Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Title : Information Security
Course Code : CS6404
Date : 07-03-2022

Soltion 2 a :

Threat

A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system. Threats can also be defined as the possibility of a successful cyber attack to get access to the sensitive data of a system unethically. Examples of threats include computer viruses, Denial of Service DoS attacks, data breaches, and even sometimes dishonest employees.

Types of Threat

Threats could be of three types, which are as follows:

Intentional- Malware, phishing, and accessing someone's account illegally, etc. are examples of intentional threats.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Title : Information Security
Course Code : CS6404
Date : 07-03-2022

Natural- Natural disasters can also damage the data, they are known as natural threats.

2 - Vulnerability:

In cybersecurity, a vulnerability is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals.

Types of Vulnerability
Vulnerabilities could be of many types, based on different criteria, some of them are:

Network
Operating system
Human
Process

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Title : Information Security
Course Code : CS6404
Date : 07-03-2022

Risk:

Cyber risk is a potential consequence of the loss or damage of assets or data caused by a cyber threat. Risk can never be completely removed, but it can be managed to a level that satisfies an organization's tolerance for risk.

Cyber risks can be defined with this simple formula- Risk = Threat + Vulnerability. Cyber risks are generally determined by examining the threat actor and type of vulnerabilities that the system has.

There are two types of cyber risks, which are as follows:

1. External- External cyber risks are those which come from outside an organization
2. Internal- Internal cyber risks come from insiders.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security
Date : 07-03-2022

Difference Between Threat, Vulnerability, and Risk

Threat

1. Take advantage of vulnerabilities in the system and have the potential to steal and damage data.
2. Generally, can't be controlled.
3. It may or may not be intentional.
4. Can be blocked by managing the vulnerabilities.

Vulnerability

Known as the weakness in hardware, software, or designs, which might allow cyber threats to happen.
Can be controlled.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security
Date : 07-03-2022

Generally, unintentional.
Vulnerability management is a process of identifying the problems, then categorizing them, prioritizing them, and resolving the vulnerabilities in that order.

Risks

The potential for loss or destruction of data is caused by cyber threats.
Can be controlled.
Always intentional.
Reducing data transfers, downloading files from reliable sources, updating the software regularly, hiring a professional cybersecurity team to monitor data, developing an incident management plan, etc. help to lower down the possibility of cyber risks.

Name : lakhan Kumawat
Roll No : 1906055
Course Code : CS6404
Course Title : Information Security

Solution 2 B :

An active attack or what is more commonly referred to as hacking is an actual attempt to disrupt or take down your system.

During active attacks, intruders introduce foreign data or programming into your system, and-or potentially change data within the system. During these types of attacks, hackers are actively sending traffic that can be detected. A denial of service or DDoS attack is one such example.

A passive attack, on the other hand, involves an attacker stealthily monitoring and-or collecting information on your network activity. These attacks are much more difficult to detect, because they are not actively targeting anything for disruption and therefore may go undetected for quite some time.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security
Date : 07-03-2022

Ratt lo

Solution 2 B: continue -

Important defense against these attacks

Passive :-

1. Enumeration
2. Dont be active for personal information on social media
3. Make sure you trust your friend beacuase he -she can also reveal your personal information
4. Have Antivirus installed on your local machine
5. Dont post your secret keys in the public .
6. Use VPN for your personal safety and browsing.

Defense against active attacks

1. Put your firewall on always
2. Scan your computer for virus and threats

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security
Date : 07-03-2022

Defense against active attacks

3. Make sure that services you are using are up-0-date.
4. Check task manager and end the unknown malicious tasks.
5. use authentication for communication for data fragile sites
6. Do traffic ananlysis regularly and identify unknown traffic
8. Deny notification and downloads permissions to unknown sites.
9. Always use https ssl-tls protocols for secured packet transmission over internet.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security

Solution 3 :

Informational Assets

1. Private message of users
2. Users account information
3. Users Banking details
4. Employee and company Confedential details
5. Users Devices which contain all the confedential info incomplete prototype infor

Potential Cyber security threats to assets

1.Plain text message weakly encrypted message heading to easy decryption
2. Weak passwords or login system or weak session management
3. Unknown call-message asking for bank info or insecure payment getwat involvement
4. An employee opening a malicious website or unknown mail through his iphone or laptop

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security

Solution 3 : continue --

5. Theft of manual permit document
6. keylogger spyware and unprotected VPN

Security Mechanisms
1. End to end encryption of message
2. OTP unificatoin while loggin in system
3. OTP verification + 2 step verification + 3 way handshaking with bank' clients and platform during transactions
4. Fingerprint biometric check while entering
5. Proper antivirus firewall and biometric verification while using the authorized content of system
6. Compnay Provided VPN's , antivirus , weekly - biweekly assesment of device

Name : lakhan Kumawat
Roll No : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security
Date : 07-03-2022

Solution 5:

Given : secret key - the last 3 digits of your roll number mod 26

To find : vulnerability of the cipher

To do : Identify the attack to which the cipher is vulnerable and Discuss that attack

my name : Lakhan

Last Three Digits of my roll number : 055

Therefore Secret Key is 55 mod 26 which equals to 3 , so we have to apply shift of 3.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security

Solution 5 : continue

Formula for encryption :-

$En(x)$ is equals to $(x+n) \bmod 26$

Also A B C - - - - - X Y Z

We 00 1 2 - - - 23 24 25 .

Text LAKHAN

L - 11 A-00 K-10 H-7 A-00 N-13

$L = (11+3) \bmod 26 = 14 = O$

$A = (0+3) \bmod 26 = 3 = D$

$K = (10+3) \bmod 26 = 13 = N$

$H = (7+3) \bmod 26 = 10 = K$

$A = (0+3) \bmod 26 = 3 = D$

$N = (13+3) \bmod 26 = 16 = Q$

LAKHAN - Cipher Text - ODNKDQ

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security

Solution 5 : continue

There are two types of attacks — passive attacks and active attacks. Snooping on data, eavesdropping is simple examples of passive attacks. Passive attacks are not as harmful as they do not cause any altering or modification of data. Active attacks cause data to be altered, system files to be modified and are obviously much more harmful than passive attacks.

These are some examples of active attacks to which our text is vulnerable:

Bruteforce attacks

Brute-force attacks involve trying every possible character combination to find the 'key' to decrypt an encrypted message. While brute-force attacks may take a smaller amount of time for smaller keyspaces, it will take an immeasurable amount of time for larger keyspaces.

Name : lakhan Kumawat
Roll NO : 1906055

Branch : CSE-1
Course Code : CS6404
Course Title : Information Security

Solution 5 : continue

Cipher-Only attack

In the cipher-only attack, the attacker knows the ciphertext of various messages which have been encrypted using the same encryption algorithm. The attacker's challenge is to figure the 'key' which can then be used to decrypt all messages.

Known-plaintext attack

In the known-plaintext attack, the attacker knows some of the plaintext and the ciphertext. He then has to figure the key by reverse engineering and he can decipher other messages which use the same key and algorithm.

The known-plaintext attack was effective against simple ciphers such as the substitution cipher.