**An attacker breaks into a corporate database and deletes critical files. What security goal is this attack focused on?**

Step 1: Answer

The destruction of crucial files and the attack on a corporate database compromise the system's confidentiality and integrity. Integrity and confidentiality were therefore the security objectives on which this assault was concentrated.

Step 2: Explanation

There are various security objectives that this kind of attacks should concentrate on when intruders breach a business database and erase all the vital files. These are listed below:

Confidentiality:

A security goal called confidentiality states that no one should have access to sensitive data, whether it is stored on a computer system or travelling over a network.

How can detective countermeasures act as preventive countermeasures?

Step 1:

A security control's main objective may be preventative, detective, corrective, compensating, or deterrent in nature. In the same way that regulations or training on social engineering are used to protect people, controls are also used to do so.

Information's availability, confidentiality, and integrity are all at danger due to a lack of security safeguards. The security of the people and resources inside a company is likewise subject to these dangers.

Step 2:

Countermeasures are put in place by detectives to help find any malicious activity. A detective control merely recognises and reports intrusion attempts; it does not prevent or mitigate them. Intrusion Detection Systems, for instance, are examples of this kind. Alarms.

The most popular and economical method of preventing fraud is through preventative measures. By lessening the possibility and effects of fraud, they either prevent or restrict the danger.

When a threat is identified, it can assist the user in immediately minimising harm as well as in identifying the threat that is detective counter measure and preventive countermeasure can keep track from succeeding.

Detective measures serve as preventative measures. Detective controls are made to look for any errors or abnormalities. The purpose of corrective controls is to eliminate errors or anomalies that have been found. Contrarily, preventive controls are intended to stop errors and anomalies before they start. Controls might be hybrid, automated, or both.

Why do you think DDoS attackers use zombies to attack victims instead of sending attack packets directly to victims? Come up with two reasons.

Step 1:

DDoS Attack, also known as a "Distributed Denial-of-Service (DDoS) Attack," is a type of cybercrime where the perpetrator overwhelms a server with internet traffic in an effort to prohibit users from accessing linked websites and online services.

In a botnet run by the hacker, zombie machines frequently collaborate to carry out tasks like sending spam via email and performing distributed denial-of-service (DDoS) assaults against web sites. The majority of victims have no idea that their machines have turned zombie.

Step 2:

Distributed denial-of-service (DoS) assaults paralyse the victim's servers and systems and jam their network access points with pointless traffic, as with any denial-of-service attack. Technically, distributed denial-of-service assaults are more sophisticated than the denial-of-service attacks of the past. With distributed DoS, the attacker sets up an online network of compromised devices, or "zombies," that, when directed, attack the victim. The "zombies" frequently continue to attack the victim even after the "control" equipment is destroyed. Additionally, hackers don't even need to build their own "zombie armies"; instead, they can rent "armies" from other hackers that have amassed as many as 20,000 machines.

Step 3:

In a botnet run by the hacker, zombie machines frequently collaborate to carry out tasks like sending spam via email and performing distributed denial-of-service (DDoS) assaults against web sites.

Assaults known as distributed denial-of-service (DDoS) attacks, in which numerous computers simultaneously overwhelm a target website, can be carried out using zombies. It is meant for a website's server to crash from a high number of simultaneous requests, blocking legitimate people from accessing the website.