Qtext :
In an organization, IT Help Desk received several complaints that the employees are receiving Viagra spam. Investigation revealed that one of the employee's computers was sending out those Viagra spam. They found that a program was installed (probably by a hacker) on the employee's computer that made it automatically send out tons of spam emails without the computer owner's knowledge. Identify five ways a hacker could get into the computer to set this up?

Answer 1. Hacked password 2. Out of date patches/updates 3. No anti-virus software or out of date anti-virus software 4. Clicking an unknown link or attachment 5. Downloading unknown or unsolicited programs on to your computer Your answer is also considered

Qtext :
(a) Explain clearly with examples between threat, vulnerability, and risk

(b) Explain a scenario in which existence of a threat might not pose any risk to the organization. [6 + 2 = 8]

Answer Threat: A threat is any form of hazard that has the potential to destroy or steal data, disrupt operations, or cause harm in general. Malware, phishing, data breaches, and even unethical employees are all examples of threats. Threat actors, who might be individuals or groups with a variety of backgrounds and motives, express threats. Understanding threats is essential for developing effective mitigations and making informed cybersecurity decisions. Threat intelligence is information regarding threats and threat actors. Vulnerability: A vulnerability is a flaw in hardware, software, personnel, or procedures that threat actors can use to achieve their objectives. Physical vulnerabilities, such as publicly exposed networking equipment, software vulnerabilities, such as a buffer overflow vulnerability in a browser, and even human vulnerabilities, such as an employee vulnerable to phishing assaults, are all examples of vulnerabilities. Vulnerability management is the process of identifying, reporting and repairing vulnerabilities. A zero-day vulnerability is a vulnerability for which a remedy is not yet available. Risk: The probability of a threat and the consequence of a vulnerability are combined to form risk. To put it another way, the risk is the likelihood of a threat agent successfully exploiting a vulnerability, which may be calculated using the formula: Risk = Likelihood of a threat * Vulnerability Impact Risk management is the process of identifying all potential hazards, analyzing their impact, and determining the best course of action. It's a never-ending procedure that examines new threats and vulnerabilities on a regular basis. Risks can be avoided, minimized, accepted, or passed to a third party depending on the response chosen. Your answer is also considered

Qtext :
In olden days, wax sealant was used to seal documents (they are probably used even today). They help verif unopened. When sealed with a custom signet ring, the sealant could also be used to verify the sender's ident were difficult to replicate. Recipients of the documents could have reasonable certainty that the message wa recognized the seal. What aspect of cybersecurity does this concept signifies? Explain this cybersecurity asp What kind of assurance does this cybersecurity aspect provides.

Answer Part A: The cybersecurity aspect this concept signifies is digital signature (1 Mark) Part B: Explain with an example the concept of digital signature using example (3 Marks) Part C: Assurance: A digital signature provides sender verification, message integrity, and nonrepudiation, or the assurance that a sender cannot deny having sent a message (3 Marks) Your answer is also considered

Qtext :
(a) Cybercrime can be categorized based on the role that the computer plays in the criminal activity. Name and explain those different categories.

(b) Consider the following cybercrimes and indicate in which category it falls

a. Offences related to child pornography involving
    i. Producing
    ii. Offering or making child pornography available
    iii. Distributing or transmitting child pornography
b. Credit card fraud; gambling
c. Data Interference
    i. The damaging, deletion, deterioration, alteration or suppression of computer data without right. [6 + 3 = 9]

Answer In cybercrimes, computers themselves can become targets, or computers can be used as a storage device, or computers can be used as communications tool. a. Offences related to child pornography involving (Computer as a storage device, communication tool) b. Credit card fraud; gambling (Computers as a communication tool) c. Data interference (Computer as target) Your answer is also considered

Qtext :
If you forget your password for a website and you click [Forgot my password], sometimes the company sends you a new password by email, sometimes it sends you your old password by email, sometimes it sends you a link for you to reset your password. Compare these three cases in terms of vulnerability of the website owner. [2 + 2 + 2 = 6]

Answer If the site tells you that your password was, that means the site is storing your password rather than just a hash of it. This means that anyone who gain access to the site's password database has access to all the passwords. If the site sends you a temporary password, there is a good chance it is not storing your actual passwords, which is the correct approach from a security perspective Your answer is also considered

Qtext :
You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log into your account and fix the problem.

a. Is there any problem here? Explain clearly.
b. What action you should take? Explain at least two different alternatives. [2 + 2 = 4]

Answer Delete the email. Better yet, use the web client (e.g. gmail, yahoo mail, etc.) and report it as spam or phishing, then delete it. Any unsolicited email or phone call asking you to enter your account information, disclose your password, financial account information, social security number, or other personal or private information is suspicious – even if it appears to be from a company you are familiar with. Always contact the sender using a method you know is legitimate to verify that the message is from them. Your answer is also considered

Qtext :
Describe the "Weaponization" phase of Cyber Kill Chain. This stage is considered challenging for defenders example of activities that adversaries perform at this stage. What kind of actions can defenders take during 1 = 6]

Answers With the knowledge of what kind of attack may be most appropriate to use against a company, an attacker would move to prepare attacks tailored to the target in the Weaponization phase. This may mean developing documents with naming schemes similar to those used by the company, which may be used in a social engineering effort at a later point. Alternatively, an attacker may work to create specific malware to affect a device identified during the recon. This phase is particularly challenging for defenders to develop mitigations for, because weaponization activity often occurs on the adversary side, away from defender-controlled network sensors. It's nonetheless an essential phase for defenders to understand, because it occurs so early in the process. Using artifacts discovered during the Reconnaissance phase, defenders may be able to infer what kind of weaponization may be occurring and prepare defenses for those possibilities. Even after discovery, it may be useful for defenders to reverse the malware to determine how it was made. This can inform detection efforts moving forward. Your answer is also considered