**QUESTION 1201**
The optimum business continuity strategy for an entity is determined by the:
- Lowest downtime cost and highest recovery cost.
- Lowest sum of downtime cost and recovery cost.
- Lowest recovery cost and highest downtime cost.
- Average of the combined downtime and recovery cost.

**Correct Answer**: B
**Topic**: Optimizing Business Continuity Strategy
**Explanation**: The best strategy balances the lowest downtime and recovery costs to minimize overall disruption and expenses.

---

**QUESTION 1202**
The PRIMARY objective of testing a business continuity plan is to:
- Familiarize employees with the business continuity plan.
- Ensure that all residual risks are addressed.
- Exercise all possible disaster scenarios.
- Identify limitations of the business continuity plan.

**Correct Answer**: D
**Topic**: Business Continuity Plan Testing
**Explanation**: The main goal of testing a BCP is to identify its limitations, ensuring that any flaws or gaps are discovered and addressed.

---

**QUESTION 1203**
In determining the acceptable time period for the resumption of critical business processes:
- Only downtime costs need to be considered.
- Recovery operations should be analyzed.
- Both downtime costs and recovery costs need to be evaluated.
- Indirect downtime costs should be ignored.

**Correct Answer**: C
**Topic**: Business Impact Analysis and Recovery Time
**Explanation**: Both downtime and recovery costs must be evaluated to determine a reasonable recovery time for critical business processes. Indirect costs, like reputational damage, should also be factored into the assessment.

---

**QUESTION 1204**
In the event of a disruption or disaster, which of the following technologies provides for continuous operations?
- Load balancing
- Fault-tolerant hardware
- Distributed backups
- High-availability computing

**Correct Answer**: B
**Topic**: Fault-Tolerant Technology for Continuity
**Explanation**: Fault-tolerant hardware is specifically designed to ensure continuous operation without interruption, even in the case of component failures.

---

**QUESTION 1205**
Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?
- Data backups are performed on a timely basis
- A recovery site is contracted for and available as needed
- Human safety procedures are in place

- Insurance coverage is adequate and premiums are current

**Correct Answer**: C
**Topic**: Human Safety in Business Continuity Planning
**Explanation**: The protection of human life is the most critical element in any business continuity plan, making human safety procedures the top priority during an audit.

---

**QUESTION 1206**
Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

- Business interruption
- Fidelity coverage
- Errors and omissions
- Extra expense

**Correct Answer**: B
**Topic**: Insurance for Employee Fraud
**Explanation**: Fidelity insurance specifically covers losses resulting from fraudulent or dishonest acts committed by employees.

---

**QUESTION 1207**
The BEST method for assessing the effectiveness of a business continuity plan is to review the:

- Plans and compare them to appropriate standards.
- Results from previous tests.
- Emergency procedures and employee training.
- Offsite storage and environmental controls.

**Correct Answer**: B
**Topic**: Business Continuity Plan Evaluation
**Explanation**: Reviewing the results of previous tests provides the best evidence of the plan's effectiveness in real disaster recovery situations.

---

**QUESTION 1208**
With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

- Clarity and simplicity of the business continuity plans.
- Adequacy of the business continuity plans.
- Effectiveness of the business continuity plans.
- Ability of IS and end-user personnel to respond effectively in emergencies.

**Correct Answer**: A
**Topic**: Stakeholder Understanding in BCPs
**Explanation**: The IS auditor's goal is to ensure that all stakeholders understand their roles in the event of a disaster, which reflects the clarity and simplicity of the business continuity plan.

---

**QUESTION 1209**
During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

- Responsibility for maintaining the business continuity plan.
- Criteria for selecting a recovery site provider.
- **Recovery strategy.**
- Responsibilities of key personnel.

**Correct Answer: C**
**Topic: Business Continuity Planning**
**Explanation:**
The most appropriate strategy is selected based on the relative risk level and criticality identified in the

business impact analysis (BIA). The other choices are made after the selection or design of the appropriate recovery strategy.

---

**QUESTION 1210**
During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:

- Assessment of the situation may be delayed.
- **Execution of the disaster recovery plan could be impacted.**
- Notification of the teams might not occur.
- Potential crisis recognition might be ineffective.

**Correct Answer: B**
**Topic: Crisis Management**
**Explanation:**
Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C, and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster.

---

**QUESTION 1211**
An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?

- Review and evaluate the business continuity plan for adequacy.
- Perform a full simulation of the business continuity plan.
- Train and educate employees regarding the business continuity plan.
- Notify critical contacts in the business continuity plan.

**Correct Answer: A**
**Topic: Risk Assessment and BCP Evaluation**
**Explanation:**
The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization.

---

**QUESTION 1212**
Integrating business continuity planning (BCP) into an IT project aids in:

- The retrofitting of the business continuity requirements.
- **The development of a more comprehensive set of requirements.**
- The development of a transaction flowchart.
- Ensuring the application meets the user's needs.

**Correct Answer: B**
**Topic: IT Project Management and BCP Integration**
**Explanation:**
Integrating business continuity planning (BCP) into the development process ensures complete coverage of the requirements through each phase of the project. Retrofitting of the business continuity plan's requirements occurs when BCP is not integrating into the development methodology.

---

**QUESTION 1213**
The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

- Duration of the outage.
- **Type of outage.**
- Probability of the outage.
- Cause of the outage.

**Correct Answer: A**
**Topic: BCP Activation Criteria**

**Explanation:**
The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.

---

**QUESTION 1214**
An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

- Alignment of the BCP with industry best practices.
- **Results of business continuity tests performed by IS and end-user personnel.**
- Off-site facility, its contents, security, and environmental controls.
- Annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

**Correct Answer: B**
**Topic: BCP Effectiveness Testing**
**Explanation:**
The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives.

---

**QUESTION 1215**
To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) in order to determine:

- The business processes that generate the most financial value for the organization and therefore must be recovered first.
- The priorities and order for recovery to ensure alignment with the organization's business strategy.
- **The business processes that must be recovered following a disaster to ensure the organization's survival.**
- The priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

**Correct Answer: C**
**Topic: Business Impact Analysis (BIA)**
**Explanation:**
To ensure the organization's survival following a disaster, it is important to recover the most critical business processes first. The BIA helps prioritize recovery based on critical business functions.

---

**QUESTION 1216**
A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

- The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
- The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
- **The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.**
- The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

**Correct Answer: B**
**Topic: Business Continuity Plan Evaluation**
**Explanation:**
It is a common mistake to use scenario planning for business continuity. Planning for just selected scenarios denies the fact that even improbable events can cause an organization to break down.

**QUESTION 1217**
A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

- Full-scale test with relocation of all departments, including IT, to the contingency site.
- Walk-through test of a series of predefined scenarios with all critical personnel involved.
- IT disaster recovery test with business departments involved in testing the critical applications.
- **Functional test of a scenario with limited IT involvement.**

**Correct Answer: D**
**Topic: BCP Testing Strategy**
**Explanation:**
After a tabletop exercise, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery.

---

**QUESTION 1218**
Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

- **It improves security at a cost in functionality.**
- It improves functionality at a cost in security.
- It improves security at a cost in system performance.
- It improves performance at a cost in functionality.

**Correct Answer: A**
**Topic: Security Principles**
**Explanation:**
"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality."

**QUESTION 1219**
Which of the following is the MOST important reason for conducting periodic reviews of business continuity plans?

- To verify that business continuity arrangements are still in line with business goals.
- **To ensure that the plan is updated to reflect changes in the organization.**
- To ensure that recovery time objectives (RTOs) meet industry standards.
- To ensure that a detailed disaster recovery test is scheduled.

**Correct Answer: B**
**Topic: Business Continuity Plan Review**
**Explanation:**
A periodic review is essential to make sure the business continuity plan reflects any changes in business processes, technologies, or organizational structure. This ensures that the plan is current and effective.

---

**QUESTION 1220**
Which of the following would MOST likely be included in a business continuity plan's recovery strategies?

- The identification of critical applications and business functions.
- **The type and number of alternate facilities for recovery.**
- The cost of procuring backup software for recovery.
- The selection of personnel for disaster recovery.

**Correct Answer: B**
**Topic: Recovery Strategies**
**Explanation:**
Recovery strategies typically include planning for alternative work locations, IT resources, and other physical and personnel needs to ensure business continuity in the event of an emergency.

---

**QUESTION 1221**
In the event of a data breach, the IS auditor's FIRST priority should be to:
- Notify law enforcement authorities.
- Ensure that the breach is contained and the source is identified.
- **Assess the magnitude of the breach and its impact.**
- Contact the affected customers.

**Correct Answer: C**
**Topic: Incident Management and Response**
**Explanation:**
The primary objective is to understand the scope and impact of the breach to determine the necessary response. Containment and identification of the source should follow as part of the response strategy.

---

**QUESTION 1222**
Which of the following is the BEST way to ensure that a business continuity plan (BCP) is effective?
- Regularly test and update the BCP to reflect changes in the business environment.
- Assign responsibility for testing the BCP to the IT department.
- **Involve all departments in the BCP testing process.**
- Assign recovery objectives and criticality ratings to all departments.

**Correct Answer: C**
**Topic: BCP Effectiveness**
**Explanation:**
Involving all departments in the testing process ensures that the business continuity plan covers all aspects of the organization and that all areas are prepared for a real recovery scenario.

---

**QUESTION 1223**
A financial institution has a business continuity plan (BCP) that outlines the recovery of critical business functions and systems. The NEXT step in ensuring the recovery process is complete would be to:
- Test and validate the recovery procedures through simulations.
- Review the BCP to identify potential gaps in the recovery process.
- **Conduct a full-scale disaster recovery test.**
- Notify all stakeholders of the recovery procedures.

**Correct Answer: C**
**Topic: BCP Testing and Validation**
**Explanation:**
A full-scale disaster recovery test helps verify whether the entire recovery process can be executed successfully under real-world conditions, ensuring that all functions are properly restored.

---

**QUESTION 1224**
Which of the following is the MOST critical step in developing an effective business continuity plan (BCP)?
- Identifying the maximum acceptable downtime (MAD).
- **Conducting a business impact analysis (BIA).**
- Assigning disaster recovery responsibilities to staff.
- Reviewing IT security measures.

**Correct Answer: B**
**Topic: Business Impact Analysis**
**Explanation:**
The Business Impact Analysis (BIA) is the foundational step in BCP because it helps identify the most critical business functions and their dependencies, forming the basis for the continuity plan.

---

**QUESTION 1225**
Which of the following is the PRIMARY concern when selecting a backup site for disaster recovery?
- **The proximity of the site to the organization's primary location.**
- The cost of the site.

- The number of staff available at the site.
- The type of disaster the site is designed to recover from.

**Correct Answer: A**
**Topic: Disaster Recovery Site Selection**
**Explanation:**
Proximity is crucial because the site needs to be close enough to minimize downtime and distance-related challenges during recovery. However, it should still be far enough to avoid the same impact from regional disasters.

---

**QUESTION 1226**
Which of the following is MOST important when conducting a business continuity plan (BCP) tabletop exercise?

- **Ensuring all departments participate in the exercise.**
- Ensuring that IT systems are tested under real-world conditions.
- Reviewing the technical aspects of the disaster recovery plan.
- Evaluating the cost of disaster recovery procedures.

**Correct Answer: A**
**Topic: BCP Tabletop Exercise**
**Explanation:**
The success of a tabletop exercise depends on the involvement of all relevant departments. It helps ensure that the entire organization is prepared for recovery, not just the IT department.

---

**QUESTION 1227**
Which of the following actions is MOST effective in preventing unauthorized access to critical systems in an organization?

- **Implementing multi-factor authentication.**
- Restricting user access to read-only mode.
- Assigning different levels of access based on job roles.
- Enforcing frequent password changes.

**Correct Answer: A**
**Topic: Access Control and Security Measures**
**Explanation:**
Multi-factor authentication (MFA) is one of the most effective methods for preventing unauthorized access by requiring multiple forms of identification.

---

**QUESTION 1228**
Which of the following strategies is MOST effective for ensuring that an organization's critical data is protected from a ransomware attack?

- Encrypting all sensitive data at rest and in transit.
- Using backup systems to store data off-site.
- **Implementing strong access controls and segmenting networks.**
- Regularly updating antivirus software.

**Correct Answer: C**
**Topic: Data Protection and Ransomware Prevention**
**Explanation:**
Strong access controls and network segmentation help limit the attack surface and prevent ransomware from spreading across critical systems. Backups and encryption are also important, but segmentation provides an additional layer of security.

---

**QUESTION 1229**
Which of the following would MOST likely indicate the need to review an organization's business continuity plan (BCP)?

- The organization changes its IT systems.

- The organization experiences high turnover in IT staff.
- The organization moves to a new office location.
- **The organization undergoes a significant merger or acquisition.**

**Correct Answer: D**
**Topic: BCP Review Triggers**
**Explanation:**
A merger or acquisition often leads to changes in organizational structure, processes, and priorities, making it essential to review and potentially update the business continuity plan to ensure that it aligns with the new organization.

---

**QUESTION 1230**
TEMPEST is hardware for which of the following purposes?
- A) Eavesdropping
- B) Social engineering
- C) Virus scanning
- D) Firewalling
- E) None of the choices

**Correct Answer: A**
**Topic:** TEMPEST and Eavesdropping
**Explanation:**
TEMPEST refers to the monitoring of electromagnetic emissions from hardware to intercept data, even in closed systems. It is commonly associated with **eavesdropping** on data transmitted by electronic devices.

---

**QUESTION 1231**
Human error is being HEAVILY relied upon by which of the following types of attack?
- A) Eavesdropping
- B) DoS
- C) DDoS
- D) ATP
- E) Social Engineering
- F) None of the choices

**Correct Answer: E**
**Topic:** Social Engineering Attacks
**Explanation:**
**Social engineering** attacks exploit human errors, such as deception or manipulation, to gain access to systems or sensitive information.

---

**QUESTION 1232**
Zombie computers are being HEAVILY relied upon by which of the following types of attack?
- A) Eavesdropping
- B) DoS
- C) DDoS
- D) ATP
- E) Social Engineering
- F) None of the choices

**Correct Answer: C**
**Topic:** DDoS and Zombie Computers
**Explanation:**
In **Distributed Denial of Service (DDoS)** attacks, a large number of compromised "zombie" computers are used to flood a target system with requests, overwhelming it and causing service disruption.

---

**QUESTION 1233**
Attack amplifier is often being HEAVILY relied upon by which of the following types of attack?

- A) Packet dropping
- B) ToS
- C) DDoS
- D) ATP
- E) Wiretapping
- F) None of the choices

**Correct Answer: C**
**Topic:** DDoS and Attack Amplifiers
**Explanation:**
In **DDoS** attacks, an **attack amplifier** exploits third-party systems with poorly designed protocols to amplify the attack, resulting in a flood of traffic directed at the target.

---

**QUESTION 1234**
Back Orifice is an example of:

- A) A virus
- B) A legitimate remote control software
- C) A backdoor that takes the form of an installed program
- D) An eavesdropper
- E) None of the choices

**Correct Answer: C**
**Topic:** Backdoors and Remote Access
**Explanation:**
**Back Orifice** is a type of **backdoor** that can be installed on a system to allow unauthorized remote access. It can also be used to monitor activities and compromise security.

---

**QUESTION 1235**
Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs?

- A) Rootkits
- B) Virus
- C) Trojan
- D) Tripwire
- E) None of the choices

**Correct Answer: A**
**Topic:** Rootkits and System Integrity
**Explanation:**
**Rootkits** are malicious programs designed to modify system binaries or hook into OS functions to hide the presence of other malicious software, making detection more difficult.

---

**QUESTION 1235**
Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

- A) Direct access attacks
- B) Indirect access attacks
- C) Port attack
- D) Window attack
- E) Social attack
- F) None of the choices

**Correct Answer: A**
**Topic:** Direct Access Attacks
**Explanation:**

**Direct access attacks** involve using consumer devices, such as USB drives or portable media, to secretly transfer data or install malicious software on the target system.

---

**QUESTION 1236**
Which of the following types of attack almost always requires physical access to the targets?

- A) Direct access attack
- B) Wireless attack
- C) Port attack
- D) Window attack
- E) System attack
- F) None of the choices

**Correct Answer: A**
**Topic:** Physical Access and Direct Access Attacks
**Explanation:**
**Direct access attacks** require physical access to the target system in order to install malicious software, modify settings, or extract data.

---

**QUESTION 1237**
Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

- A) Key pair
- B) Oakley
- C) Certificate
- D) 3-DES
- E) One-time pad
- F) None of the choices

**Correct Answer: E**
**Topic:** One-time Pad Encryption
**Explanation:**
The **one-time pad** is a theoretically unbreakable encryption method when used correctly, relying on a key that is as long as the message itself and used only once.

---

**QUESTION 1238**
Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

- A) Blowfish
- B) Tripwire
- C) Certificate
- D) DES
- E) One-time pad
- F) None of the choices

**Correct Answer: E**
**Topic:** One-time Pad and Cryptography
**Explanation:**
The **one-time pad** encryption method uses a unique pair of key-codes, securely distributed and used only once to encrypt and decrypt a message, ensuring perfect secrecy when properly applied.

---

**QUESTION 1239**
Why is one-time pad not always preferable for encryption (choose all that apply):

- A) It is difficult to use securely.
- B) It is highly inconvenient to use.
- C) It requires licensing fee.
- D) It requires internet connectivity.

- E) It is Microsoft only.
- F) None of the choices

**Correct Answer: A, B**
**Topic:** One-time Pad Encryption Limitations
**Explanation:**
While the **one-time pad** is unbreakable when used correctly, it is often impractical due to the difficulty of securely distributing and managing the key, and it is highly inconvenient for everyday use.

---

**QUESTION 1240**
You may reduce a cracker's chances of success by (choose all that apply):
- A) Keeping your systems up to date using a security scanner.
- B) Hiring competent people responsible for security to scan and update your systems.
- C) Using multiple firewalls.
- D) Using multiple firewalls and IDS.
- E) None of the choices

**Correct Answer: A, B**
**Topic:** Reducing Cracker's Success
**Explanation:**
You can reduce the chances of a successful attack by **keeping systems up-to-date** with security patches and using **competent personnel** to manage security systems and audits.

---

**QUESTION 1241**
Which of the following measures can protect systems files and data, respectively?
- A) User account access controls and cryptography
- B) User account access controls and firewall
- C) User account access controls and IPS
- D) IDS and cryptography
- E) Firewall and cryptography
- F) None of the choices

**Correct Answer: A**
**Topic:** Protecting System Files and Data
**Explanation:**
**User account access controls** protect system files by managing who can access them, while **cryptography** can protect the data from unauthorized access or tampering.

---

**QUESTION 1242**
Which of the following is by far the most common prevention system from a network security perspective?
- A) Firewall
- B) IDS
- C) IPS
- D) Hardened OS
- E) Tripwire
- F) None of the choices

**Correct Answer: A**
**Topic:** Network Security Prevention
**Explanation:**
The **firewall** is the most common network security prevention system, blocking unauthorized access and monitoring traffic based on predefined security rules.

---

**QUESTION 1243**
Which of the following are designed to detect network attacks in progress and assist in post-attack forensics?

- A) Intrusion Detection Systems
- B) Audit trails
- C) System logs
- D) Tripwire
- E) None of the choices

**Correct Answer: A**
**Topic:** Intrusion Detection Systems (IDS)
**Explanation:**
**Intrusion Detection Systems (IDS)** detect network attacks as they occur and help with post-attack forensic analysis to understand the attack's origin and impact.

---

**QUESTION 1244**
"Nowadays, computer security comprises mainly "preventive" measures."

- A) True
- B) True only for trusted networks
- C) True only for untrusted networks
- D) False
- E) None of the choices

**Correct Answer: A**
**Topic:** Preventive Measures in Computer Security
**Explanation:**
Modern computer security primarily involves **preventive measures** like firewalls, which help protect systems before an attack occurs.

---

**QUESTION 1245**
The majority of software vulnerabilities result from a few known kinds of coding defects, such as (choose all that apply):

- A) Buffer overflows
- B) Format string vulnerabilities
- C) Integer overflow
- D) Code injection
- E) Command injection
- F) None of the choices

**Correct Answer: A, B, C, D, E**
**Topic:** Common Software Vulnerabilities
**Explanation:**
Most software vulnerabilities stem from coding defects like **buffer overflows**, **format string vulnerabilities**, **integer overflows**, and **code/command injection**, which can be exploited by attackers.

---

**QUESTION 1246**
ALL computer programming languages are vulnerable to command injection attack.

- A) True
- B) False

**Correct Answer: B**
**Topic:** Command Injection Vulnerability
**Explanation:**
Not all programming languages are susceptible to **command injection**. For example, languages like **Java** mitigate certain vulnerabilities but are still vulnerable to code and command injection in specific cases.

---

**QUESTION 1247**
Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

- A) Buffer overflow
- B) Format string vulnerabilities
- C) Integer misappropriation
- D) Code injection
- E) None of the choices

**Correct Answer: A**
**Topic:** Buffer Overflow Vulnerabilities
**Explanation:**
A **buffer overflow** occurs when a process attempts to write more data to a fixed-length buffer than it can hold, potentially overwriting adjacent memory and causing system crashes or vulnerabilities.

---

**QUESTION 1248**
Buffer overflow aims primarily at corrupting:

- A) System processor
- B) Network firewall
- C) System memory
- D) Disk storage
- E) None of the choices

**Correct Answer: C**
**Topic:** Buffer Overflow Impact
**Explanation:**
**Buffer overflow** attacks primarily target **system memory**, where the overflow can overwrite critical data and lead to program malfunctions or security breaches.

---

**QUESTION 1249**
Which of the following measures can effectively minimize the possibility of buffer overflows?

- A) Sufficient bounds checking
- B) Sufficient memory
- C) Sufficient processing capability
- D) Sufficient code injection
- E) None of the choices

**Correct Answer: A**
**Topic:** Preventing Buffer Overflows
**Explanation:**
Performing **sufficient bounds checking** ensures that data written to a buffer does not exceed its allocated size, helping to prevent **buffer overflow** vulnerabilities.

---

**QUESTION 1250**
Which of the following types of attack makes use of unfiltered user input as the format string parameter in the printf() function of the C language?

- A) Buffer overflows
- B) Format string vulnerabilities
- C) Integer overflow
- D) Code injection
- E) Command injection
- F) None of the choices

**Correct Answer: B**
**Topic:** Format String Vulnerabilities
**Explanation:**
**Format string vulnerabilities** arise when unfiltered user input is used as the format string parameter

in functions like printf(). Malicious input can exploit this vulnerability to print data from memory or execute arbitrary code.

---

**QUESTION 1251**
Which of the following kinds of function are particularly vulnerable to format string attacks?

- A) C functions that perform output formatting
- B) C functions that perform integer computation
- C) C functions that perform real number subtraction
- D) VB functions that perform integer conversion
- E) SQL functions that perform string conversion
- F) SQL functions that perform text conversion

**Correct Answer: A**
**Topic:** Functions Vulnerable to Format String Attacks
**Explanation:**
**C functions that perform output formatting**, like printf(), are particularly vulnerable to **format string attacks**, as these functions handle user-provided data in ways that can be exploited.

---

**QUESTION 1252**
Integer overflow occurs primarily with:

- A) String formatting
- B) Debug operations
- C) Output formatting
- D) Input verifications
- E) Arithmetic operations
- F) None of the choices

**Correct Answer: E**
**Topic:** Integer Overflow
**Explanation:**
**Integer overflow** typically occurs during **arithmetic operations** when a value exceeds the maximum size that can be stored in a variable, leading to unexpected behavior or vulnerabilities.

---

**QUESTION 1253**
Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

- A) Format string vulnerabilities
- B) Integer overflow
- C) Code injection
- D) Command injection
- E) None of the choices

**Correct Answer: C**
**Topic:** Code Injection
**Explanation:**
**Code injection** takes advantage of **unchecked assumptions** the system makes about its inputs. Attackers can inject malicious code into a program's input fields to execute arbitrary commands.

---

**QUESTION 1254**
Which of the following terms refers to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders?

- A) ILD&P
- B) ICT&P
- C) ILP&C
- D) ILR&D
- E) None of the choices

**Correct Answer: A**
**Topic:** Information Leakage Detection and Prevention (ILD&P)
**Explanation:**
**ILD&P (Information Leakage Detection and Prevention)** systems are designed to detect and prevent unauthorized transmission of sensitive information from an organization's systems to outsiders, ensuring data security.

---

**QUESTION 1255**
Network ILD&P are typically installed:

- A) On the organization's internal network connection.
- B) On the organization's internet network connection.
- C) On each end-user station.
- D) On the firewall.
- E) None of the choices

**Correct Answer: B**
**Topic:** Network ILD&P Installation
**Explanation:**
**Network ILD&P systems** are typically installed on the organization's **internet network connection**. These systems analyze traffic to detect unauthorized information transmissions.

---

**QUESTION 1256**
Host Based ILD&P primarily addresses the issue of:

- A) Information integrity
- B) Information accuracy
- C) Information validity
- D) Information leakage
- E) None of the choices

**Correct Answer: D**
**Topic:** Host-Based ILD&P
**Explanation:**
**Host-Based ILD&P** systems are focused on preventing **information leakage** by monitoring and controlling access to data before it leaves the organization.

---

**QUESTION 1257**
Software is considered malware based on:

- A) The intent of the creator
- B) Its particular features
- C) Its location
- D) Its compatibility
- E) None of the choices

**Correct Answer: A**
**Topic:** Malware Definition
**Explanation:**
**Malware** is defined by the **intent** of the creator, not by the software's features. Its goal is to damage, infiltrate, or gain unauthorized access to systems, typically without the owner's consent.

---

**QUESTION 1258**
Which of the following are valid examples of Malware (choose all that apply):

- A) Viruses
- B) Worms
- C) Trojan horses
- D) Spyware
- E) All of the above

**Correct Answer: E**
**Topic:** Examples of Malware
**Explanation:**
**Viruses**, **worms**, **trojan horses**, and **spyware** are all examples of **malware**, which is software designed to perform malicious actions on a computer system.

---

**QUESTION 1259**
Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

- A) Virus
- B) Worm
- C) Trojan horse
- D) Spyware
- E) Rootkits
- F) None of the choices

**Correct Answer: C**
**Topic:** Trojan Horse
**Explanation:**
A **Trojan horse** is a program that appears to be legitimate or harmless but secretly contains malicious code designed to damage, steal information, or otherwise harm the system when executed.

---

**QUESTION 1260**
Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to immediate yet undesirable effects, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals.
True or False?
**Correct Answer: B (False)**
**Topic:** Trojan Horse Payload
**Explanation:**
While **Trojan horses** conceal harmful payloads, the payload doesn't always take immediate effect. Often, it installs further malicious software or opens backdoors to serve longer-term malicious goals.

---

**QUESTION 1261**
Which of the following terms is used more generally for describing concealment routines in a malicious program?

- A) Virus
- B) Worm
- C) Trojan horse
- D) Spyware
- E) Rootkits
- F) Backdoor
- G) None of the choices

**Correct Answer: E**
**Topic:** Rootkits
**Explanation:**
**Rootkits** are specialized malicious software tools designed to conceal the presence of harmful processes or files. They often prevent detection by system monitoring tools.

---

**QUESTION 1262**
Which of the following refers to a method of bypassing normal system authentication procedures?

- A) Virus
- B) Worm

- C) Trojan horse
- D) Spyware
- E) Rootkits
- F) Backdoor
- G) None of the choices

**Correct Answer: F**
**Topic:** Backdoor
**Explanation:**
A **backdoor** is a method for bypassing normal authentication procedures, often used by hackers to maintain remote access to a compromised system.

---

**QUESTION 1263**
To install backdoors, hackers generally prefer to use:
- A) Either Trojan horse or computer worm
- B) Either Tripwire or computer virus
- C) Either eavesdropper or computer worm
- D) Either Trojan horse or eavesdropper
- E) None of the choices

**Correct Answer: A**
**Topic:** Installing Backdoors
**Explanation:**
Hackers typically use **Trojan horses** or **computer worms** to install backdoors, which allow them to maintain access to a compromised system.

---

**QUESTION 1264**
In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:
- A) Wormnets
- B) Trojannets
- C) Spynets
- D) Botnets
- E) Rootnets
- F) Backdoor

**Correct Answer: D**
**Topic:** Botnets
**Explanation:**
**Botnets** are networks of infected computers (often called "zombies") controlled by attackers to perform coordinated actions like launching attacks or sending spam.

---

**QUESTION 1265**
In a botnet, malbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?
- A) Chat system
- B) SMS system
- C) Email system
- D) Log system
- E) Kernel system
- F) None of the choices

**Correct Answer: A**
**Topic:** Botnet Communication
**Explanation:**
In a **botnet**, the **malbot** (malicious bot) logs into a **chat system** (such as an IRC channel) to receive instructions from the attacker for coordinated actions.

---

**QUESTION 1266**
Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

- A) System patcher
- B) Porn dialer
- C) War dialer
- D) T1 dialer
- E) T3 dialer
- F) None of the choices

**Correct Answer: B**
**Topic:** Dialer Software
**Explanation:**
A **porn dialer** is malicious software that takes control of a user's modem to dial a premium-rate telephone number, incurring high charges for the infected user.

---

**QUESTION 1267**
Which of the following is an oft-cited cause of vulnerability of networks?

- A) Software monoculture
- B) Software diversification
- C) Single line of defense
- D) Multiple DMZ
- E) None of the choices

**Correct Answer: A**
**Topic:** Network Vulnerability
**Explanation:**
**Software monoculture** refers to the reliance on a single software platform (like Windows), which makes systems vulnerable if that software is compromised. Attackers can exploit widespread software vulnerabilities, affecting large numbers of systems.

---

**QUESTION 1268**
Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

- A) Poorer performance
- B) Poor scalability
- C) Weak infrastructure
- D) High costs in terms of training and maintenance
- E) None of the choices

**Correct Answer: D**
**Topic:** Network Inhomogeneity Drawbacks
**Explanation:**
Introducing **inhomogeneity** (diversifying software or systems) increases **costs** due to the need for additional training and maintenance. While it may enhance security, it can also complicate management and increase operational overhead.

---

**QUESTION 1269**
Which of the following may be deployed in a network as lower-cost surveillance and early-warning tools?

- A) Honeypots
- B) Hardware IPSs
- C) Hardware IDSs
- D) Botnets
- E) Stateful inspection firewalls
- F) Stateful logging facilities

- G) None of the choices

**Correct Answer: A**
**Topic:** Honeypots
**Explanation:**
**Honeypots** are decoy systems or resources set up to attract attackers. These are used for surveillance and early-warning, as they allow network administrators to study attack techniques and identify threats in real time.

---

**QUESTION 1270**
All Social Engineering techniques are based on flaws in:
- A) Human logic
- B) Hardware logic
- C) Software logic
- D) Device logic
- E) Group logic
- F) None of the choices

**Correct Answer: A**
**Topic:** Social Engineering
**Explanation:**
Social engineering exploits flaws in **human logic** or cognitive biases. These flaws are manipulated to deceive individuals into revealing confidential information or performing actions that compromise security.

---

**QUESTION 1271**
Relatively speaking, firewalls operated at the application level of the seven-layer OSI model are:
- A) Almost always less efficient
- B) Almost always less effective
- C) Almost always less secure
- D) Almost always less costly to setup
- E) None of the choices

**Correct Answer: A**
**Topic:** Application Layer Firewalls
**Explanation:**
Firewalls that operate at the **application level** (Layer 7) are generally **less efficient** due to the heavy CPU processing required to analyze application data, compared to packet filtering firewalls that operate at lower layers.

---

**QUESTION 1272**
Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:
- A) Almost always less efficient
- B) Almost always less effective
- C) Almost always less secure
- D) Almost always less costly to setup
- E) None of the choices

**Correct Answer: E**
**Topic:** Physical Layer Firewalls
**Explanation:**
No firewalls operate at the **physical level** (Layer 1) of the OSI model, as firewalls typically function at higher layers such as Layer 3 (network layer) or Layer 7 (application layer).

---

**QUESTION 1273**
Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?
- A) Pretexting

- B) Backgrounding
- C) Check making
- D) Bounce checking
- E) None of the choices

**Correct Answer: A**
**Topic:** Pretexting
**Explanation:**
**Pretexting** involves creating a fabricated scenario to persuade someone into disclosing information or performing an action that benefits the attacker. It often involves research or using known information to build trust.

---

**QUESTION 1274**
Pretexting is an act of:

- A) DoS
- B) Social engineering
- C) Eavesdropping
- D) Soft coding
- E) Hard coding
- F) None of the choices

**Correct Answer: B**
**Topic:** Social Engineering
**Explanation:**
**Pretexting** is a form of **social engineering**, where attackers create a fabricated story or scenario to manipulate individuals into disclosing information or taking certain actions.

---

**QUESTION 1275**
With Deep Packet Inspection, which of the following OSI layers are involved?

- A) Layer 2 through Layer 7
- B) Layer 3 through Layer 7
- C) Layer 2 through Layer 6
- D) Layer 3 through Layer 6
- E) Layer 2 through Layer 5
- F) None of the choices

**Correct Answer: A**
**Topic:** Deep Packet Inspection
**Explanation:**
**Deep Packet Inspection (DPI)** examines the entire packet, including both the header and the data (payload), at layers **2 through 7** of the OSI model. This allows DPI to detect and filter packets based on more than just header information, such as protocols and content.

---

**QUESTION 1276**
Squid is an example of:

- A) IDS
- B) Caching proxy
- C) Security proxy
- D) Connection proxy
- E) Dialer
- F) None of the choices

**Correct Answer: B**
**Topic:** Squid Proxy
**Explanation:**
**Squid** is a **caching proxy** server that stores copies of frequently accessed web pages, reducing bandwidth usage and improving response time for users accessing the same content multiple times.

**QUESTION 1277**
Which of the following types of firewall treats each network frame or packet in isolation?

- A) Stateful firewall
- B) Hardware firewall
- C) Combination firewall
- D) Packet filtering firewall
- E) Stateless firewall
- F) None of the choices

**Correct Answer: E**
**Topic:** Stateless Firewall
**Explanation:**
A **stateless firewall** examines each packet in isolation, without considering whether the packet is part of an ongoing session or connection, making it less aware of the context of traffic compared to stateful firewalls.

---

**QUESTION 1278**
Which of the following types of attack involves a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files?

- A) Local DoS attacks
- B) Remote DoS attacks
- C) Distributed DoS attacks
- D) Local Virus attacks
- E) None of the choices

**Correct Answer: A**
**Topic:** Local DoS Attacks
**Explanation:**
A **Local DoS (Denial of Service)** attack involves a program that creates an infinite loop, making many copies of itself and consuming system resources (like memory or CPU), which may lead to system unresponsiveness or crashes.

---

**QUESTION 1279**
What is the best defense against Local DoS attacks?

- A) Patch your systems
- B) Run a virus checker
- C) Run anti-spy software
- D) Find this program and kill it
- E) None of the choices

**Correct Answer: D**
**Topic:** Local DoS Defense
**Explanation:**
In a **Local DoS attack**, a program creates an infinite loop or makes excessive copies of itself, consuming system resources. The best defense is to identify and **kill** the malicious program causing the DoS attack.

---

**QUESTION 1280**
Which of the following are examples of tools for launching Distributed DoS Attack (choose all that apply):

- A) TFN
- B) TFN2K
- C) Trin00
- D) Stacheldracht
- E) Tripwire

**Correct Answer: A, B, C, D**
**Topic:** Distributed DoS Attack Tools
**Explanation:**
Tools like **TFN**, **TFN2K**, **Trin00**, and **Stacheldracht** are used for conducting **Distributed Denial of Service (DDoS)** attacks, where multiple machines are used to flood a target system with traffic. **Tripwire** is not a DDoS tool; it is a security monitoring tool.

---

**QUESTION 1281**
What is the best defense against Distributed DoS Attack?

- A) Patch your systems
- B) Run a virus checker
- C) Run anti-spy software
- D) Find the DoS program and kill it
- E) None of the choices

**Correct Answer: A**
**Topic:** DDoS Attack Defense
**Explanation:**
For defending against **Distributed DoS (DDoS)** attacks, the best defense is to **patch your systems** and ensure your firewalls are correctly configured to filter malicious traffic.

---

**QUESTION 1282**
What is wrong with a Black Box type of intrusion detection system?

- A) You cannot patch it
- B) You cannot test it
- C) You cannot examine its internal workings from outside
- D) You cannot tune it
- E) None of the choices

**Correct Answer: C**
**Topic:** Black Box IDS
**Explanation:**
A **Black Box** Intrusion Detection System (IDS) is one where its internal workings are not visible to the user. This lack of transparency means it is difficult to **examine** or **modify** its internal processes, which can hinder troubleshooting and optimization.

---

**QUESTION 1283**
Which of the following are often considered as the first defensive line in protecting a typical data and information environment?

- A) Certificates
- B) Security token
- C) Password
- D) Biometrics
- E) None of the choices

**Correct Answer: C**
**Topic:** First Line of Defense
**Explanation:**
**Passwords** are the first line of defense for protecting data and information. They are used by users to authenticate their identity before accessing systems and resources.

---

**QUESTION 1284**
Which of the following are the characteristics of a good password?

- A) It has mixed-case alphabetic characters, numbers, and symbols
- B) It has mixed-case alphabetic characters and numbers
- C) It has mixed-case alphabetic characters and symbols

- D) It has mixed-case alphabetic characters, numbers, and binary codes
- E) None of the choices

**Correct Answer: A**
**Topic:** Good Password Characteristics
**Explanation:**
A good password should include **mixed-case alphabetic characters**, **numbers**, and **symbols**. This increases complexity and makes the password harder to guess or crack.

---

**QUESTION 1285**
What is the recommended minimum length of a good password?

- A) 6 characters
- B) 8 characters
- C) 12 characters
- D) 18 characters
- E) 22 characters
- F) None of the choices

**Correct Answer: B**
**Topic:** Password Length
**Explanation:**
A good password should be at least **8 characters** long. Longer passwords are more secure as they are harder to guess or brute-force.

---

**QUESTION 1286**
Which of the following is a good tool to use to help enforce the deployment of good passwords?

- A) Password cracker
- B) Local DoS attacker
- C) Network hacker
- D) Remote windowing tool
- E) None of the choices

**Correct Answer: A**
**Topic:** Enforcing Good Passwords
**Explanation:**
A **password cracker** can be used to test the strength of passwords by attempting to crack them. This tool helps identify weak passwords and enforce the policy of using strong passwords.

---

**QUESTION 1287**
Which of the following is a good time frame for making changes to passwords?

- A) Every 180 to 365 days
- B) Every 30 to 45 days
- C) Every 10 to 20 days
- D) Every 90 to 120 days
- E) None of the choices

**Correct Answer: D**
**Topic:** Password Change Frequency
**Explanation:**
It is recommended to change passwords every **90 to 120 days** to reduce the risk of them being compromised over time.

---

**QUESTION 1288**
You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):

- A) 60 - 75 degrees Fahrenheit
- B) 10 - 25 degrees Celsius

- C) 30 - 45 degrees Fahrenheit
- D) 1 - 15 degrees Celsius
- E) 20 - 35 degrees Fahrenheit
- F) 0 - 5 degrees Celsius

**Correct Answer: A, B**
**Topic:** Computer Room Temperature
**Explanation:**
Computer rooms should be kept between **60 - 75 degrees Fahrenheit** (or **10 - 25 degrees Celsius**) to ensure proper functioning of equipment and to avoid overheating.

---

**QUESTION 1289**
You should keep all computer rooms at reasonable humidity levels, which are in between:

- A) 20 - 70 percent
- B) 10 - 70 percent
- C) 10 - 60 percent
- D) 70 - 90 percent
- E) 60 - 80 percent
- F) None of the choices

**Correct Answer: A**
**Topic:** Computer Room Humidity
**Explanation:**
Humidity levels in computer rooms should be kept between **20 - 70 percent** to avoid condensation or static buildup that could damage equipment.

---

**QUESTION 1290**
A virus typically consists of what major parts (choose all that apply):

- A) A mechanism that allows them to infect other files and reproduce
- B) A trigger that activates delivery of a "payload"
- C) A payload
- D) A signature
- E) None of the choices

**Correct Answer: A, B, C**
**Topic:** Virus Components
**Explanation:**
A virus typically consists of:

- A **mechanism** to infect other files and replicate,
- A **trigger** to activate the virus,
- A **payload** which is the malicious code that performs actions like corrupting files or stealing information.

---

**QUESTION 1291**
Within a virus, which component is responsible for what the virus does to the victim file?

- A) The payload
- B) The signature
- C) The trigger
- D) The premium
- E) None of the choices

**Correct Answer: A**
**Topic:** Virus Payload
**Explanation:**
The **payload** of a virus defines what happens to the victim file, such as deleting it, altering its contents, or stealing information.

---

**QUESTION 1292**
Which of the following can be thought of as the simplest and almost cheapest type of firewall?
- A) Stateful firewall
- B) Hardware firewall
- C) PIX firewall
- D) Packet filter
- E) None of the choices

**Correct Answer: D**
**Topic:** Simple Firewalls
**Explanation:**
A **packet filter** firewall is the simplest and most cost-effective type of firewall. It works by filtering packets based on predefined rules but does not inspect the contents of the packet.

---

**QUESTION 1293**
**Screening router inspects traffic through examining:**
A) Message header
B) Virus payload
C) Message content
D) Attachment type
E) None of the choices
**Correct Answer:** A
**Section:** Mixed Questions
**Explanation:**
A packet filter firewall is the simplest and cheapest type of firewall, typically using a screening router to inspect and filter traffic based on predefined rules, specifically examining the message header for network addresses.

---

**QUESTION 1294**
**A major portion of what is required to address nonrepudiation is accomplished through the use of:**
A) Strong methods for authentication and ensuring data validity
B) Strong methods for authentication and ensuring data integrity
C) Strong methods for authorization and ensuring data integrity
D) Strong methods for authentication and ensuring data reliability
E) None of the choices
**Correct Answer:** B
**Section:** Mixed Questions
**Explanation:**
Nonrepudiation is primarily achieved through strong authentication methods and ensuring data integrity, ensuring that both the sender and recipient can trust the authenticity of the information.

---

**QUESTION 1295**
**Why is it not preferable for a firewall to treat each network frame or packet in isolation?**
A) Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
B) Such a firewall is costly to set up.
C) Such a firewall is too complicated to maintain.
D) Such a firewall is CPU hungry.
E) Such a firewall offers poor compatibility.
**Correct Answer:** A
**Section:** Mixed Questions
**Explanation:**

Stateless firewalls process each packet independently, unable to track the context of an ongoing connection, which means they cannot discern legitimate traffic from malicious packets.

---

**QUESTION 1296**
**Phishing attack works primarily through:**
A) Email and hyperlinks
B) SMS
C) Chat
D) Email attachment
E) News
F) File download
G) None of the choices
**Correct Answer:** A
**Section:** Mixed Questions
**Explanation:**
Phishing attacks often occur through emails that appear legitimate, with embedded links directing the recipient to fraudulent websites designed to steal personal information.

---

**QUESTION 1297**
**Which of the following types of attack often take advantage of curiosity or greed to deliver malware?**
A) Gimmes
B) Tripwire
C) Icing
D) Soft coding
E) Pretexting
F) None of the choices
**Correct Answer:** A
**Section:** Mixed Questions
**Explanation:**
Gimmes, also known as Trojan Horses, exploit curiosity or greed, often using email attachments that promise something enticing, prompting users to open them and unknowingly infect their systems with malware.

---

**QUESTION 1298**
**Gimmes often work through:**
A) SMS
B) IRC chat
C) Email attachment
D) News
E) File download
F) None of the choices
**Correct Answer:** C
**Section:** Mixed Questions
**Explanation:**
Gimmes, or Trojan Horses, typically arrive as email attachments with enticing offers, tricking recipients into opening them and exposing their system to malware.

---

**QUESTION 1299**
**Talking about biometric authentication, physical characteristics typically include (choose all that apply):**
A) Fingerprints
B) Eye retinas

C) Irises
D) Facial patterns
E) Hand measurements
F) None of the choices
**Correct Answer:** A, B, C, D, E
**Section:** Mixed Questions
**Explanation:**
Biometric authentication involves physical characteristics like fingerprints, eye retinas, irises, facial patterns, and hand measurements, all of which are used for verification purposes.

---

**QUESTION 1300**
**Talking about biometric authentication, which of the following is often considered as a mix of both physical and behavioral characteristics?**
A) Voice
B) Finger measurement
C) Body measurement
D) Signature
E) None of the choices
**Correct Answer:** A
**Section:** Mixed Questions
**Explanation:**
Voice is considered a mix of both physical (sound of the voice) and behavioral (speech patterns) characteristics in biometric authentication.