CYBERSECURITY

DARK WEB

WIE3003 INFORMATION SYSTEM CONTROL AND SECURITY
NG XIAN HENG U2102855

VULNERABILITIES, CYBER-ATTACKS, AND THREATS

Cyber-attack

RANSOMWARE

A type of malware that encrypts a victim's files.
The attacker will demand a ransom from the victim to gain access to the encrypted data after payment.
To mitigate ransomware, regularly back up data, use updated antivirus software, keep software current, implement network security measures, encrypt data, and monitor for unusual activity.

Cyber-attack

DENIAL-OF-SERVICE

An attack in which the attacker tries to make a targeted server or service unavailable to its users by disrupting the services of a host.
The attacker will flood the network with irrelevant traffic to slow down a legitimate request.
To mitigate DoS attacks effectively, implement network filtering mechanisms such as firewalls and intrusion prevention systems, coupled with rate limiting techniques, to control and manage incoming traffic,

Vulnerabilities

DATA BREACH

An incident where unauthorized individuals gain access to confidential or sensitive information from a database.
An attacker gains access to a system through phishing, malware, or other methods, and starts to extract data from the system. The stolen data can then be used by attackers for various purposes.
To mitigate data breaches, enforce strict access controls, encrypt sensitive data, regularly update security protocols.

Cyber-attack

PHISHING

Phishing is a cyber-attack where attackers impersonate a trusted entity to trick individuals into revealing sensitive information.
It works by sending fraudulent emails or messages that appear to be from legitimate sources.
To mitigate phishing, be cautious with emails, check email addresses for accuracy, use antivirus software, and educate employees about the risks and signs of phishing.

Threats

MALWARE

Malicious software designed to cause damange to server, network or computers.
It's delivered through emails, websites, or downloads, then infects systems to perform malicious activities.
To mitigate malware, use updated antivirus software, be cautious with downloads and emails, and keep all software current.

Cyber-attack

CROSS-SITE SCRIPTING (XSS)

XSS is a security vulnerability where attackers inject malicious scripts into web pages.
It works by exploiting the trust a website has in user-provided data, enabling the attacker to execute malicious code in the victim's browser.
To mitigate XSS, validate and sanitize user inputs, use HTTPOnly cookies, implement Content Security Policy (CSP), escape user-generated content, and keep software updated.

ADVANCED TECHNOLOGIES IN MITIGATING CYBER THREAT

ANOMALY DETECTION

AI-powered systems can analyze network traffic patterns and user behaviour to identify anomalies that may indicate a DoS attack or unauthorized access attempt.

NATURAL LANGUAGE PROCESSING (NLP)

NLP algorithms can analyze unstructured data sources, such as logs, emails, and social media, to identify indicators of potential security threats.