QUESTION 160
Which of the following are included in Technical Controls? Each correct answer represents a complete solution. Choose all that apply.

A. Identification and authentication methods
B. Configuration of the infrastructure
C. Password and resource management
D. Implementing and maintaining access control mechanisms
E. Security devices
F. Conducting security-awareness training

Answer: ABCDE
Explanation:
Technical Controls are also known as Logical Controls. These controls include the following: Implementing and maintaining access control mechanisms Password and resource management Identification and authentication methods Security devices Configuration of the infrastructure Answer: F is incorrect. It is a part of Administrative Controls.

QUESTION 161
What are the various phases of the Software Assurance Acquisition process according to the U.S. Department of Defense (DoD) and Department of Homeland Security (DHS) Acquisition and Outsourcing Working Group?

A. Implementing, contracting, auditing, monitoring
B. Requirements, planning, monitoring, auditing
C. Planning, contracting, monitoring and acceptance, follow-on
D. Designing, implementing, contracting, monitoring

Answer: C
Explanation:
Software Assurance Acquisition process defines the level of confidence that software is free from vulnerabilities. It is designed into the software or accidentally inserted at anytime during its lifecycle, and the software works in a planned manner. According to the U.S. Department of Defense and Department of Homeland Security Acquisition and Outsourcing Working Group, the Software Assurance Acquisition process contains the following phases: 1.Planning 2.Contracting 3.Monitoring and acceptance 4.Follow-on

QUESTION 162
Companies use some special marks to distinguish their products from those of other companies. These marks can include words, letters, numbers, drawings, etc. Which of the following terms describes these special marks?

A. Business mark
B. Trademark
C. Sales mark
D. Product mark

Answer: B
Explanation:
A trademark is a mark that is used by a company to distinguish its products from those of other companies. There are various ways a company uses its trademark to distinguish its products from others. It can use words, letters, numbers, drawings, pictures, and so on, in its trademark.

Answer: D, A, and C are incorrect. There is no such mark as product mark, business mark, or sales mark.

QUESTION 163
Which of the following features of SIEM products is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems?

A. Security knowledge base
B. Graphical user interface
C. Asset information storage and correlation
D. Incident tracking and reporting

Answer: B
Explanation:
SIEM product has a graphical user interface (GUI) which is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. A graphical user interface (GUI) is a type of user interface that allows people to interact with programs in more ways than typing commands on computers. The term came into existence because the first interactive user interfaces to computers were not graphical; they were text- and-keyboard oriented and usually consisted of commands a user had to remember and computer responses that were infamously brief. A GUI offers graphical icons, and visual indicators, as opposed to text-based interfaces, typed command labels or text navigation to fully represent the information and actions available to a user. The actions are usually performed through direct manipulation of the graphical elements.

QUESTION 164
Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

A. Cryptographer
B. Cryptography
C. Kerberos
D. Cryptanalysis

Answer: D
Explanation:
Cryptanalysis is the process of analyzing cipher text and finding weaknesses in cryptographic algorithms. These weaknesses can be used to decipher the cipher text without knowing the secret key. Answer: C is incorrect. Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model, and provides secure communication between Windows 2000 Server domains and clients. Answer: A is incorrect. A cryptographer is a person who is involved in cryptography.

Answer: B is incorrect. Cryptography is a branch of computer science and mathematics. It is used for protecting information by encoding it into an unreadable format known as cipher text.

QUESTION 165
Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS?

A. DIAP

B. DTIC
C. DARPA
D. DISA

Answer: C
Explanation:
The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface. DARPA supplies technological options for the entire Department, and is designed to be the "technological engine" for transforming DoD. Answer: D is incorrect. The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands. DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. Answer: B is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today. DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public. DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other U.S. Government agency personnel and their contractors. Answer: A is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the armed forces throughout the day-to-day operations, and in the time of crisis. The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net- centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.

QUESTION 166
Which of the following are the scanning methods used in penetration testing? Each correct answer represents a complete solution. Choose all that apply.

A. Vulnerability
B. Port
C. Services
D. Network

Answer: ABD
Explanation:
The vulnerability, port, and network scanning tools are used in penetration testing. Vulnerability scanning is a process in which a Penetration Tester uses various tools to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular

targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses. Answer: C is incorrect. This option comes under vulnerability scanning.

QUESTION 167
Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.

A. Password policies
B. Data classification
C. Data encryption
D. Vulnerability assessments

Answer: ABD
Explanation:
The following methods can be helpful to eliminate social engineering threat: Password policies Vulnerability assessments Data classification Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments. These assessments usually consist of using known hacker tools and common hacker techniques to breach a network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

QUESTION 168
Digital rights management (DRM) consists of compliance and robustness rules. Which of the following features does the robustness rule have? Each correct answer represents a complete solution. Choose three.

A. It specifies the various levels of robustness that are needed for asset security.
B. It specifies minimum techniques for asset security.
C. It specifies the behaviors of the DRM implementation and applications accessing the implementation.
D. It contains assets, such as device key, content key, algorithm, and profiling data.

Answer: ABD
Explanation:
The DRM (digital rights management) technology includes the following rules: 1.Compliance rule:

This rule specifies the behaviors of the DRM implementation, and applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant 2.Robustness rule: This rule has the following features: It specifies the various levels of robustness that are needed for asset security. It contains assets, such as device key, content key, algorithm, and profiling data. It specifies minimum techniques for asset security.

QUESTION 169
Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?

A. Denial-of-service attack
B. Dictionary attack
C. Man-in-the-middle attack
D. Password guessing attack

Answer: C
Explanation:
When an attacker successfully inserts an intermediary software or program between two communicating hosts, it is known as man-in-the-middle attack.

QUESTION 170
Which of the following is an example of penetration testing?

A. Implementing NIDS on a network
B. Implementing HIDS on a computer
C. Simulating an actual attack on a network
D. Configuring firewall to block unauthorized traffic

Answer: C
Explanation:
Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration testing is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer: A, B, and D are incorrect. Implementing NIDS and HIDS and configuring firewall to block unauthorized traffic are not examples of penetration testing.

QUESTION 171
Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

A. Common data security architecture (CDSA)
B. Application program interface (API)