic(s) used Domain Trust Modi... ✓

Defence Evasion tactic(s) used Timestamp modifi... ✓

Credential Access tactic(s) used Cached Domain Cre... ✓

Discovery tactic(s) used Account Discovery ✓

Lateral Movement tactic(s) used Network Mapping ✓

Collection tactic(s) used Data from Network... ✓

Command and Control tactic(s) used Remote Access Sof... ✓

Exfiltration tactic(s) used Transfer Data to ... ✓

Impact tactic(s) used Service Stop ✓

  16/16

 Reuse  Embed

Activity 2 - Select a discovered issue (centre row) from the Case study 2's network and drag to the appropriate "Essential Eight" that would solve the issue.

Application control
Application control is implemented on all workstations and servers to restrict the execution of executables to an approved set.

Daily Backups
Backups of important information, software and configuration settings are performed monthly. Backups are moved for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.

Configure Microsoft Office macro settings
Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.

Patch operating systems
Security patches are also in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

User application hardening
Web browsers are configured to block or disable support for Flash content.

Multi factor authentication
Multi-factor authentication is used to authenticate all users of remote access solutions.

Patch applications
Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendor, independent third parties.

Restrict administrative privileges
Privileged access to systems, applications and data repositories is validated. Policy security controls are used to prevent privileged users from loading malware, breaching the web and other may follow via online services.

Access to HR Payroll ✓

Simple Authentication System ✓

HR system ageing ✓

Help Form accessed

4/4

Reuse Embed

ESSENTIAL EIGHT MATURITY MODEL FOR CYBER SECURITY

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 DEFENCE-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.

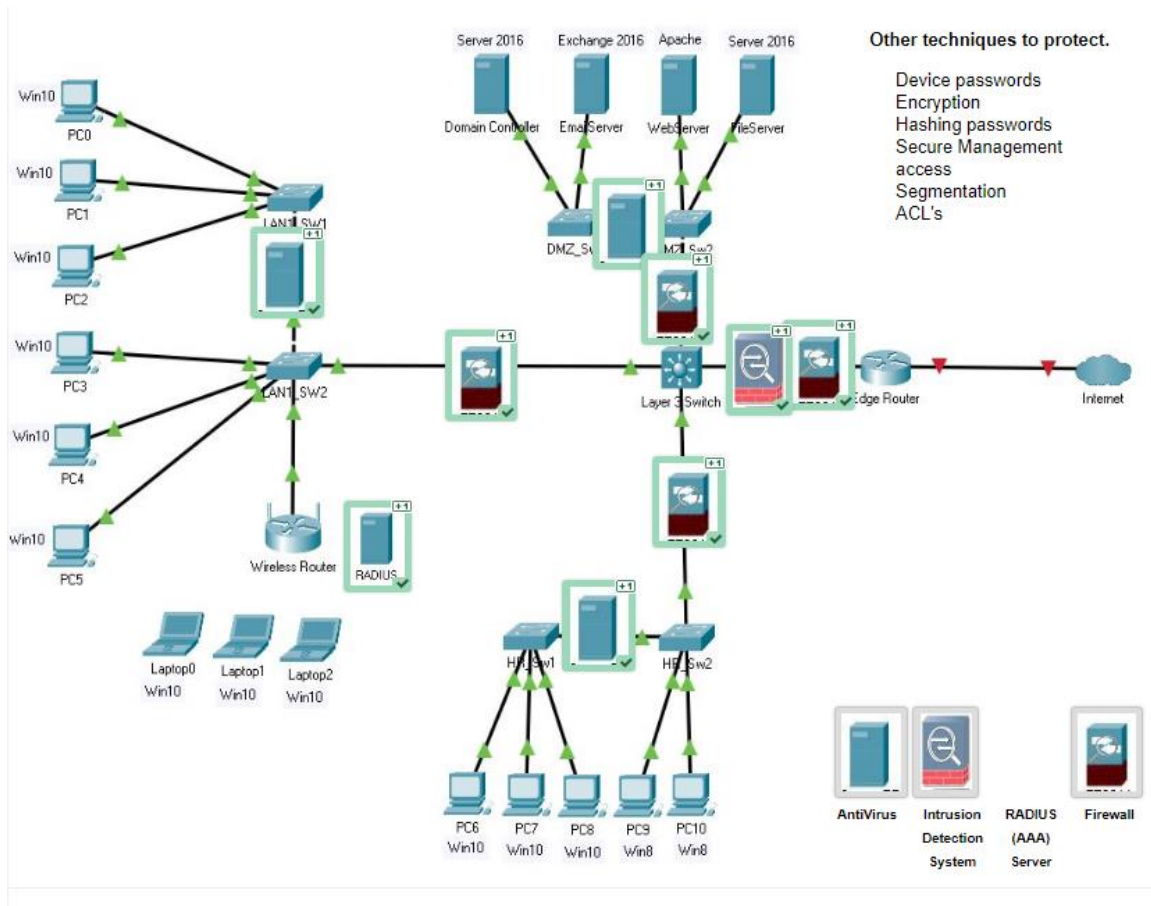
In contrast to: Defence-in-Breadth

– 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>

Activity 2 - Secure The Network Using Defence-In-Depth Stage 2 - Operating Systems. Drop the correct statement under the headings.

Application Control <div>Prevent .exe ✓ (+1)</div> <div>Prevent installers ✓ (+1)</div> <div>Prevent DLL ✓ (+1)</div> <div>Prevent scripts ✓ (+1)</div>	Daily backups <div>Perform Daily ✓ (+1)</div> <div>Restore Plan ✓ (+1)</div> <div>Offsite storage ✓ (+1)</div>	Restrict administrative privileges <div>revalidate staff members ✓ (+1)</div> <div>create separate attributable accounts ✓ (+1)</div> <div>identify tasks which require administrative privileges ✓ (+1)</div>	User application hardening <div>Disable unneeded features ✓ (+1)</div> <div>Block Flash ✓ (+1)</div>
Configure Microsoft Office macro settings <div>Block macros from the Internet ✓ (+1)</div> <div>Disable VBA macros ✓ (+1)</div>	Patch applications <div>Update Applications ✓ (+1)</div> <div>Restrict Java ✓ (+1)</div> <div>Remove Flash from Office ✓ (+1)</div>	Multi-factor authentication <div>Authenticator App ✓ (+1)</div> <div>SMS prompt ✓ (+1)</div>	Patch operating systems <div>Patch Server Vulnerabilities ✓ (+1)</div> <div>Patch Router Vulnerabilities ✓ (+1)</div> <div>Patch PC Vulnerabilities ✓ (+1)</div>

Activity 3 - Essential 8 Categories

Prevents attacks	<div>USER APPLICATION HARDENING ✓ (+1)</div>	<div>CONFIGURE MICROSOFT OFFICE MACROS ✓ (+1)</div>	<div>PATCH APPLICATIONS ✓ (+1)</div>	<div>APPLICATION WHITELIST ✓ (+1)</div>
Limits extent of attacks	<div>RESTRICT ADMIN PRIVILEGE ✓ (+1)</div>	<div>PATCH OPERATING SYSTEM ✓ (+1)</div>	<div>MULTI-FACTOR AUTHENTICATION ✓ (+1)</div>	
Recovers data & system availability		<div>DAILY BACKUP ✓ (+1)</div>		

week6 - ontological model of attacks - figure1 ấ

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

Group Activity

Which tactics were used by the attackers?

Target?

Communication Method, Direct or Indirect?

Compliance Principle?

Technique?

Medium?

Goal?

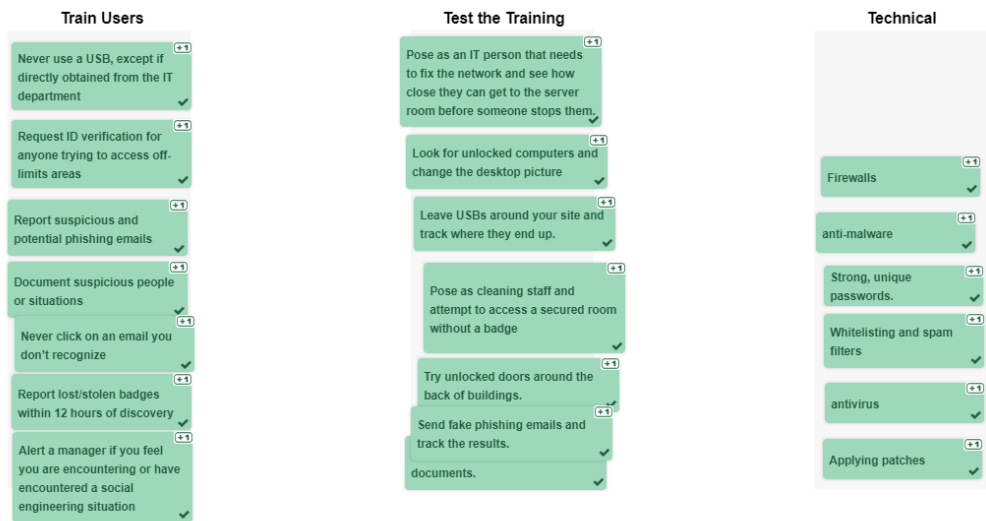
What mitigation techniques could be used for this kind of attack?



Mitigation Strategies

Build a positive security culture	Staff are aware of their security responsibilities and report potential phishing attacks as soon as possible
	Not think they shouldn't say anything because they might get in trouble
Learn the psychological triggers	Attackers exploit several psychological triggers to get past people's natural defenses
	Create situations of false urgency and heightened emotion
	Rely on people's conditioned responses to authority
Train your staff	Understand the consequences of social engineering attacks
	Don't open suspicious email attachments
	Think before providing sensitive information
Test the effectiveness of the training	Simulated phishing attacks will give you a good idea of your employees' susceptibility to phishing emails
Implement appropriate technical measures	Using firewalls, antivirus, anti-malware, whitelisting and spam filters to keep malicious traffic to a minimum
	Applying patches and keeping your systems up to date
	Implementing a policy of using strong, unique passwords

Social Engineering Activity 2 - Plan Design



maturity level

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

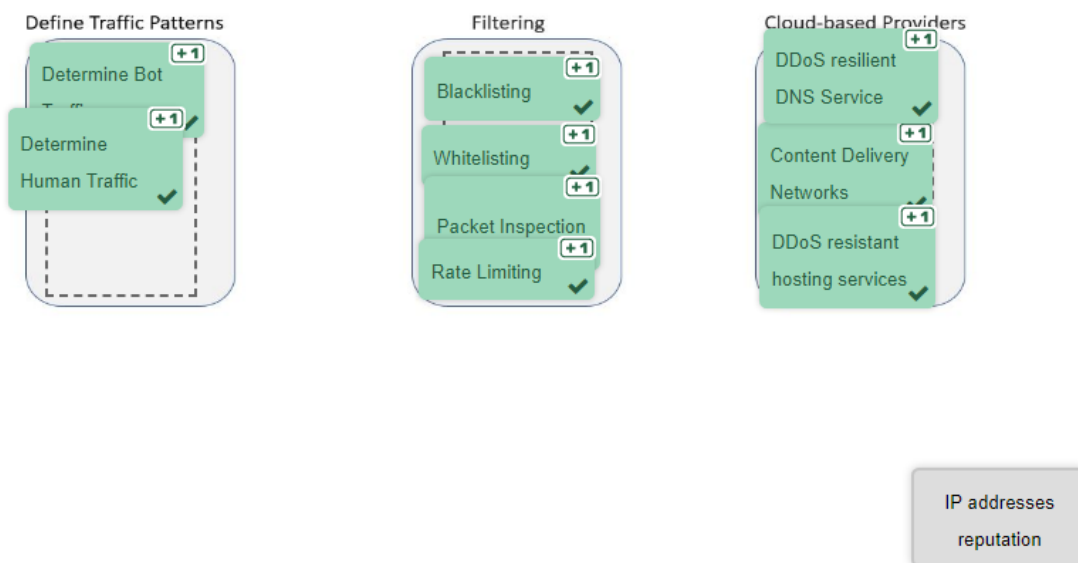
xem bảng maturity patch application a - có 1 câu hỏi là khi maturity level nào nên dc áp dụng khi cần được update within 48 hours (level 3)

WEEK 8 DDOS

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

tại sao bạn chọn đáp án đêi

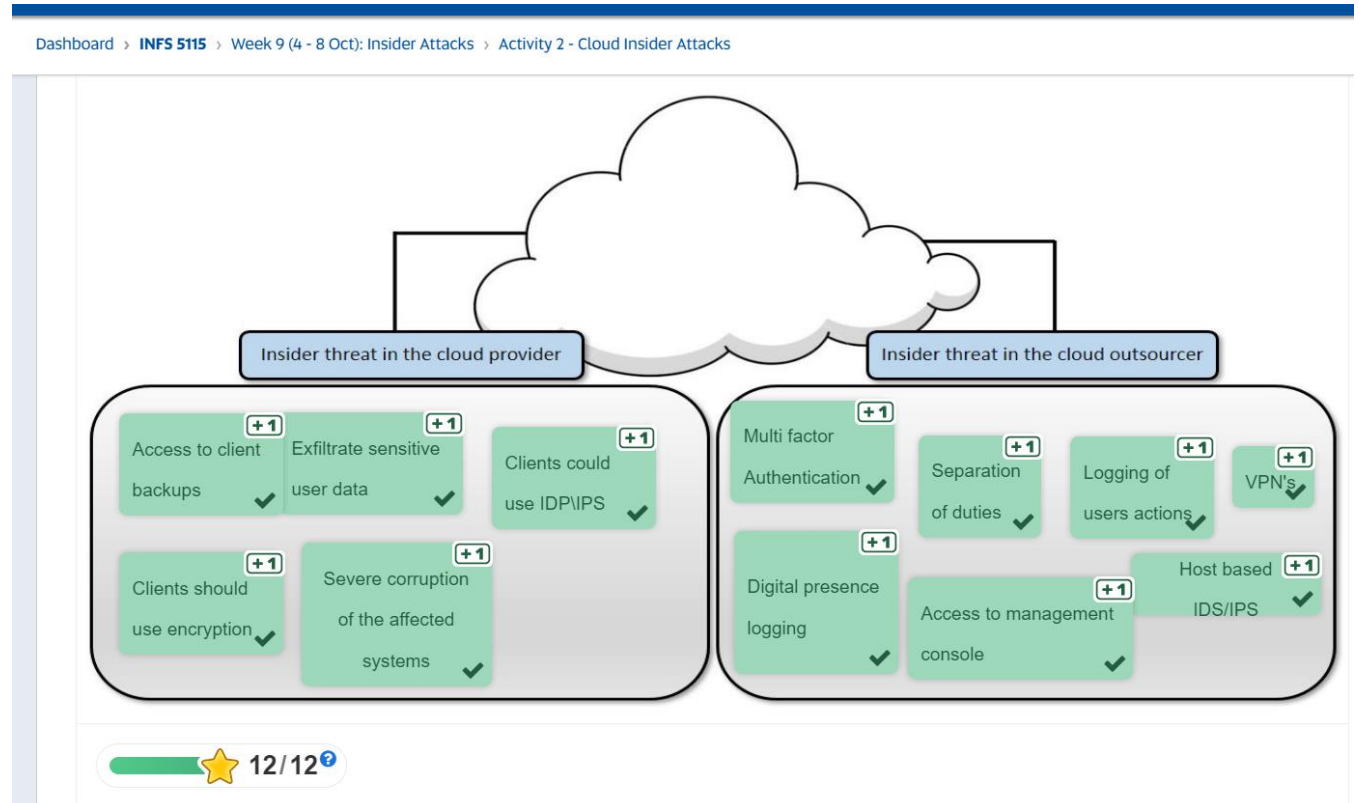
Activity 2 - Drag and Drop Mitigation Techniques



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

Question 1

Complete

Marked out of 5.00

Flag question

Background

An employee of a large Credit Union has brought a USB into the workplace to install some software onto their workstation that they believe will make them more productive. The employee installs the software and unknowingly releases a vulnerability onto the network.

Questions

- Which two of the Essential 8, if implemented to the appropriate level, would have prevented this from occurring? (2 marks)
- Justify your answers (3 marks)

Application control/whitelisting: Restricts the execution of executables, script, software libraries, and installers on all work stations to privileged hosts [UniSA SP2-2021, Week 6, Slide 14-16].

Justify: As the employee could still install an software into the network, this strategy was breached.

Restrict administrative privileges: Privileged access should only be limited to related personnel. This strategy is also used in the Insider Threat Prediction model for espionage detection and mitigation. [UniSA SP2-2021, Week 6, Slide 26, 27]

Justify: As the employee had the privilege to install an software, this also violates this principle which aims to provide the least privileges to staff to staff of the related area.

Word count: 109

Question 2

Complete

Marked out of 5.00

Flag question

There are a number of cybercrime categories.

List and describe five (5) of these categories.

(5 marks)

Source: [UniSA SP2-2021, Week 4, Slide 9, 10]

Cyber abuse - Online bullying, harassment or stalking

Online Image Abuse – Threats or act of sharing one's private images or videos online.

Online shopping fraud or romance fraud - Deception into sending money or goods to fraudsters online.

Identity theft - Theft of one's personal or business identity data to gain unauthenticated access to online accounts.

Email Compromise - Deceptive emails that aim to trick one to send his money or goods to fraudsters.

Word count: 82

Question 3

Complete

Marked out of 5.00

Flag question

Background

A cybersecurity breach within a network has compromised a database of usernames and email addresses. Investigations have determined the passwords of the users have not been stolen and are safe in an offsite location. 24 hours later the users of the network report they cannot log in and have been advised that their accounts have been locked out for 30 minutes.

Questions

- What type of attack has been performed on the users' credentials of the network? **(1 mark)**
- Justify your answer **(4 marks)**

It is possible that the type of attack used was T1110 Brute force: Credential Stuffing (Mitre Attack)

Justify: Considering that the accounts cannot be logged in, it is highly probable that adversaries used credentials from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. As occasionally after a breach incident, large amount of credentials of the victim are dumped online and can be used by adversaries to take advantage of users who use the same passwords for personal and business accounts. As many log in attempts are taken, the log in mechanism of the service prevents the users of the network to log into their accounts for 30 minutes.

Reference:

<https://attack.mitre.org/techniques/T1110/004/>

Word count: 115

Question 4

Complete

Marked out of 5.00

Flag question

When hashing a password using an algorithm, the same plaintext input will always produce the same hashed output.

- Explain the technique that is commonly used to strengthen the security of password storage, which results in different hashes being stored for different users with the same input password. **(4 marks)**
- What kind of attack does this technique protect against? **(1 mark)**

Source: [UniSA SP2-2021, Week 3, Slide 29].

In cryptographic hash functions password storage, as an adversary can use rainbow tables which relates passwords to the hash values. Salt values that are random data of given length in form of plaintext are added to the password before they are hashed. This ensures that the same passwords will have different hash values.

As an example, the original password may be "strongpassword", when a salt value which is "xyz" is added to the password, we would get "strongpasswordxyz", this would change the hash and make it impossible for adversaries to use rainbow tables. Only those with the hash key and salt value could unhash the password.

This mitigates the use of rainbow tables, and man-in-the-middle attacks where the third-party could compromise the confidentiality and possibly integrity of the data being sent.

Word count: 138

Question 5

Complete

Marked out of 5.00

Flag question

Alice has used an asymmetric cryptographic technique to encrypt data with her private key. Alice then sends the data to Bob. Bob attempts to decrypt the data using his private key and complains that he cannot decrypt the data.

- Describe the problem. **(2.5 marks)**
- Explain how Bob should decrypt the data? **(2.5 marks)**

In asymmetric cryptography, a user possesses a secret key as in symmetric cryptography but also a public key [UniSA SP2-2021, Week 3, Slide 6]. A private key refers to one only that user knows, and public key is one that both sides will know.

In practice, the ciphertext encrypted by the public key can only be deciphered by the private key, and vice versa, the ciphertext encrypted by the private key can only be decrypted by the public key.

The problem: As the message was encrypted by Alice's private key, it cannot be decrypted by Bob's private key

The solution: Bob should decrypt the data using Alice's public key.

Word count: 109

Question 6

Complete

Marked out of 5.00

Flag question

Background

Derrick, a systems administrator, has been employed at *ADC Consulting Pty Ltd* for over 10 years. His supervisor has informed him of a pending company restructure in which Derrick's unit will be absorbed into a new unit and Derrick will not be needed anymore. The following week, Derrick stops attending meetings, comes into work when everyone else is away, connects to a restricted company server, and downloads many documents that he does not need to do his job.

Questions

- What kind of threat could this behavior indicate for *ADC Consulting Pty Ltd*? Justify why this is the case. **(3 marks)**
- Explain one administrative and one technical control that *ADC Consulting Pty Ltd* can use to mitigate the impact of this threat? **(2 marks)**

Source: [UniSA SP2-2021, Week 10, Slide 4].

Derrick's behaviours indicate that he has become an internal threat for the *ADC Consulting Pty Ltd*. By using the Insider Threat Prediction Model, it could be seen that his predisposition to have grudge, stress level, and the likelihood of Derrick's wanting to cause harm to the company are high. His behaviours of violating work policies (not attending meetings), coming in the office when everyone is away, connecting to a restricted company server and downloading documents irrelevant to his work are the strongest warning signs that indicate he has become an internal threat.

To mitigate the impact of this threat, *ADC Consulting Pty Ltd* can restricts or deactivate access on his accounts privileges. One technical control could be to use multi-factor authentication on the storage, control of outbound emails and files and removable storage. Evidence of offences should be collected and preserved.

Word count: 148

Question 7

Complete

Marked out of 10.00

Flag question

Background

A medium-sized business has recently been the victim of a ransomware attack. You have been invited to offer cybersecurity advice to the business as it wishes to improve its security posture. The company has also revealed to you that they paid a hefty sum to the group responsible for the attack.

Questions

- Discuss why a company **might** pay the ransom if they are victims of ransomware, stating the potential implications of this decision. **(3 marks)**
- Discuss why a company **might not** pay the ransom if they are victims of ransomware, stating the potential implications of this decision. **(3 marks)**
- With reference to the Australian Signals Directorate's Essential 8, Describe four of the mitigation strategies that this business should implement to reduce future attacks. **(4 marks)**

As ransomware can encrypt the entire business computer systems, recovering data from it is almost impossible without the decryption key or backups. Thus, if the business has not done any data backups and has its data encrypted by the ransomware, the business might have to pay the ransom to retrieve the data if it is of importance.

The business might not pay the ransom if they possess comprehensive backups. Even though it would take hours or days to recover the entire computer system which renders the service unavailable, the business still won't suffer from huge financial losses from the ransom.

According to the Australian Signals Directorate's Essential 8, the business should implement:

- Daily backups: To prevent data losses and ensure system availability, limiting the extent of the attack [UniSA SP2-2021, Week 6, Slide 30, 31]
- Patch applications: To remove the known vulnerabilities in applications that adversaries could use to deliver the malware [UniSA SP2-2021, Week 6, Slide 30, 31]
- Patch operating systems: To remove the known vulnerabilities in OS that adversaries could use to deliver the malware
- Application control/whitelisting: To restrict the install of malware on all work stations to privileged hosts [UniSA SP2-2021, Week 6, Slide 14-16]

Question 8

Complete

Marked out of 10.00

Flag question

- Discuss the **relative importance** of confidentiality, integrity, and availability in relation to the information and systems used by a streaming company (*e.g Netflix*) that holds financial and personally identifiable information. **(5 marks)**
- The company has advised their *Chief Information Security Officer (CISO)* that they do not have the budget to address all three areas simultaneously, so it is important that you identify the key considerations for the company and highlight their order of importance for immediate consideration. **(5 marks)**

In definition, confidentiality refers to data and resources access management to prevent unauthorised disclosure and information misuse (Walkowski 2019). In the case of a streaming company, as financial and personally identifiable information would be held by the business, the utmost priority must be to safeguard the confidentiality of the information against data breaches. Taking into account the Code of Professional Conduct's Primacy of public interest, which states that public interest is always prioritised over personal interest [UniSA SP2-2021, Week 2, Slide 23], it is comprehensible that users would expect their information to be confidential and protected and that there are many legislations that would fine businesses for not being able to protect their customer's data. This matter involves the public trust to the business and depending on how high the trust is, it could either lead a business to its success or demise. As such, confidentiality must be the top priority for the streaming service.

Secondly, availability defines the property of resources being accessible and usable when demanded by authorised users. A system's utility would be limited if it is unavailable to authorised users even if it is confidential and integral [UniSA SP2-2021, Week 1, Slide 20]. Availability can be affected by power failure, hardware or software failure, natural disasters, human errors, or directly by Denial-of-Service attacks (Walkowski 2019). To a streaming service, customers need the service to always be available. Even though it is important, it cannot be compared to confidentiality. Thus, it is the second priority.

Last but not least, integrity refers to maintaining the accuracy and reliability of the data stored [UniSA SP2-2021, Week 1, Slide 14]. In other words, data integrity means that the data stored has not been tampered with and therefore is reliable. There are many factors that could intentionally (unauthorized access and modifications) or unintentionally (human errors, careless use, software flaws, or insufficient procedures for data protection mechanisms) compromise information integrity (Walkowski 2019). Compared to the other two principles, this prioritises the accuracy of data, even though this is needed, it is the least important of the three to the service.

In conclusion, as budget is limited, the business should prioritise the investment mostly in confidentiality, then availability, and lastly integrity when more budget is available

Reference:

Walkowski, D 2019, What Is The CIA Triad?, F5 Labs, viewed 2 July 2021, <<https://www.f5.com/labs/articles/education/what-is-the-cia-triad>>.

Question **9**
Complete
Marked out of 10.00
Flag question

Refer to the following case study

Peter works in a government department and has been asked to review the effectiveness of an existing advertising campaign. He is to put together a report that contains personally identifiable information. He has downloaded the required data from the department's server onto a USB drive. With a pending deadline and domestic flight to his home state in Victoria, Peter decides he will work at the airport while waiting for his flight and then email the report using the free Wi-Fi service just in time for his flight. After finishing the report, he leaves the USB drive on the couch at the airport lounge and boards his plane.

Questions

- With reference to the [ACS Code of Professional conduct](#), identify and justify three of the relevant values from this case study. (5 marks)
- Suggest two strategies that the state department can put in place to prevent a similar scenario from happening again. (5 marks)

1) Relevant clauses from the ACS Code of Professional Conduct

- a)
- value 1: The Primacy of Public Interest - a) identify those potentially impacted by your work and explicitly consider their interests; g) endeavour to preserve the confidentiality and privacy of the information of others.
 - justification: Peter did not understand or care about the significant consequences that his task could cause. With many personally identifiable information at hand, it is unacceptable for him to firstly, store the data in a USB which could be stolen or lost, secondly, work in a public place using vulnerable free Wi-Fi service, and thirdly, lose the USB due to his carelessness. He did not understand that he is responsible for maintaining the privacy of the data he has.
- b)
- value 2: The Enhancement of Quality of Life - c) understand, and give due regard to, the perceptions of those affected by your work; d) attempt to increase the feelings of personal satisfaction, competence, and control of those affected by your work.
 - justification: Peter did not understand or care about the those who could potentially have their personal information exposed by him, particularly their feelings and perceptions. His careless actions would cause huge damage to the owners of the personal information.
- c)
- value 3: Professionalism - a) take a calm, objective, informed and knowledgeable stance on your professional work, complementing your enthusiasm and engagement in it; f) refrain from any conduct or action in your professional role which may tarnish the image of the profession or detract from the good name of the ACS; g) endeavour to extend public knowledge and understanding of ICT; i) have pride in your profession, and protect and promote professionalism in ICT
 - justification: Peter violated multiple values of professionalism in his actions from how he did his job at a risky place, not caring about the customers' possible losses. His lack of knowledge violates the professionalism value. His incompetence tarnishes the image of the profession and harms the name of the ACS.

2) Strategies

- strategy 1: Provide sufficient training to provide knowledge and improve mindsets of the employees. This would be the most efficient form to prevent staff from unknowingly causing harm to the business.
- strategy 2: Control removable storage devices to disallow employees from carrying data outside of work. Besides, the data should only be accessible on the company's network.

Question **10**
Complete
Marked out of 10.00
Flag question

Background

A prospective start-up company has recruited five new IT students as their interns. These students need to perform several duties during the summer break before launching the company.

To ensure maximum efficiency, the company has granted all new employees full administrative privileges to access their entire internal network and file servers that hold the company's confidential data.

Questions

- Discuss the **risks** and associated **impact** of this approach. (5 marks)
- Explain **how** the principle of least privilege can apply to this situation. (5 marks)

Risks and the associated impact

These risks could be classified as internal risks. Even though the intern students may not aim to steal or modify the confidential data with malicious intent, it can still be due to greed, carelessness, or by accidents. Furthermore, as the interns are new, they can become victims to attacks and have their administrative credentials stolen.

As a consequence, the company has put itself in the risk of potential huge data breaches, financial and reputation losses, legislative fines, and confidential data losses.

Application of principle

According to the principle of least privilege, "Every program and every user of the system should operate using the least set of privileges necessary to complete the job" [UniSA SP2-2021, Week 1, Slide 24]. All intern students should be given only enough privileges related to their job. This restricts their access to all confidential data irrelevant to their work, minimizing the losses even if an attack was to happen and helps identifying attackers much easier.

Question **11**
Complete
Marked out of 10.00
Flag question

Background

A senior accountant of a large supermarket chain is lonely and is desperate to start living with someone else. They have received an email invitation, which requires them to join an online dating platform at a discount, by clicking on a link before the link expires in three hours. Moments after joining, they receive a friend request from overseas who has promised to come and visit at the earliest opportunity. The new friend has also indicated that times have been hard on their side and requires urgent medical attention before traveling to come and visit. In a hurry, the accountant has sent AUD \$5,000 to her new friend to cover medical and travel expenses. Shortly after sending the funds, all communication from the overseas friend ceases. Two weeks later it becomes obvious that three of the victims' friends, who clicked on the same link, were also victims.

Questions

From this social engineering attack, **identify** and **justify** your choices for the following.

- Compliance principle(s) (2 marks)
- Medium/media (2 marks)
- Target(s) (2 marks)
- Goal(s) (2 marks)
- Technique(s) (2 marks)

- Compliance principle (s) (2 marks)

The compliance principle refers to why the a victim would comply with the malicious request. In this case, it is about friendship or liking, as people are more likely to follow a friend's request. The victims were tricked into believing that their friends, the fraudster, was truly in need and thus, unknowingly send money to the fraudster.

- Medium/media (2 marks)

The medium used was a phishing email which led to an online dating platform. This type of direct communication promotes interaction between 2 parties and can easily engage targets and trick them into doing things that the adversaries want.

- Target(s) (2 marks)

Even though the victim in this scenario was a senior accountant of a large supermarket chain, the attack appears to not aim at the supermarket system, considering that the adversary immediately disappear after his goal for financial gain has been achieved. Thus, the target in this case is in every web end users whom would get randomly attacked by the fraudsters.

- Goal(s) (2 marks)

Considering the above point of adversary disappearing after he has been transferred money, although there is a small chance of the attack aiming to obtain credentials for unauthorised access, it is more likely that the motive was for financial gain - which has been achieved.

- Technique(s) (2 marks)

Phishing - Adversary sent phishing emails to trick victims to get in their environment by an offer that would expire in 3 hours.
Social Engineering - Adversary tricked targets into transferring money to his account by telling them his fake sad story.

Question **12**
Complete
Marked out of
10.00
1" Flag
question

Background

The Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report, (July 2019 to June 2020) outlines two of the current trends as listed below:

- Malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. Phishing and spear-phishing remain the most common methods used by cyber adversaries to harvest personal information or user credentials to gain access to networks, or to distribute malicious content.
- Ransomware has become one of the most significant threats given the potential impact on the operations of businesses and governments. Cybercriminals often illicitly obtain user logins and credentials through spear phishing, before utilising remote desktop protocol (RDP) services to deploy ransomware on their targets.

You are the **Chief Information Security Officer (CISO)** for an organisation and have been asked to assess the security challenges for employees working at home during the Covid-19 crisis.

Question

With consideration of the above threats:

- Discuss five (5) security challenges that your company might face as a result of employees working from home. (5 marks)
- Discuss the appropriate security controls that you might implement as a result of this. (5 marks)

Security challenges

1. Employees working from home could be a potential threats considering that they could become victims of social engineering attacks.
2. Usually, with sufficient privileges from the stolen credentials, adversaries also compromise multiple application security layers.
3. Concerning working practices, as no one is there to monitor how the workers work, they can intentionally or unintentionally create vulnerabilities to the business system.
4. As employees can use their personal devices, if vulnerabilities are not patched properly, they could be hacked and adversaries would have a point of access to the confidential data through the personal machines. Plus, as the personal devices are not scanned by the system security, they could become a persistent threat to the system.
5. With compromised credentials, adversaries could expand their presence by sending spearphishing emails to other staff and increase the privileges they have.

Appropriate security controls

As a result of this, training is the most important priority to improve the mindsets of employees against social engineering attacks and how to protect their devices.

The company should provide secure work devices to the employees that already has a scanner for threats and can automatically update patches.

The principle of least privileges should be used to minimize the impact in case an account is compromised.

Multi-factor authentication should be used to avoid unauthorised access and provide immediate notification when one happens.

Techniques in identifying internal threats should also be implemented to locate the malicious employees and attackers when they try to obtain information outside of their related work.

Question **13**
Complete
Marked out of
10.00
1" Flag
question

The Glossary of Key Information Security Terms defines **adequate security** as "Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information"

Demonstrate your understanding as to why it is important for organisations to **continuously** assess and evaluate security measures that are adequate for their needs? (10 marks)

Adequate security means that the riskier and larger the consequences that loss, misuse, or unauthorised access to or edit of the company's information could cause, the more secure the company's system should be.

As the scale of a company grows, the chance of it becoming a target to the attackers is higher and thus, has higher risks to data breaches. Depending on the type and volume of information that the company stores, the losses would also scale up proportionally. Thus, they should strengthen their security accordingly to provide confidentiality, integrity, and availability to the data through cost-effective management methods, controls of personnel, operations, and technical. That is why companies need to continuously assess and adapt to new security measures that will adapt with their growing requirements.