|  |  |
| --- | --- |
| As we increase the level of security, we usually decrease the level of productivity. Discuss   1. Explain Parkerian hexad in detail using it’s diagram 2. Phincolin Associates Limited’s email and file servers were encrypted in a ransomware attack. 3. Which element of the CIA triad is most affected?   Ii. What immediate steps would you take to restore and prevent the element in (i) for future incidents?  Using the concept of defense in depth, what layers might we use to secure ourselves against someone removing confidential data from our office on a USB flash drive?  Based on the Parkerian hexad, what principles are affected if we lose a shipment of encrypted backup tapes that contain personal and payment information for our customers?  If the Web servers in our environment are based on Microsoft’s Internet Information Server (IIS) and a new worm is discovered that attacks Apache Web servers, what do we not have?  If we develop a new policy for our environment that requires us to use complex and automatically generated passwords that are unique to each system and are a minimum of 30 characters in length, such as !Hs4(j0qO$&zn1%2SK38cn^!Ks620!, what will be adversely impacted?  Considering the CIA triad and the Parkerian hexad, what are the advantages and disadvantages of each model?  An online retail business is facing increasing cyber threats, including DDoS attacks and phishing attempts. The company needs to identify these threats and implement appropriate controls.   * Identify at least three major threats to the online retail business. * For each threat, describe the potential vulnerabilities that could be exploited. * Propose specific controls to mitigate each threat and explain how these controls would be implemented and monitored.   **Write short notes on Identity verification**   1. If we are developing a multifactor authentication system for an environment where we might find larger-than-average numbers of disabled or injured users, such as a hospital, which authentication factors might we want to use or avoid? Why? 2. Based on the Parkerian hexad, what principles are affected if we lose a shipment of encrypted backup tapes that contain personal and payment information for our customers?   **The history of cryptography and Modern cryptographic tools**  1. Above we saw that "CAESAR" becomes "RPTHPG" using a key P. Can you find a key that will turn "RPTHPG" back into "CAESAR"?  2. A plaintext was encrypted with a Caesar cipher, resulting in the following:  DOOV ZHOO WKDW HQGV ZHOO  work out what the plaintext was?  You are provided with the ciphertext ZKDWH LV D PHVVDJH LQ FLSKHU WHAW. Assume the message is in English.   * 1. Determine the shift key using brute force methods and explain how you identified the key.   2. Decrypt the message. | **1. Security vs Productivity**   * Higher security = more controls (passwords, encryption, monitoring). * These slow processes and reduce ease of use. * Trade-off between protection and efficiency.   **2. Parkerian Hexad (6 principles)**   * **Confidentiality** – prevent unauthorized disclosure. * **Integrity** – prevent unauthorized modification. * **Availability** – ensure access. * **Possession/Control** – who holds data. * **Authenticity** – verify source. * **Utility** – usefulness of data. *(Diagram: hexagon with the 6 principles as points).*   **3. Ransomware Attack** i. Most affected = **Availability**. ii. Steps:   * Isolate infected systems. * Restore from backups. * Apply patches, use endpoint security. * Implement regular backups + training.   **4. Defense in Depth (USB data theft)**   * Physical security (locks, guards). * Endpoint control (disable USB ports). * DLP software (monitor transfers). * Encryption of sensitive files. * Policies + user awareness.   **5. Lost Encrypted Backup Tapes (Hexad)**   * **Possession** (lost tapes). * **Confidentiality** (risk if encryption weak). * **Availability** (if no other backup).   **6. Apache Worm vs IIS**   * We do **not have vulnerability exposure** (IIS unaffected by Apache worm).   **7. Very Complex Password Policy**   * Adversely impacts **Availability/Utility** (hard to use/remember). * **CIA triad**: Strengthens Confidentiality & Integrity, weakens Availability. * **Hexad**: Affects Utility & Availability.   **8. Online Retail Threats**   * **DDoS**: Exploits server capacity → Control: firewalls, CDNs, rate limiting. * **Phishing**: Exploits users → Control: awareness training, email filters. * **SQL Injection**: Exploits weak coding → Control: input validation, WAF. *(Monitor via SIEM, IDS/IPS, logs.)*   **9. Identity Verification**   * Process of confirming a person’s identity. * Methods: ID documents, biometrics, OTPs. * Used in KYC, access control, and fraud prevention.   **10. MFA in Hospital Setting**   * Avoid: biometrics requiring mobility (fingerprint, retina for disabled). * Use: smart cards, tokens, PINs, voice/face recognition. * Reason: Accessibility for all users.   **11. Lost Encrypted Backup Tapes (Hexad repeat)**   * **Possession**, **Confidentiality**, **Availability** may be affected.   **12. History of Cryptography & Modern Tools**   * Ancient: Caesar cipher, substitution. * Middle ages: Vigenère cipher. * Modern: DES, AES, RSA, ECC, Hashing. * Tools: TLS/SSL, PGP, VPNs.   **13a. Caesar Cipher Key**   * "CAESAR" → "RPTHPG" means shift **+13**. * Key = 13 (ROT13).   **13b. Ciphertext**   * "DOOV ZHOO WKDW HQGV ZHOO" = **ALL’S WELL THAT ENDS WELL**.   **14a. Ciphertext: “ZKDWH LV D PHVVDJH LQ FLSKHU WHAW”**   * Brute force shifts until words make sense. * Shift = **3**.   **14b. Decryption**   * Plaintext = **WHAT IS A MESSAGE IN CIPHER TEXT**. |

|  |  |
| --- | --- |
| During an internal red team exercise, you compromise the workstation of an employee in the Human Resources department. To your surprise, the employee has administrative access to the Human Resource database, email distribution lists, and payroll software. As the attacker, you now have the same access.  A. List Three (3) specific exploits or damaging actions you could perform  using the employee's access.  B. Now take on the role of the security analyst and for each action you listed, explain why it was possible based on flawed access control decisions.  C. For each action, recommend one realistic and proportionate mitigation  using principles such as least privilege, access revocation, or access control models | **A.**  **Possible Exploits (Attacker actions)**   1. Alter payroll records (e.g., increase salary or redirect payments). 2. Exfiltrate sensitive employee data (PII, salary, bank details). 3. Send malicious/phishing emails through HR distribution lists.   **B. Why Possible (Flawed Access Control)**   1. **Payroll alteration** → Employee had unnecessary admin rights to payroll software. 2. **Data exfiltration** → Over-privileged access to HR database beyond job needs. 3. **Phishing via email lists** → Broad access to distribution lists without restriction.   **C. Mitigations**   1. **Payroll alteration** → Apply **least privilege**: HR staff should not have admin rights, only limited roles. 2. **Data exfiltration** → Use **role-based access control (RBAC)** with strict separation of duties. 3. **Phishing via email lists** → Restrict distribution list management; enable **logging and monitoring**; revoke unnecessary rights. |

|  |  |
| --- | --- |
| 1.  If we are developing a multifactor authentication system for an environment where we might find larger-than-average numbers of disabled or injured users, such as a hospital, which authentication factors might we want to use or avoid? Why?  2. Based on the Parkerian hexad, what principles are affected if we lose a shipment of encrypted backup tapes that contain personal and payment information for our customers? | **1. MFA in a hospital (disabled/injured users)**   * **Use**: Smart cards, tokens, PINs, voice recognition, facial recognition (accessible options). * **Avoid**: Fingerprint, retina/iris scans, or complex typing (may be hard for injured/disabled). * **Why**: Must ensure accessibility while still maintaining security.   **2. Parkerian Hexad – Lost encrypted backup tapes**   * **Possession/Control** → Lost tapes are physically out of organization’s control. * **Availability** → If no other backup, data may be unrecoverable. * **Confidentiality** → Still protected *if encryption strong*, but at risk if keys are compromised. |

|  |  |
| --- | --- |
| Harm occurs when a threat is realized against a vulnerability. To protect against harm, we can neutralize the threat, close the vulnerability, or both. | * **Threat** = potential danger (e.g., hacker, malware). * **Vulnerability** = weakness exploitable by a threat (e.g., unpatched software). * **Harm** = actual damage when a threat exploits a vulnerability.   **Protection approaches:**   1. **Neutralize the threat** → e.g., block attacker IP, remove malware. 2. **Close the vulnerability** → e.g., patch software, disable weak services. 3. **Do both** → strongest defense, prevents future exploitation. |

|  |  |
| --- | --- |
| You are the new Information Security Officer at a mid-sized hospital. One morning, all patient records become inaccessible due to a ransomware attack. Management panics and demands answers. Using only your knowledge from the CIA Triad, Parkerian Hexad, and defense-in-depth principles:  i. Identify THREE (3) security principles (from both CIA and Parkerian Hexad) that are violated in this incident and justify each with reference to the scenario.  ii. Describe THREE (3) specific layers in the defense-in-depth model that should have prevented or delayed this attack, and explain how they could have helped.  iii. The IT manager argues: "We had firewalls and antivirus, so this shouldn't have happened!" Based on the concepts from your reading, explain why such technical controls alone are insufficient, and suggest one non-technical control that could have made a difference.  iv. Assuming backups exist, explain the risk management process you would follow to recover and prevent future incidents, identifying one vulnerability, one threat, and one control in your answer. | **i. Three Security Principles Violated**   * **Availability (CIA & Hexad)** → Patient records are inaccessible. * **Integrity (CIA & Hexad)** → Files are modified/encrypted by attackers. * **Possession/Control (Hexad)** → Attackers control the hospital’s data instead of the hospital.   **ii. Three Defense-in-Depth Layers**   1. Network Perimeter → Firewalls and IDS/IPS could block malicious traffic or phishing connections before reaching users. 2. Host Layer → Endpoint protection and timely patching could stop ransomware from executing on the workstation. 3. Data Layer → Encrypted + offline backups would ensure data recovery even if systems are compromised.   **iii. Why Firewalls + Antivirus Are Insufficient**   * Attackers bypass perimeter tools with phishing, zero-day exploits, or insider actions. * **Non-technical control**: Security awareness training & policies — reduces human error and social engineering success.   **iv. Risk Management Process**   * i. Identify Assets → What to protect (data, systems). * ii. Identify Threats → Potential dangers (hackers, malware). * iii. Assess Vulnerabilities → Weaknesses (unpatched software). * iv. Assess Risks → Likelihood + impact of threat exploiting vulnerability. * v. Mitigate Risks → Apply controls (patching, training, backups).   “All Tigers Value Risk Management” |

**Defense-in-depth layers** you listed:

**i. External Network** → ISPs, internet traffic filtering, DDoS protection.  
**ii. Network Perimeter** → Firewalls, IDS/IPS, VPN gateways.  
**iii. Internal Network** → Segmentation, monitoring, internal firewalls.  
**iv. Host** → Endpoint security, patching, antivirus, configuration hardening.  
**v. Application** → Secure coding, input validation, WAF, access control.  
**vi. Data** → Encryption, backups, DLP, strong access control.

**i. Identify Assets**

* Find what you must protect (e.g., patient data, servers, networks, staff).
* Assets = anything of value to the organization.

**ii. Identify Threats**

* List possible dangers to those assets (e.g., hackers, malware, natural disasters, insider misuse).

**iii. Assess Vulnerabilities**

* Check weaknesses that threats can exploit (e.g., unpatched systems, weak passwords, no backups).

**iv. Assess Risks**

* Combine threat + vulnerability + impact.
* Example: Ransomware (threat) + unpatched system (vulnerability) → High risk of downtime + data loss.

**v. Mitigate Risks**

* Apply controls to reduce risks.
* Options: Avoid (don’t use risky tech), Reduce (patch, firewalls, training), Transfer (insurance, outsourcing), Accept (if low risk).