Vendor: CompTIA

Exam Code: CA1-001

Exam Name: CompTIA Advanced Security Practitioner (CASP) Beta Exam

Version: Demo

Topic 1, Volume A

QUESTION NO: 1

You need to ensure that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future?

A. Perfect forward secrecy
B. Secure socket layer
C. Secure shell
D. Security token

Answer: A
Explanation:
Perfect forward secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.

Forward secrecy has been used as a synonym for perfect forward secrecy, since the term perfect has been controversial in this context. However, at least one reference distinguishes perfect forward secrecy from forward secrecy with the additional property that an agreed key will not be compromised even if agreed keys derived from the same long-term keying material in a subsequent run are compromised.

Answer option C is incorrect. Secure Shell (SSH) is a program that is used for logging into a remote computer over a network. Secure Shell can be used to execute commands on a remote machine and to move files from one machine to another. SSH uses strong authentication and secure communications over insecure channels.

Answer option B is incorrect. Secure Sockets Layer (SSL) is a protocol that was developed by Netscape for transmitting private documents via the Internet. It uses a cryptographic system that uses public and private keys to encrypt data. A public key is globally available and a private key is known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support the SSL protocol. Several web sites use this protocol to obtain confidential user information. When the SSL protocol is used to connect to a Web site, the URL must begin with https instead of http.

Answer option D is incorrect. Security token can be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Security tokens are used to prove one's identity electronically (as in the case of a customer trying to access his bank account). The token is used in addition to or in place of a password to prove that the customer is who he claims to be. The token acts like an electronic key to access something.

QUESTION NO: 2

The Security Development Lifecycle (SDL) consists of various security practices that are grouped under seven phases. Which of the following security practices are included in the Requirements phase?

Each correct answer represents a complete solution. Choose all that apply.

A. Incident Response Plan
B. Create Quality Gates/Bug Bars
C. Attack Surface Analysis/Reduction
D. Security and Privacy Risk Assessment

Answer: B,D
Explanation:
The Requirements phase of the Security Development Lifecycle (SDL) includes the following security practices:
• Security and Privacy Requirements
• Create Quality Gates/Bug Bars
• Security and Privacy Risk Assessment

Answer option C is incorrect. Attack Surface Analysis/Reduction is a security practice included in the Design phase of the Security Development Lifecycle (SDL).

Answer option A is incorrect. Incident Response Plan is a security practice included in the Release phase of the Security Development Lifecycle (SDL).

QUESTION NO: 3

Which of the following components of a VoIP network is frequently used to bridge video conferencing connections?

A. MCU
B. Videoconference station
C. IP Phone
D. Call agent

Answer: A

Explanation:

A Multipoint Control Unit (MCU) is a device frequently used to bridge video conferencing connections. The Multipoint Control Unit is an endpoint on the LAN that provides the ability for 3 or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and optional Multipoint Processors (MPs).
Answer option C is incorrect. IP Phones provide IP endpoints for voice communication. Answer option D is incorrect. A call agent provides call control for IP phones, CAC, bandwidth control and management, and address translation. Unlike a gatekeeper, which in a Cisco environment typically runs on a router, a call agent typically runs on a server platform. Cisco Unified Communications Manager is an example of a call agent.

The call agent controls switching logic and calls for all the sites under the central controller. A central gateway controller includes both centralized configuration and maintenance of call control functionality, when new functionality needs to be added, only the controller needs to be updated.

Answer option B is incorrect. A videoconference station provides access for end-user involvement in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. A user can view video streams and hear audio that originates at a remote user station.

QUESTION NO: 4

Which of the following is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies?

A. SAML
B. SOAP
C. SPML
D. XACML

Answer: D

Explanation:

XACML stands for extensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.

Latest version 2.0 was ratified by OASIS standards organization on 1 February 2005. The planned version 3.0 will add generic attribute categories for the evaluation context and policy delegation

profile (administrative policy profile).

Answer option B is incorrect. SOAP, defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks, it relies on extensible Markup Language as its message format, and usually relies on other Application Layer protocols for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

Answer option C is incorrect. Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used to exchange user, resource and service provisioning information between cooperating organizations.

SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations.

SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations.

Answer option A is incorrect. Security Assertion Markup Language (SAMLJ is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION NO: 5

You work as a Network Administrator for uCertify Inc. You want to allow some users to access a particular program on the computers in the network. What will you do to accomplish this task?

A. Apply remote access policies
B. Apply NTFS permissions
C. Apply group policies
D. Apply account policies

Answer: C

Explanation:

In order to accomplish the task, you should apply group policy in the network.

A group policy that is created by an administrator affects all users on a computer or all users on a domain. Group policies can be used for defining, customizing, and controlling the functioning of network resources, computers, and operating systems. They can be set for a single computer with multiple users, for users in workgroups, or for computers in a domain. Administrators can configure group policy settings for users as well as for computers in many ways. Group policies can be used to allow or restrict the access of a particular program by a particular user. It can also be used to configure the desktop, the Start menu, the taskbar. the Control Panel, security settings, among other things. In Windows XP, group policies can be configured by using the Group Policy Console dialog box, which can be opened by running the GPEDIT.MSC command from the Start menu.

Answer option D is incorrect. An account policy controls the password expiration policy, the lockout policy, and other password features.

Answer option B is incorrect. NTFS permissions are attributes of the folder or file for which they are configured. These include both standard and special levels of settings. The standard settings are combinations of the special permissions which make the configuration more efficient and easier to establish.

Answer option A is incorrect. A remote access policy specifies how remote users can connect to the network and the requirements for each of their systems before they are allowed to connect. It defines the methods users can use to connect remotely such as dial up or VPN. This policy is used to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data.

QUESTION NO: 6

Which of the following is the most secure authentication scheme and uses a public key cryptography and digital certificate to authenticate a user?

A. Form-based authentication
B. Basic authentication
C. Digest authentication
D. Certificate-based authentication

Answer: D

Explanation:
Certificate-based authentication is the most secure authentication scheme. A certificate-based authentication scheme is a scheme that uses a public key cryptography and digital certificate to authenticate a user. A digital certificate is an electronic document that includes identification information, public key, and the digital signature of a certification authority based on that certification authority's private key. When a user connects to the server, he presents his digital certificate containing the public key and the signature of the certification authority. The server verifies the validity of the signature and whether the certificate has been provided by a trusted certificate authority or not. The server then authenticates the user by using public key cryptography to prove that the user truly holds the private key associated with the certificate.
Answer option B is incorrect. Basic authentication is a simple method of authentication that provides minimum security. It should be used only when security is not critical because basic authentication requests are not encrypted.
Answer option A is incorrect. Form-based authentication Form-based authentication allows users to create their own custom forms. It requires session tracking for the authentication, so that the container may use the login form. It is not a secure authentication scheme.
Answer option C is incorrect. Digest authentication is a secure authentication method in which passwords are sent across a network as a hash value rather than as clear text. It is a more secure authentication method as compared to Basic authentication. Digest authentication works across proxy servers and firewalls.

QUESTION NO: 7

Which of the following security practices are included in the Implementation phase of the Security Development Lifecycle (SDL)? Each correct answer represents a complete solution. Choose two.

A. Establish Design Requirements
B. Perform Static Analysis
C. Use Approved Tools
D. Execute Incident Response Plan

Answer: A,B,C
Explanation:
Security practices performed during each phase of the Security Development Lifecycle (SDL) process are as follows:

Phases	Security Practices
Training	• Core Security Training
Requirements	• Security and Privacy Requirements • Create Quality Gates/Bug Bars • Security and Privacy Risk Assessment
Design	• Establish Design Requirements • Attack Surface Analysis/Reduction • Threat Modeling
Implementation	• Use Approved Tools • Deprecate Unsafe Functions • Perform Static Analysis
Verification	• Perform Dynamic Analysis • Fuzz Testing • Attack Surface Review
Release	• Incident Response Plan • Final Security Review • Release/Archive
Response	• Execute Incident Response Plan

C:\Documents and Settings\user-nwz\Desktop\1.JPG

QUESTION NO: 8

In which of the following activities an organization identifies and prioritizes technical, organizational, procedural, administrative, and physical security weaknesses?

A. Social engineering

B. Vulnerability assessment
C. White box testing
D. Penetration testing

Answer: B

Explanation:

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed for include, but are not limited to, nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.

Vulnerability is the most reliable weakness that any programming code faces. These programming codes may be buffer overflow, xss, sql injection, etc. A piece of malware code that takes advantage of a newly announced vulnerability in a software application, usually the operating system or a Web server, is known as an exploit.

Answer option C is incorrect. White box is one of the three levels of penetration testing performed for an organization or network. This final level simulates an attacker with extensive knowledge of the organization and its infrastructure and security controls. The knowledge would come either from independent research and information gathering or from a trusted inside source with full knowledge of the network and its defenses.

Answer option A is incorrect. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name. IP address, employee ID, or other information that can be misused.

Answer option D is incorrect. A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known 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 test 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.

QUESTION NO: 9

SDLC phases include a minimum set of security tasks that are required to effectively incorporate security in the system development process. Which of the following are the key security activities for the development/acquisition phase?

Each correct answer represents a complete solution. Choose two.

A. Prepare initial documents for system certification and accreditation
B. Conduct the risk assessment and use the results to supplement the baseline security controls
C. Determination of privacy requirements
D. Initial delineation of business requirements in terms of confidentiality, integrity, and availability

Answer: A,B

Explanation:

Key security activities for the development/acquisition phase are as follows:

• Conduct the risk assessment and use the results to supplement the baseline security controls
• Analyze security requirements
• Perform functional and security testing
• Prepare initial documents for system certification and accreditation
• Design security architecture

Answer options D and C are incorrect. Key security activities for the initiation phase are as follows:

• Initial definition of business requirements in terms of confidentiality, integrity, and availability
• Determination of information categorization and identification of known special handling requirements in transmitting, storing, or creating information
• Determination of privacy requirements

QUESTION NO: 10

Which of the following is an XML-based framework developed by OASIS and used to exchange user, resource and service provisioning information between cooperating organizations?

A. SOAP
B. SAML
C. SPML
D. XACML

Answer: C

Explanation:

Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used to exchange user, resource and service provisioning information between cooperating organizations.

SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations.
Answer option A is incorrect. SOAP, defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on extensible Markup Language as its message format, and usually relies on other Application Layer protocols for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

Answer option D is incorrect. XACML stands for extensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.

Latest version 2.0 was ratified by OASIS standards organization on 1 February 2005. The planned version 3.0 will add generic attribute categories for the evaluation context and policy delegation profile (administrative policy profile).

Answer option B is incorrect. Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION NO: 11

Which of the following terms is about communicating the user's need and ability to communicate, and the medium through which that communication may occur?

A. Data sharing
B. Presence
C. Instant messaging
D. Audio conferencing

Answer: B

Explanation:
Presence, in the world of telephony, is about communicating the user's need and ability to communicate, and the medium through which that communication may occur. If a user is connected to the Internet, presence may dictate that the user wants to be reached through the medium of IP telephony. The point of presence is to allow the user to be located and contacted wherever the user is physically using the preferred method of the user.

Answer option A is incorrect. Data sharing is one important element of collaboration. H.323 also offers data sharing as an optional capability. Data sharing is the practice of making data used for scholarly research available to other investigators.

Answer option D is incorrect. Audio conferencing is a method of communication in which the calling party wishes to have more than one called party listens in to the audio portion of the call. The conference calls may be designed to allow the called party to participate during the call, or the call may be set up so that the called party merely listens into the call and cannot speak. It can be designed so that the calling party calls the other participants and adds them to the call.

Answer option C is incorrect. Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.

IM falls under the umbrella term online chat, as it is a real-time text-based networked communication system, but is distinct in that it is based on clients that facilitate connections between specified known users (often using Buddy List, Friend List or Contact List), whereas online chat also includes web-based applications that allow communication between users in a multi-user environment.

QUESTION NO: 12

Which technology can be used to help ensure the efficient transport of VoIP traffic?

A. DNS
B. QoS
C. H.323
D. RSTP

Answer: B

Explanation: Answer option B is correct.
Quality of Service (QoS) is a technology for prioritizing traffic on the network. VoIP requires optimization of bandwidth to ensure users do not experience "call drops" created by lack of bandwidth due to congestion issues. QoS is a mechanism to provide this optimization.

QUESTION NO: 13

In which of the following attacks does an attacker intercept call-signaling SIP message traffic and masquerade as the calling party to the called party and vice-versa?

A. Call tampering
B. Man-in-the-middle
C. Eavesdropping
D. Denial of Service

Answer: B
Explanation: VoIP is more vulnerable to man-in-the-middle attacks. In the man-in-the-middle attack, the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, and vice-versa. The attacker can hijack calls via a redirection server after gaining this position.

Answer option A is incorrect. Call tampering involves tampering a phone call in progress.
Answer option D is incorrect. DoS attacks occur by flooding a target with unnecessary SIP call-signaling messages. It degrades the service and causes calls to drop prematurely and halts call processing.

Answer option C is incorrect. In eavesdropping, hackers steal credentials and other information.

QUESTION NO: 14

Which of the following protocols is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features?

A. SIP
B. MGCP
C. H.323

D. RTP

Answer: D

Explanation:

Real-time Transport Protocol (RTP), developed by the Audio-Video Transport Working Group of the IETF and first published in 1996, defines a standardized packet format for delivering audio and video over the Internet. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features. For these, it carries media streams controlled by H.323, MGCP, Megaco, SCCP, or Session Initiation Protocol (SIP) signaling protocols, making it one of the technical foundations of the Voice over IP industry. RTP is usually used in conjunction with the RTP Control Protocol (RTCP). When both protocols are used in conjunction, RTP is usually originated and received on even port numbers, whereas RTCP uses the next higher odd port number. RTP and RTCP typically use unprivileged UDP ports (1024 to 65535).

Answer option C is incorrect. H.323 is a group of protocols defined by the International Telecommunication Union for multimedia conferences over Local Area Networks. The H.323 collection of protocols collectively may use up to two TCP connections and four to six UDP connections. H.323 inspection is used for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 application inspecti

Answer option A is incorrect. Session Initiation Protocol (SIP), designed by Henning Schulzrinne and Mark Handley in 1996, is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet (VoIP). Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games. The protocol can be used for creating, modifying, and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc. The SIP protocol is a TCP/IP-based Application Layer protocol. Within the OSI model, it is sometimes placed in the session layer. SIP is designed to be independent of the underlying transport layer; it can run on TCP, UDP, or SCTP. It is a text-based protocol, sharing many elements of the Hypertext Transfer Protocol (HTTP) upon which it is based, allowing for easy inspection by administrators. SIP clients typically use TCP or UDP (typically on port 5060 and/or 5061) to connect to SIP servers and other SIP endpoints.

Answer option B is incorrect. MGCP stands for Media Gateway Control Protocol. The Media Gateway Control Protocol is architecture for controlling media gateways on Internet Protocol (IP) networks and the public switched telephone network (PSTN). It is a master/slave protocol used to control media gateways from external call control elements called media gateway controllers or call agents. A network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet is called as media gateway. MGCP supports a large number of devices on an internal network with a limited set of external (global)

addresses using NAT and PAT.

QUESTION NO: 15

Collaboration platform offers a set of software components and services that enable users to communicate, share information, and work together for achieving common business goals. What are the core elements of a collaboration platform?

Each correct answer represents a part of the solution. Choose three.

A. Product and service integration
B. Real-time communication
C. Change management
D. Team collaboration
E. Messaging

Answer: B,D,E
Explanation: Collaboration platform is an unified electronic platform that supports both synchronous and asynchronous communication using a variety of devices and channels. It offers a set of software components and services. These components and services enable users to communicate, share information, and work together for achieving common business goals.

A collaboration platform consists of the following core elements:
• Messaging {email, calendaring and scheduling, contacts),
• Team collaboration {file synchronization, ideas and notes in a wiki, task management, full-text search)
• Real-time communication {presence, instant messaging, Web conferencing, application/desktop sharing, voice, audio and video conferencing)

QUESTION NO: 16

Which of the following stages are involved in the successful implementation of a collaboration platform? Each correct answer represents a part of the solution. Choose two.

A. Ongoing collaboration solution design
B. Federated identity management
C. Platform implementation
D. Product and service integration

Answer: A,C

Explanation:

The following stages are involved in the successful implementation of a collaboration platform are as follows:

1. Platform implementation
2. Ongoing collaboration solution design

QUESTION NO: 17

You work as a Network Administrator for uCertify Inc. You want the clients and servers in your organization to be able to communicate in a way that prevents eavesdropping and tampering of data on the Internet. Which of the following will you use to accomplish the task?

A. EFS
B. WEP
C. SSL
D. MS-CHAP

Answer: C

Explanation: In order to accomplish the task, you should use SSL in the organization's network. Secure Sockets Layer (SSL) is a protocol used to transmit private documents via the internet. SSL uses a combination of public key and symmetric encryption to provide communication privacy, authentication, and message integrity. Using the SSL protocol, clients and servers can communicate in a way that prevents eavesdropping and tampering of data on the Internet. Many Web sites use the SSL protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:. By default, SSL uses port 443 for secured communication.

Answer option B is incorrect. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, i.e., authentication and encryption. It provides security for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream.

Answer option 0 is incorrect. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the new version of MS-CHAP. MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the environment consisting of both Windows NT and Windows 2000/XP dial-up clients. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data.

Answer option A is incorrect. Encrypting File System (EFS) is used to encrypt sensitive data in files stored on disks using the NTFS file system. EFS is easy to manage, difficult to hack, and transparent to the owner of a file and to applications because it runs as an integrated system service. Only the owner of a protected file can open the file and work on it. Using EFS involves a minimum of administrative effort.

QUESTION NO: 18

Which of the following are the functions of a network security administrator? Each correct answer represents a complete solution. Choose three.

A. Backing up the files
B. Writing computer software
C. Maintaining and implementing a firewall
D. Developing, maintaining, and implementing IT security

Answer: A,C,D
Explanation:
A network security administrator is a person who is responsible for providing security of any network. A network security administrator concentrates on network design and security. Following are the functions of a network administrator:
• Developing, maintaining, and implementing IT security
• Maintaining and implementing a firewall
• Monitoring and securing the network and server
• Monitoring critical system files

QUESTION NO: 19

Which of the following is frequently used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it?

A. Fuzzer
B. Port scanner
C. MegaPing
D. UDP scan

Answer: B

Explanation:

A port scanner is a software application designed to probe a network host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. To portscan a host is to scan for listening ports on a single target host. To portsweep is to scan multiple hosts for a specific listening port. The latter is typically used in searching for a specific service, for example, an SQL-based computer worm may portsweep looking for hosts listening on TCP/UDP port 1433.

Answer option A is incorrect. The programs and frameworks that are used to create fuzz tests or perform fuzz testing are called fuzzers. Fuzzing has evolved from a niche technique into a full testing discipline with support from both the security research and traditional QA testing communities. Fuzzing (Fuzz testing) is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions. Fuzzing is commonly used to test for security problems in software or computer systems.

Answer option D is incorrect. UDP scan is little difficult to run. UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. Most UDP port scanners use this scanning method, and use the absence of a response to infer that a port is open. However, if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open. This method is also affected by ICMP rate limiting.

Answer option C is incorrect. MegaPing is used to provide all essential network utilities for information system specialists, system administrators, or individuals. It also includes comprehensive security scanner, host and port monitor, and network utilities. All these scanners can scan individual computers, domains, any range of IP addresses, selected type of computers inside domains, and user specified host lists.

QUESTION NO: 20

You work as a Network Administrator for uCertify Inc. You need to conduct network reconnaissance, which is carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized/allowed.

What will you do?

A. Use a SuperScan
B. Use a netcat utility
C. Use a vulnerability scanner
D. Use an idle scan

Answer: C
Explanation:
In the given scenario, you will use a vulnerability scanner. The vulnerability scanner can be used to conduct network reconnaissance. Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed. Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

Answer option B is incorrect. Netcat is a freely available networking utility that reads and writes data across network connections by using the TCP/IP protocol. Netcat has the following features:
• It provides outbound and inbound connections for TCP and UDP ports.
• It provides special tunneling such as UDP to TCP, with the possibility of specifying all network parameters.
• It is a good port scanner.
• It contains advanced usage options, such as buffered send-mode (one line every N seconds), and hexdump (to stderr or to a specified file) of transmitted and received data.
• It is an optional RFC854 telnet code parser and responder.

Answer option A is incorrect. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the hostname of the remote system. It can also be used as an enumeration tool for the following:
• NetBIOS information
• User and Group Accounts information
• Network shares
• Trusted Domains
• Services probing

QUESTION NO: 21

Which of the following arise every time an application takes a user-supplied data and sends it to a Web browser without first confirming or encoding the content?

A. Injection flaws
B. Cookies
C. One-click attacks
D. XSS flaws

Answer: D

Explanation:

Cross Site Scripting vulnerabilities or XSS flaws arise every time an application takes a user-supplied data and sends it to a Web browser without first confirming or encoding the content. A number of times attackers find these flaws in Web applications. XSS flaws allow an attacker to execute a script in the victim's browser, allowing him to take control of user sessions, disfigure Web sites, and possibly launch worms, viruses, malware, etc. to steal and access critical data from the user's database.

Answer option A is incorrect. Injection flaws are the vulnerabilities where a foreign agent illegally uses a sub-system. They are the vulnerability holes that can be used to attack a database of web applications. It is the most common technique of attacking a database. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing involuntary commands or changing data. Injection flaws include XSS (HTML Injection) and SQL Injection.

Answer option B is incorrect. Cookies are small collections of data stored on a client computer by a web server. By themselves, cookies are not a source of insecurity, but the way they are used can be. Programmers can foolishly store passwords or secret information in a cookie. A browser flaw could permit a site to read another site's cookies. Cookies containing session information could be stolen from a client computer and used by a hacker to hijack the user's logon session. Cookies are used to track a user's activities, and thus can leave a trail of sites users have visited. Users should block third-party cookies. Users should also use a secure browser and apply patches and updates as they become available.

Answer option C is incorrect. Cross-site request forgery, also known as one-click attack or session riding, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. The attack works by including a link or script in a page that accesses a site to which the user is known to have authenticated.

QUESTION NO: 22

How many levels of threats are faced by the SAN?

A. 3
B. 7
C. 2
D. 5

Answer: A
Explanation:
Storage area network transfers and stores crucial data; often, this makes storage area network vulnerable to risks. There are three different levels of threats faced by the SAN:
• Level one: These types of threats are unintentional and may result in downtime and loss of revenue. However, administrators can prevent these threats.
• Level two: These types of threats are simple malicious attacks that use existing equipments.
• Level three: These types of threats are large scale attacks and are difficult to prevent. These threats come from skilled attackers using uncommon equipments.

QUESTION NO: 23

Which of the following components are contained in Xsan?

Each correct answer represents a complete solution. Choose all that apply.

A. Ethernet network
B. SAN volume
C. Xsan metadata controller
D. Server clients

Answer: A,B,C
Explanation:
Xsan, introduced by Apple, is an enterprise-class SAN file system. It is a 64-bit duster file system specifically designed for small and large computing environments. It helps multiple Mac desktops and Xserve systems to share RAID storage volumes over a high-speed Fibre Channel network. Xsan comprises the following components:
• SAN volume
• Fibre Channel network
• Xsan metadata controller
• Xsan clients

• Ethernet network
• Network clients

QUESTION NO: 24

Which of the following statements are true about network-attached storage (NAS)? Each correct answer represents a complete solution. Choose all that apply.

A. NAS systems do not contain hard disks.
B. NAS uses file-based protocols, such as NFS, SMB/CIFS, or AFP.
C. NAS is connected to a computer network providing data access to heterogeneous network clients.
D. NAS is file-level computer data storage.

Answer: B,C,D
Explanation:
Network-attached storage (NAS) is file-level computer data storage connected to a computer network providing data access to heterogeneous network clients. NAS systems contain one or more hard disks, often arranged into logical, redundant storage containers or RAID arrays. It removes the responsibility of file serving from other servers on the network. NAS uses file-based protocols, such as NFS, SMB/CIFS, or AFP. NAS units rarely limit clients to a single protocol.

QUESTION NO: 25

Which of the following is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program?

A. Gray box testing
B. White box testing
C. Black box testing
D. Fuzzing

Answer: D
Explanation:
The programs and frameworks that are used to create fuzz tests or perform fuzz testing are called fuzzers. Fuzzing has evolved from a niche technique into a full testing discipline with support from both the security research and traditional QA testing communities. Fuzzing (Fuzz testing) is an

automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions. Fuzzing is commonly used to test for security problems in software or computer systems.

Answer option C is incorrect. Black box testing is also known as specification-based testing. It ignores the internal logic of an application. It refers to test activities using specification-based testing methods to discover errors in an application. The test activities are based on requirements and specifications of the application. It focuses on the following errors:
• Specification-based function errors
• Specification-based component/system behavior errors
• Specification-based performance errors
• User-oriented usage errors
• Black box interface errors

Answer option B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods:

Control flow-based testing
o Create a graph from source code.
o Describe the flow of control through the control flow graph.
o Design test cases to cover certain elements of the graph.

Data flow-based testing
o Test connections between variable definitions.
o Check variation of the control flow graph.
o Set DEF (n) contains variables that are defined at node n.
o Set USE (n) are variables that are read.

Answer option A is incorrect. Gray box testing is a combination of black box and white box testing. It is non-intrusive and impartial, as it does not require that a tester have access to the source code. It treats a system as a black box in the sense that it must be analyzed from the outside. Basically, it is used to find out defects related to bad design or bad implementation of the system. This type of testing is more commonly used with Web applications, as the Internet has a pretty stable interface.

QUESTION NO: 26

Which of the following statements are true about OCSP and CRL?

Each correct answer represents a complete solution. Choose all that apply.

A. The OCSP checks certificate status in real time
B. The CRL is a list of subscribers paired with digital certificate status.
C. The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current.
D. The CRL allows the authenticity of a certificate to be immediately verified.

Answer: A,B,C

Explanation:

Certificate Revocation List (CRL) is one of the two common methods when using a public key infrastructure for maintaining access to servers in a network. Online Certificate Status Protocol (OCSP), a newer method, has superseded CRL in some cases.

The CRL is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason for revocation. The dates of certificate issue, and the entities that issued them, are also included. The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current OCSP overcomes this limitation by checking certificate status in real time. The OCSP allows the authenticity of a certificate to be immediately verified.

QUESTION NO: 27

Which of the following is SAN management software and is designed for cross-platform workgroup collaboration?

A. SANmaestro
B. SANmelody
C. VisualSAN
D. MetaSAN

Answer: D

Explanation:

MetaSAN, developed by Tiger Technology Sari, is high-speed file sharing SAN management software. It is designed for cross-platform workgroup collaboration. This software allows users of Windows, Linux, and Mac OS X to share files with one another. MetaSAN enables sharing one (or

more) high speed RAID device with multiple computers using Fibre Channel, iSCSI, Ethernet, or InfiniBand interconnect.

Answer option C is incorrect. VisualSAN provides administrators with a single view of all devices across their storage networks. It delivers advanced network, performance, and configuration management capabilities. The VisualSAN management suite comprises three modules:
1.VisualSAN Network Manager
2.VisualSAN Configuration Manager
3.VisualSAN Performance Manager

Answer option B is incorrect. Standards Intel/AMD blades, servers, or virtual machines are converted by SANmelody into fully capable storage servers that perform virtualizing disks and serve them over existing networks to application servers. It enhances performance through built-in caching that minimizes delays from slow mechanical drives. SANmelody equitably distributes the available disk space into multiple applications spread across several machines.

Answer option A is incorrect. SANmaestro is an analysis and decision support tool. It monitors, reports, charts, gathers, and analyzes system performance and resource utilization information from multiple networked systems. This tool fits the organizations reporting and analysis needs, as it generates useful reports and charts.

This tool is used to collect system performance and utilization metrics. SANmaestro can analyze historical data accumulated over long periods {up to two years).

QUESTION NO: 28

End point security is an information security concept that assumes that each device (end point) is responsible for its own security. Which of the following tools are examples of end point security software?

Each correct answer represents a complete solution. Choose all that apply.

A. Grayware
B. Anti-malware
C. Anti-spyware
D. Anti-virus
E. Spam filters

Answer: B,C,D,E

Explanation:
End point security is an information security concept that assumes that each device (end point) is responsible for its own security. The examples of end point security software are:
• Anti-malware
• Anti-virus
• Anti-spyware
• Spam filters

Anti-malware programs can combat malware by providing real time protection against the installation of malware software on a computer. This type of protection works in the same way as that of antivirus protection. Anti-malware software scans all incoming network data for malware software and blocks any threats it comes across.

Anti-malware software programs can be used for detection and removal of malware software that has already been installed in a computer system. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found.

Anti-Virus software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.

Anti-Virus software is a class of program that searches your hard drive, floppy drive, and pen drive for any known or potential viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their computer assets.

Popular Anti-Virus packages are as follows:
• Bit Defender Anti-Virus
• McAfee Virus Scan
• Kaspersky Anti-Virus
• F-Secure Anti-Virus
• Symantec Norton Anti-Virus
• Panda Titanium Anti-Virus
• Avira Anti-Virus
• Avast Anti-Virus
• Trend Micro Anti-Virus
• Grisoft AVG Anti-Virus
• ESET Nod32 Anti-Virus
• Webroot Anti-Virus
• Quick Heal Anti-Virus

• eTrust EZ Anti-Virus
• ZoneAlarm Anti-Virus

Anti-spyware is software that is designed to protect a computer against malware, adware, spyware, rogueware, etc. It is a quite different from antivirus software because it does not specialize in viruses. Protection against spyware helps to defend against bugs that can send out unauthorized information about victim, steal confidential information, slow down Internet connection, install unwanted programs on the computer, etc.

Spam filters are utilities that stop spam (unsolicited) mails from reaching users. Spam filters are available as modules or components for mail servers (both incoming and outgoing). Administrators can also install spam and matware-scanning modules on firewalls and proxy servers. Administrators should opt for tools that place suspect messages in a special folder or queue that enables users to double-check the automated filters.

Answer option A is incorrect. Grayware refers to applications or files that are not classified as viruses or trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization. Often grayware performs a variety of undesired actions such as irritating users with pop-up windows, tracking user habits and unnecessarily exposing computer vulnerabilities to attack.

QUESTION NO: 29

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. What are the essential elements required for continuous monitoring?

Each correct answer represents a complete solution. Choose all that apply.

A. Ongoing assessment of system security controls
B. Security tools definition
C. Security status monitoring and reporting
D. Security impact analyses
E. Configuration management and change control

Answer: A,C,D,E
Explanation:
Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management

decisions. Following are the four essential elements required for continuous monitoring:
• Configuration management and change control
• Security impact analyses
• Ongoing assessment of system security controls
• Security status monitoring and reporting

QUESTION NO: 30

Which of the following statements are true about Continuous Monitoring? Each correct answer represents a complete solution. Choose all that apply.

A. It involves tracking changes to the information system that occur during its lifetime, and then determines the impact of those changes on the system security.
B. Continuous monitoring process is used extensively in the U.S. Federal Government.
C. Continuous monitoring in any system takes place after initial system security accreditation.
D. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation.

Answer: A,C
Explanation:
Continuous monitoring in any system takes place after initial system security accreditation. It involves tracking changes to the information system that occur during its lifetime, and then determines the impact of those changes on the system security. Due to the necessary changes in hardware, software, and firmware during the lifetime of an information system, an evaluation of the results of these modifications has to be conducted to determine whether corresponding changes necessarily have to be made to security controls, to bring the system to the desired security state.

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government.

QUESTION NO: 31

Mary is a new security administrator. She wants to focus most of her efforts on the areas that have the greatest risk. Which of the following areas poses the greatest risk?

A. Employees
B. Hackers
C. Cyber terrorism
D. Viruses

Answer: A
Explanation:
Employees pose the greatest risk. Even malware is often introduced to a network through lack of diligence on the part of employees.

Answer option B is incorrect. While hackers are a real problem, they pose less risk than internal employees.

Answer option D is incorrect. Viruses are a legitimate concern. However, they are often introduced due to employees failing to follow security polices.

Answer option C is incorrect. It is the case that cyber terrorism is a real threat. However, it is less of a threat than employees.

QUESTION NO: 32

Mike is trying to reduce the risks posed by end user activities. He is particularly concerned about how to deal with employees who take work home. Which of the following is the most likely risk posed by employees taking work home?

A. The employee selling confidential data
B. SQL Injection
C. Cost of transporting work data
D. Getting malware from home on the media used to transport work data

Answer: D
Explanation:
Employees who take work home, must take it on some sort of media. That media could pick up a virus or spyware from their home computer, which will then be brought back to the corporate network.

Answer option A is incorrect, Employees selling confidential data is always a possible risk, however it is less likely.

Answer option B is incorrect. SQL Injection is most likely accomplished by an external hacker.

Answer option C is incorrect. There is no significant cost associated.

QUESTION NO: 33

New technologies can pose unique and new risks that must be managed. Which of the following new technologies poses the most risk due to regulatory compliance?

A. Tablets
B. Smart phones
C. Cloud computing
D. Virtualization

Answer: C
Explanation:
Since cloud servers might be distributed anywhere in the world, the issue of complying with national regulations is a tricky one.
Answer option B is incorrect. While smart phones do pose risks, those risks are not due to regulatory issues.
Answer option D is incorrect. Virtualization, like smartphones, does pose its own security risks, but those risks are not primarily due to regulatory compliance.
Answer option A is incorrect. Tablets are not an issue for regulatory compliance. Tablets may have their own security issues, but do not have specific regulatory issues.

QUESTION NO: 34

Cloud computing is significantly impacting the definition of network perimeters. Which of the following is NOT a network perimeter issue with cloud computing?

A. Where is the data actually physically stored?
B. What is the viability of the cloud provider?
C. What regulatory requirements apply to the data given the data and the location of the servers?
D. What protections are in place on the cloud?

Answer: B
Explanation:
While the viability of the provider is an important issue to consider, it is not a network perimeter issue.

Answer options C, A, and D are incorrect. These are all significant network perimeter issues associated with cloud computing.

QUESTION NO: 35

Network boundaries can be logical or physical. Which of the following are boundaries a network administrator cannot control?

A. Informational
B. Logical
C. External
D. Physical

Answer: C
Explanation:
External boundaries are those outside your network. This term does not refer to your network perimeter. A network administrator cannot control external boundaries.
Answer options D and B are incorrect. Physical and logical boundaries are two broad classes of boundaries that are under your administrative control.
Answer option A is incorrect. An information domain is a legitimate domain the administrator must address. Information domain arises from the practice of partitioning information resources according to access control, need, and levels of protection required.

QUESTION NO: 36

A partnership is a for profit business association of two or more persons. Which of the following statements are true about partnership? Each correct answer represents a complete solution. Choose all that apply.

A. Each and every partner shares directly in the organization's profits and shares control of the business operation.
B. A partnership is an arrangement where parties agree to cooperate to advance their mutual interests.
C. The consequence of this profit sharing is that employees are jointly and independently liable for the partnership's debts.
D. Partnerships present the involved parties with special challenges that must be navigated unto agreement.

Answer: A,B,D

Explanation:

A partnership is a for profit business association of two or more persons. Because the business component is defined broadly by state laws and because persons can include individuals, groups of individuals, companies, and corporations, partnerships are highly adaptable in form and vary in complexity.

A partnership is an arrangement where parties agree to cooperate to advance their mutual interests. Partnerships present the involved parties with special challenges that must be navigated unto agreement. Each and every partner shares directly in the organization's profits and shares control of the business operation. The consequence of this profit sharing is that partners are jointly and independently liable for the partnership's debts.

QUESTION NO: 37

Which of the following statements are true about audit findings?

Each correct answer represents a complete solution. Choose all that apply.

A. Audit findings is described as dutifulness, obligingness, pliability, tolerance, and treatability.
B. Audit findings involve contracting out of a business function to an external provider/buyer.
C. The effective audit findings is designed to mitigate incomplete findings, as well as those that do not meet the intent of the process approach, have missing criteria or have incomplete objective evidence.
D. Audit findings are an effective method to facilitate the necessary improvements within a quality management system.

Answer: C,D

Explanation:

Audit findings are an effective method to facilitate the necessary improvements within a quality management system. The Effective Audit Findings is designed to mitigate incomplete findings, as well as those that do not meet the intent of the process approach, have missing criteria or have incomplete objective evidence. It helps organization in improving how it receives and interprets findings from second- and third-party auditors with the ultimate objective of quality management system improvement.

Answer option A is incorrect. Compliance is described as dutifulness, obligingness, pliability, tolerance, and tractability. Compliance means that an organization must take care of the organization's internal regulations, as well as follow the laws of the country and requirements of

local legislation and regulations.

Answer option B is incorrect. Outsourcing is the term which is used to define the process of contracting a business function to someone else. It involves contracting out of a business function to an external provider/buyer.

QUESTION NO: 38

Risk analysis provides the higher management the details necessary to determine the risks that should be mitigated, transferred, and accepted. What are the various stages in the risk analysis process?

Each correct answer represents a complete solution. Choose all that apply.

A. Management
B. Threat assessment
C. Evaluation of control
D. Monitoring
E. Asset control
F. Inventory

Answer: A,B,C,D,F
Explanation:
Risk analysis provides the higher management the details necessary to determine the risks that should be mitigated, transferred, and accepted. It recognizes risks, quantifies the impact of threats, and supports budgeting for security. It adjusts the requirements and objectives of the security policy with the business objectives and motives. The following are the stages in the risk analysis process.
1. inventory
2. Threat assessment
3. Evaluation of control
4. Management
5. Monitoring

QUESTION NO: 39

Denial of service attacks are quite common. Whether it is an ICMP flood, Syn Flood, or SMURF

attack, they all are based on the concept of_____.

A. Circumventing the firewall
B. Resource exhaustion
C. Exploiting OS vulnerabilities
D. Avoiding the IDS

Answer: B
Explanation:
Resource exhaustion is the term for the situation wherein a target system has exhausted all of its resources and can no longer respond to legitimate requests. All denial of service attacks are based on this concept.
Answer option A is incorrect. While many DoS attacks to involve circumvention the firewall, this is not a necessary component of a DoS.
Answer option D is incorrect. Avoiding IDS detection is actually very difficult for a DoS attack.
Answer option C is incorrect, Many DoS attacks do depend on exploiting OS vulnerabilities, However, this is not the basic concept of a DoS.

QUESTION NO: 40

Resource exhaustion includes all of the following except_____

A. Opening too many connections
B. Allocating all system memory to a single application
C. Overflowing a buffer with too much data
D. Flooding a network with excessive packets

Answer: C
Explanation:
Buffer overflow attacks is related to resource exhaustion but is not the same thing. The reason being that the buffer overflow is based on programmers not checking array bounds, rather than exhausting resources.

Answer options A, B, and D are incorrect. All of these are examples of resource exhaustion.

QUESTION NO: 41

Which of the following security measures would be most effective against a memory exhaustion DoS attack?

A. SPI Firewall
B. Secure programming
C. Checking user inputs
D. Truncating buffers

Answer: B

Explanation:

Memory exhaustion happens when a flaw in an application allows the application to keep consuming more memory leaving none available for other applications.
Answer option C is incorrect. Checking user inputs is an effective defense against SQL injection attacks, but not memory exhaustion attacks.

Answer option D is incorrect. Truncating buffers is an effective defense against a buffer overflow attack, .but not against memory exhaustion attacks.

Answer option A is incorrect. An SPI firewall is effective in stopping a syn flood, but would not help against a memory exhaustion attack.

QUESTION NO: 42

Which of the following federal regulations requires federal agencies to be able to monitor activity in a "meaningful and actionable way"?

A. FISMA
B. HIPAA
C. Sarbanes-Oxley
D. CAN SPAM

Answer: A

Explanation:

The Federal Information Security Management Act requires continuous monitoring of affected federal systems.

Answer option B is incorrect. The Health Information Portability and Accountability Act Governs the privacy of health records.
Answer option C is incorrect. Sarbanes Oxley addresses the retention of documents and records in publically traded companies.

Answer option D is incorrect. CAN SPAN regulates unsolicited email, commonly called spam.

QUESTION NO: 43

_____is defined as maintaining ongoing awareness of information.

A. Intrusion detection
B. Vulnerability assessment
C. Continuous Monitoring
D. Security Awareness

Answer: C
Explanation:
This is the definition of continuous monitoring. Ongoing is the keyword. Monitoring that is intermittent is very different than continuous monitoring.

Answer option B is incorrect. Vulnerability scanning can be part of continuous monitoring. And some vulnerability scanners have the option to monitor in real time, but a vulnerability scanner is only part of continuous monitoring.

Answer option A is incorrect. Intrusion detection should be real time and continuous, but does not involved risk management decisions or an awareness of information security.

Answer option D is incorrect. Security awareness is only one aspect of continuous monitoring.

QUESTION NO: 44

Denise works as a Security Administrator for a community college. She is assessing the various risks to her network. Which of the following is not a category of risk assessment?

A. Cost determination
B. Risk determination
C. Vulnerability assessment
D. Likelihood assessment

Answer: A
Explanation:

Of course the cost of addressing a risk must be computed, but that is not part of risk assessment.
Answer option D is incorrect. Likelihood assessment is a key part of risk assessment. How likely is a given threat? What threats are the most likely to your network?

Answer option B is incorrect. Determining what risks your network has, is one of the first steps in risk assessment.

Answer option C is incorrect. Assessing your networks vulnerabilities is a key part of risk assessment.

Answer option C is incorrect. Assessing your networks vulnerabilities is a key part of risk assessment.

QUESTION NO: 45

Which of the following is the best description of vulnerability assessment?

A. Determining what threats exist to your network.
B. Determining the impact to your network if a threat is exploited.
C. Determining the weaknesses in your network that would allow a threat to be exploited
D. Determining the likelihood of a given threat being exploited.

Answer: C
Explanation:
Weaknesses in your network due to inherent technology weaknesses, mis-configuration, or lapses in security are vulnerabilities.

Answer option A is incorrect. Determining the threats to your network is threat assessment not vulnerability assessment. In fact this phase is done before vulnerability assessment
Answer option D is incorrect. Determining the likelihood of a given attack is likelihood assessment. This would be done after vulnerability assessment.

Answer option B is incorrect. Impact analysis is certainly important, but this is done after vulnerability assessment.

QUESTION NO: 46

Juan is trying to perform a risk analysis of his network. He has chosen to use OCTAVE. What is OCTAVE primarily used for?

A. A language for vulnerability assessment
B. A comprehensive risk assessment model
C. A threat assessment tool
D. An impact analysis tool

Answer: B
Explanation:
OCTAVE, or Operationally Critical, Threat, Asset and Vulnerability Evaluation is a comprehensive risk assessment model. Answer option A is incorrect. OVAL, or Open Vulnerability Assessment Language is the language for vulnerability assessment. Answer options C and D are incorrect. Threat assessment and impact analysis are both part of OVAL, but only a part

QUESTION NO: 47

_____applies enterprise architecture concepts and practices in the information security domain.

A. ESA
B. OWASP
C. OVAL
D. AAR

Answer: A
Explanation:
Enterprise Security Architecture (ESA) is a system for applying network architecture principles and guidelines to network security.

Answer option D is incorrect. An After Action Report (AAR) is conducted to assess what went wrong after a breach.

Answer option C is incorrect. Open Vulnerability and Assessment Language (OVAL) is a standard to assess vulnerabilities in a system.

Answer option B is incorrect. The Open Web Application Security Project (OWASP) is a set of standards for security web applications.

QUESTION NO: 48

Which of the following is a written document and is used in those cases where parties do not imply a legal commitment or in those situations where the parties are unable to create a legally enforceable agreement?

A. Patent law
B. Memorandum of understanding (MOU)
C. Memorandum of agreement (MOA)
D. Certification and Accreditation (COA or CnA)

Answer: B
Explanation:
A memorandum of understanding (MOU) is a document that defines a bilateral or multilateral agreement between two parties. This document specifies a convergence of will between the parties, representing a proposed common line of action. A memorandum of understanding is generally used in those cases where parties do not imply a legal commitment or in those situations where the parties are unable to create a legally enforceable agreement. It is a proper substitute of a gentlemen's agreement.

Answer option A is incorrect. Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time.

Answer option C is incorrect. A memorandum of agreement (MOU) is a document that is written between two parties to cooperatively work together on a project for meeting the pre-decided objectives. The principle of an MOA is to keep a written understanding of the agreement between two parties.

A memorandum of agreement is used in various heritage projects. It can also be used between agencies, the public and the federal or state governments, communities, and individuals. A memorandum of agreement (MOA) lays out the main principles of a positive cooperative effort.
Answer option D is incorrect. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C8A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3.

Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

QUESTION NO: 49

Mark works as a Human Resource Manager for uCertify Inc. He is responsible to hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. What will Mark do to accomplish the task?

A. Job rotation
B. Mandatory Vacations
C. Job responsibility
D. Separation of duties

Answer: A
Explanation:
Job rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breadth of exposure to the entire operation.

Job rotation is practiced to allow qualified employees to gain more insights into the processes of a company, and to reduce boredom and increase job satisfaction through job variation. This process helps an organization to improve its overall security by rotating employees among different job positions.

Answer option B is incorrect. Mandatory vacations are vacations that are forced on employees to avail them. These vacations can ensure that employees take the time off that they should. It is important that employees not get burned out. Which would make them less effective in carrying out their duties. Mandatory vacations ensure that employees are effective all the time when they are on duty.

Answer option C is incorrect. Job responsibility is the specific work task an employee is required to perform on a regular basis.

Answer option D is incorrect. Separation of duties ensures that no one person is given the power to abuse the trust that others place in the information security. In any situation in which too much responsibility for a process falls to one person, there is the potential for abuse.

Another reason to separate duties is that if the person with all of the knowledge of a certain area or function suddenly leaves the company or dies in a tragic accident, then that knowledge is gone with the person. Someone else would have to quickly take over the position, possibly without adequate training, leaving the information vulnerable to attack while the new person learns the job. Separation of duties ensures that transition is smooth.

QUESTION NO: 50

Mark works as a Network Security Administrator for uCertify Inc. The organization is using an intranet to distribute information to its employees. A database residing on the network contains employees' information, such as employee name, designation, department, phone extension, date of birth, date of joining, etc. He is concerned about the security because the database has all information about employees, which can help an unauthorized person to recognize an individual.

Which Personally Identifiable Information should be removed from the database so that the unauthorized person cannot identify an individual?

A. Date of birth
B. Employee name
C. Employee code
D. Date of joining

Answer: A

Explanation:

According to the scenario, date of birth is uniquely identified information that can help the unauthorized person to recognize an individual. Therefore, Mark should remove date of birth of all employees from the database.

QUESTION NO: 51

Which of the following elements are essential elements of a privacy policy? Each correct answer represents a complete solution. Choose two.

A. Opt-out provision
B. Reliability
C. Availability
D. Notification

Answer: D

Explanation:

The essential elements of a privacy policy, which provides a high-level management statement of direction, are notifications and opt-out provisions.

QUESTION NO: 52

Which of the following is used to provide for the systematic review, retention and destruction of documents received or created in the course of business?

A. Document retention policy
B. Document research policy
C. Document entitled policy
D. Document compliance policy

Answer: A

Explanation:

A document retention policy is used to provide for the systematic review, retention and destruction of documents received or created in the course of business. It will identify documents that need to be maintained and consist of guidelines for how long certain documents should be kept and how they should be destroyed.

Answer options B, D. and C are incorrect. These are not valid options.

QUESTION NO: 53

Which of the following is a log that contains records of login/logout activity or other security-related events specified by the systems audit policy?

A. Process tracking
B. Logon event
C. Object Manager
D. Security Log

Answer: D

Explanation:

The Security log records events related to security like valid and invalid logon attempts or events related to resource usage, such as creating, opening, or deleting files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer.

Answer option B is incorrect. In computer security, a login or logon is the process by which individual access to a computer system is controlled by identifying and authorizing the user referring to credentials presented by the user.

Answer option C is incorrect. Object Manager is a subsystem implemented as part of the Windows Executive which manages Windows resources.

QUESTION NO: 54

Which of the following types of Incident Response Teams (IRT) is responsible for a logical or physical segment of the infrastructure, usually of a large organization or one that is geographically dispersed?

A. Distributed IRT
B. Outsourced IRT
C. Coordinating IRT
D. Central IRT

Answer: A

Explanation:

The various types of Incident Response Team (IRT) are as follows:
• Central IRT: It handles all incidents for the organization, usually either a small organization or one that is centrally located.
• Distributed IRT: It is responsible for a logical or physical segment of the infrastructure, usually of a large organization or one that is geographically dispersed.
• Coordinating IRT: It is a combination of central IRT and distributed IRT. Generally, the central team provides guidance to distributed IRTs, develops policies and standards, etc. The distributed team manages and implements incident response.
• Outsourced IRT: It states that the successful IRTs are comprised of the employees of the same organization, or may be fully or partially outsourced.

QUESTION NO: 55

Risk assessment helps in determining the extent of potential threats and risks associated with an IT system throughout its SDLC. Which of the following steps covered by the risk assessment methodology?

Each correct answer represents a complete solution. Choose three.

A. Vulnerability Identification
B. Cost Analysis
C. Threat Identification
D. System Characterization

Answer: A,C,D

Explanation:

Risk assessment is the first process of risk management. It helps in determining the extent of potential threats and risks associated with an IT system throughout its SDLC.

The risk assessment methodology covers nine steps which are as follows:

- Step 1 - System Characterization
- Step 2 - Threat Identification
- Step 3 - Vulnerability Identification
- Step 4 - Control Analysis
- Step 5 - Likelihood Determination
- Step 6 - Impact Analysis
- Step 7 - Risk Determination
- Step 8 - Control Recommendations
- Step 9 - Results Documentation

QUESTION NO: 56

Which of the following are the purposes of the Cost-benefit analysis process? Each correct answer represents a complete solution. Choose two.

A. To determine if an investment is sound
B. To describe the future value on the investment of the project
C. To see how it compares with alternate projects
D. To support benefit management, measurement, and reporting

Answer: A,C

Explanation:

The Cost-benefit analysis (CBA) process is used to calculate and compare benefits and costs of a project for the following purposes:

• To determine if an investment is sound

• To see how it compares with alternate projects

Answer options D and B are incorrect. These are not the purposes of the Cost-benefit analysis process,

QUESTION NO: 57

Which of the following is the capability to correct flows in the existing functionality without affecting other components of the system?

A. Manageability
B. Reliability
C. Maintainability
D. Availability

Answer: C

Explanation:

• Availability: It is used to make certain that a service/resource is always accessible.

• Manageability: It is the capability to manage the system for ensuring the constant health of the system with respect to scalability, reliability, availability, performance, and security.

• Maintainability: It is the capability to correct flows in the existing functionality without affecting other components of the system.

• Answer option B is incorrect. It is not a valid option.

QUESTION NO: 58

Which of the following is an approximate of the average or mean time until a component's first failure or disruption in the operation of the product, process, procedure, or design takes place?

A. MTBF
B. HMA
C. MSDS

D. MTF

Answer: D

Explanation:

Mean Time to Failure (MTTF) is an approximate of the average, or mean time until a components first failure, or disruption in the operation of the product, process, procedure, or design takes place. MTTF presumes that the product CANNOT be repaired and the product CANNOT continue any of its regular operations.

In many designs and components, MTTF is especially near to the MTBF, which is a bit longer than MTTF. This is due to the fact that MTBF adds the repair time of the designs or components. MTBF is the average time between failures to include the average repair time, or MTTR.
Answer option A is incorrect. Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation.

Answer option B is incorrect. Hash-based Message Authentication Code (HMAC) is a specific construction for calculating a Message Authentication Code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC. The resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits, and on the size and quality of the cryptographic key.

Answer option C is incorrect. A Material Safety Data Sheet (MSDS) is a document that specifies a set of guidelines regarding the proper handling, transporting, storage, and disposal of a hazardous substance or chemical. It also contains information on first-aid treatment, as it is helpful in case of accident or exposure to toxic material. This sheet is displayed in areas where such untoward incidents can be possible, so that in case of any emergency, proper actions, based on the information provided on the sheet, can be taken to handle the situation. The companies or organizations are required to create and paste MSDS in hazardous areas.

QUESTION NO: 59

Which of the following standard organizations promulgates worldwide proprietary industrial and commercial standards?

A. IEEE
B. ANSI

C. ISO
D. W3C

Answer: C
Explanation:
The International Organization for Standardization, widely known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments.

Answer option B is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

Answer option A is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.

Answer option D is incorrect. The World Wide Web Consortium (W3C) is an international industry consortium that develops common standards for the World Wide Web to promote its evolution and interoperability. It was founded in October 1994 by Tim Berners-Lee, the inventor of the Web, at the Massachusetts Institute of Technology, Laboratory for Computer Science [MIT/LCS] in collaboration with CERN, where the Web had originated, with support from DARPA and the European Commission.

QUESTION NO: 60

Which is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality?

A. Agreement

B. Service Improvement Plan
C. Benchmarking
D. COBIT

Answer: C
Explanation:
Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance.

Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make improvements or adapt specific best practices, usually with the aim of increasing some aspect of performance.

Answer option A is incorrect. COBIT stands for Control Objectives for Information and Related Technology. COBIT is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes, and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

Answer options B and D are incorrect. These are not valid options.

QUESTION NO: 61

Which of the following statements are true about prototypes?

Each correct answer represents a complete solution. Choose three.

A. It reduces initial project risks within a business organization.
B. It reduces the closeness between what a developer has defined for application architecture and what business management has understood.
C. It confirms technology recommendations for an application.
D. It helps verify some of the application requirements that are not dearly defined by a user.

Answer: A,C,D

Explanation:

The following are the purposes of creating a prototype:

1. It reduces initial project risks within a business organization.
2. It helps verify some of the application requirements that are not clearly defined by a user.
3. It confirms technology recommendations for an application.
4. It reduces the gap between what a developer has defined for an application architecture and what business management has understood.
5. It also reduces the gap between what a user has defined for an application requirement or scenario and what a developer has defined in the application development.

Answer:

QUESTION NO: 62

Which of the following is a structured review process to analyze what happened, why it happened, and how it can be done better, by the participants and those responsible for the project or event?

A. After action report
B. After action analysis
C. After action summary
D. After action review

Answer: D

Explanation:

An after action review (AAR) is a structured review process to analyze what happened, why it happened, and how it can be done better, by the participants and those responsible for the project or event. It occurs within a cycle of establishing the leader's intent, planning, preparation, action and review.

Answer options A, B, and C are incorrect. These are not valid options.

QUESTION NO: 63

Which of the following statements are true about capability-based security?

A. It is a concept in the design of secure computing systems, one of the existing security models.
B. It is a computer security model based on the Actor model of computation.
C. It is a scheme used by some computers to control access to memory.
D. It is a concept in the design of secure computing systems.

Answer: D

Explanation:

Capability-based security is a concept in the design of secure computing systems. A capability (known in some systems as a key) is a communicable, unforgivable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure.

Although most operating systems implement a facility which resembles capabilities, they typically do not provide enough support to allow for the exchange of capabilities among possibly mutually untrusting entities to be the primary means of granting and distributing access rights throughout the system. A capability-based system, in contrast, is designed with that goal in mind.
Answer options B, C, and A are incorrect. These are not correct statements about capability-based security.

QUESTION NO: 64

Which of the following statements are true about Fibre Channel over Ethernet (FCoE)?

Each correct answer represents a complete solution. Choose three.

A. It replaces the FCO and FC1 layers of the Fibre Channel stack with Ethernet.
B. It is an encapsulation of Fibre Channel frames over Ethernet networks.
C. It allows Fibre Channel to use 10 Gigabit Ethernet networks while preserving the Fibre Channel protocol.
D. It maps Fibre Channel over selected half duplex IEEE 802.3.

Answer: A,B,C

Explanation:

Fibre Channel over Ethernet (FCoE) is an encapsulation of Fibre Channel frames over Ethernet networks. It allows Fibre Channel to use 10 Gigabit Ethernet networks while preserving the Fibre Channel protocol. FCoE maps Fibre Channel over selected full duplex IEEE 802.3 networks for providing I/O consolidation over Ethernet and reducing network complexity in the datacenter. The

FCoE protocol specification replaces the FCO and FC1 layers of the Fibre Channel stack with Ethernet.

Answer option D is incorrect. It is not a correct statement about Fibre Channel over Ethernet (FCoE).

QUESTION NO: 65

which of the following is the randomness collected by an operating system or application for use in cryptography or other uses that require random data?

A. Confusion
B. Diffusion
C. Digital signature
D. Entropy

Answer: D
Explanation:
Non-repudiation is one of the security methods that is used to acknowledge the data delivery. It is a method of providing an acknowledgement to the sender of the data and an assurance of the sender's identity to the receiver, so that neither sender nor the receiver can later deny the data having processed by them. Nowadays, non-repudiation is achieved through digital signatures, as it ensures that the data or information, being transferred, has been electronically signed by the purported person (receiver). It also ensures the furnishing of the signature by the sender since a digital signature can be created only by one person.

Answer options B, A, and A are incorrect. These are not valid options.

QUESTION NO: 66

Which of the following is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally?

A. File carving
B. Virtual backup appliance
C. Backup
D. Data recovery

Answer: D

Explanation:

Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often the data are being salvaged from storage media such as internal or external hard disk drives, solid-state drives (SSD), USB flash drive, storage tapes, CDs, DVDs, RAID, and other electronics. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.

Answer option C is incorrect. A backup or the process of backing up is making copies of data which may be used to restore the original after a data loss event.

Answer option A is incorrect. File carving is the process of reassembling computer files from fragments in the absence of filesystem metadata.

Answer option B is incorrect. A virtual backup appliance (VBA) is a small virtual machine that backs up and restores other virtual machines.

QUESTION NO: 67

Which of the following refers to any system whereby things that are of value to an entity or group are monitored and maintained?

A. Asset management
B. Investment management
C. Service management
D. Product management

Answer: A

Explanation:

Asset management deals with the management of assets of an organization. An asset is defined as an item of value. It is essential for a company to identify, track, classify, and assign ownership for the most important assets. The main idea behind asset management is to ensure that the assets are protected.

Answer options B, D, and C are incorrect. These are not valid options.

QUESTION NO: 68

Which of the following are examples of privilege escalation? Each correct answer represents a complete solution. Choose two.

A. John uses SQL commands to login to a website he does not have authorization to
B. Juan logs in with his account, then takes over Anita's privileges
C. John logs in as a standard user but uses a flaw in the system to get admin privilege
D. Fred uses Ophcrack to get a Windows XP password

Answer: B,C

Explanation:

In both cases the user had some authentic access, but then got additional privileges they had not been authorized.

Answer option C is incorrect. This is an example of SQL injection.

Answer option D is incorrect. This is an example of password cracking.

QUESTION NO: 69

Allen is a network administrator for a hosting company. Multiple different companies store data on the same server. Which of the following is the best method to reduce security issues from co-mingling?

A. Install each data set on a separate drive
B. Install each data set on a separate partition
C. Install each data set on the same drive, but use EFS to encrypt each data set separately.
D. Install each data set on a separate VM

Answer: D

Explanation:

Visualization completely separates the data and prevents commingling. Visualization is a technology that enables customers to run multiple operating systems concurrently on a single physical server, where each of the operating systems runs as a self-contained computer, visualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device, or network resources. It is a computing technology that enables a single user to access multiple physical devices. The goal of visualization is usually a more effective use of resources. It simplifies provisioning, while adding flexibility at the same time.

Answer options B and A are incorrect. An operating system can view partitions and drives just as if they were different folders/directories on the same drive.

Answer option C is incorrect. Encrypting the data sets with EFS will inhibit users' access for the data.

QUESTION NO: 70

Allen needs a program that injects automatically semi-random data into a program or stacks and detects bugs. What will he use?

A. Fuzzer
B. Happy path
C. Boundary value analysis
D. Agile testing

Answer: A
Explanation:
A fuzzer is a program that is used to inject automatically semi-random data into a program/stack and detect bugs. The programs and frameworks that are used to create fuzz tests or perform fuzz testing are called fuzzers. Fuzzing has evolved from a niche technique into a full testing discipline with support from both the security research and traditional QA testing communities. Fuzzing (Fuzz testing) is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions. Fuzzing is commonly used to test for security problems in software or computer systems.

Answer option C is incorrect. Boundary value analysis is a software testing technique in which tests are designed to include representatives of boundary values.

Answer option B is incorrect. A happy path is a default scenario that features no exception or error conditions, and contains the sequence of activities that will be executed if everything goes as anticipated.

Answer option D is incorrect. Agile testing is a software testing practice. It follows the principles of agile software development. This testing does not accentuate the testing procedures and focuses on ongoing testing against the newly developed code until quality software from an end customer's perspective results. It is built upon the philosophy that testers need to adapt to the rapid

deployment cycles and changes in the testing patterns.

QUESTION NO: 71

Allen is using a security feature that ensures that if hackers want to compromise a private key, they will only be able to access data in transit protected by that key and not any future data because future data will not be associated with that compromised key?

Which security feature is he using?

A. IPSec
B. PGP
C. SPKI
D. PFS

Answer: D
Explanation:
PFS (Perfect Forward Secrecy) will ensure that the same key will not be generated again, so forcing a new diffie-hellman key exchange. Perfect forward secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.
Forward secrecy has been used as a synonym for perfect forward secrecy, since the term perfect has been controversial in this context. However, at least one reference distinguishes perfect forward secrecy from forward secrecy with the additional property that an agreed key will not be compromised even if agreed keys derived from the same long-term keying material in a subsequent run are compromised.

Answer option C is incorrect. Simple public key infrastructure (SPKI) does not deal with public authentication of public key information, that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP's web of trust. SPKI does not bind people to keys, since the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an 'authorization loop'' in SPKI terminology, where authorization is integral to its design.

Answer option B is incorrect. Pretty Good Privacy (PGP) is an encryption method that uses public-key encryption to encrypt and digitally sign e-mail messages during communication between e-mail clients. PGP is effective, easy to use. and free. Therefore, it is one of the most common ways to protect messages on the Internet.

Answer option A is incorrect. Internet Protocol Security (IPSec) is an Internet Protocol security standard. It is used to provide a general, policy-based IP layer security mechanism that is used for providing host-by-host authentication. IPSec policies can be defined as having security rules and settings that control the flow of inbound data,

QUESTION NO: 72

Which of the following is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously?

A. Electronic mail
B. Instant messaging
C. Video conferencing
D. Audio conferencing

Answer: C
Explanation:
Video conferencing is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously. Video conferencing differs from videophone calls in that it's designed to serve a conference rather than individuals.

It uses telecommunications of audio and video to bring people at different sites together for a meeting. This can be as simple as a conversation between two people in private offices (point-to-point) or involve several sites (multi-point) with more than one person in large rooms at different sites. Besides the audio and visual transmission of meeting activities, videoconferencing can be used to share documents, computer-displayed information, and whiteboards.

Answer option D is incorrect. Audio conferencing is a method of communication in which the calling party wishes to have more than one called party listens in to the audio portion of the call. The conference calls may be designed to allow the called party to participate during the call, or the call may be set up so that the called party merely listens into the call and cannot speak. It can be designed so that the calling party calls the other participants and adds them to the call.
Answer option B is incorrect. Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The users text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.

IM falls under the umbrella term online chat, as it is a real-time text-based networked communication system, but is distinct in that it is based on clients that facilitate connections between specified known users (often using Buddy List, Friend List or Contact List), whereas online chat also includes web-based applications that allow communication between users in a multi-user environment.

Answer option A is incorrect. E-mail (electronic mail) is a method of exchanging of computer-stored messages by telecommunication. E-mail messages are usually encoded in ASCII text. However, a user can also send non-text files, such as graphic images and sound files, as attachments sent in binary streams. E-mail was one of the first applications being made available on the Internet and is still the most popular one. A large percentage of the total traffic over the Internet is of the e-mails. E-mails can also be exchanged between online service provider users and in networks other than the Internet, both public and private.

E-mails can be distributed to lists of people as well as to individuals. A shared distribution list can be managed by using an e-mail reflector. Some mailing lists allow you to subscribe by sending a request to the mailing list administrator. A mailing list that is administered automatically is called a list server.

E-mail is one of the protocols included with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols. A popular protocol for sending e-mails is Simple Mail Transfer Protocol and a popular protocol for receiving it is POP3. Both Netscape and Microsoft include an e-mail utility with their Web browsers.

QUESTION NO: 73

Which of the following statements best describe the advantages of Simple Object Access Protocol (SOAP): Each correct answer represents a complete solution. Choose three.

A. It is versatile enough to allow for the use of different transport protocols.
B. It is simple and extensible.
C. It allows easier communication through proxies and firewalls than previous remote execution technology.
D. It is language and platform dependent.

Answer: A,B,C
Explanation:
The advantages of SOAP are as follows:
• It allows easier communication through proxies and firewalls than previous remote execution

technology.
• It is versatile enough to allow for the use of different transport protocols. The standard stacks use HTTP as a transport protocol, but other protocols are also usable.
• It is platform independent.
• It is language independent.
• It is simple and extensible.

QUESTION NO: 74

An organization s network uses public keys for message encryption. Which of the following manages security credentials in the network and issues certificates to confirm the identity and other attributes of a certificate in relation to other entities?

A. Certificate Authority
B. Certificate Revocation List
C. Public Key Infrastructure
D. Online Certificate Status Protocol

Answer: A
Explanation:
Certification authority (CA) is an entity in a network, which manages security credentials and public keys for message encryption. It issues certificates that confirm the identity and other attributes of a certificate in relation to other entities. Depending on the public key infrastructure implementation, a certificate includes the owners name, the owner's public key, information about the public key owner, and the expiry date of the certificate.

Answer option B is incorrect. CRL stands for Certificate Revocation List. In CRL, the certificates that are revoked by the Certificate Authority (CA) are mentioned. It becomes necessary for NetScreen to check the status of certificates received against a CRL to ensure their validity in phase 1 negotiation. The firewall recovers the CRL that is defined in the CRL certificate if a CRL is not loaded into the NetScreens database. The firewall attempts to recover the CRL defined in the CA certificate by means of LDAP or HTTP. In case the CRL is not defined in the CA certificate it can use the URL defined by the user for the CRL.

Answer option D is incorrect. Online Certificate Status Protocol (OCSP) is used for obtaining the revocation status of an X.509 digital certificate. It is used to verify the status of a certificate. It was created as an alternative to certificate revocation lists (CRL). It provides more timely information about the revocation status of a certificate. It also eliminates the need for clients to retrieve the CRLs themselves. Therefore, it generates to less network traffic and provides better bandwidth

management. It is described in RFC 2560 and is on the Internet standards track.

Answer option C is incorrect. A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message.

QUESTION NO: 75

What is the goal of a black-box penetration testing?

A. To simulate a user to include customizable scripts, additional tools and configurable kernels in personalized distributions
B. To simulate an external hacking or cyber warfare attack
C. To simulate an attacker who has some knowledge of the organization and its infrastructure
D. To simulate a malicious insider who has some knowledge and possibly basic credentials to the target system

Answer: B
Explanation:
Black Box is a kind of Penetration testing, which assumes no prior knowledge of the infrastructure to be tested. The testers must first determine the location and extent of the systems before commencing their analysis. Black box testing simulates an attack from someone who is unfamiliar with the system.

Answer option D is incorrect. A white box penetration testing has a goal to simulate a malicious insider who has some knowledge and possibly basic credentials to the target system.
Answer option A is incorrect. BackTrack has a goal to simulate a user to include customizable scripts, additional tools and configurable kernels in personalized distributions.

Answer option C is incorrect. A grey box penetration testing has a goal to simulate an attacker who has some knowledge of the organization and its infrastructure.

QUESTION NO: 76

You work as a System Administrator for uCertify Inc. The company has a Windows-based network. A user requests you to provide him instructions regarding the installation of application software's on his computer. You want to show the user how to perform the configuration by taking control of his desktop. Which of the following tools will you use to accomplish the task?

A. Remote desktop
B. Task Manager
C. Remote Assistance
D. Computer Management

Answer: C

Explanation:

In order to accomplish the task, you should use the Remote Assistance tool. By using Remote Assistance, you can take shared control of the users desktop, which will allow you to perform the necessary configurations on the shared desktop while the remote user is watching it straight away.

QUESTION NO: 77

Which of the following is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems?

A. System Development Life Cycle
B. Security Requirements Traceability Matrix
C. Security Development Life Cycle
D. Product lifecycle management

Answer: A

Explanation:

The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems.

The following are the five phases in a generic System Development Life Cycle:

1. Initiation
2. Development/acquisition
3. Implementation
4. Operation/maintenance
5. Disposal

Answer option C is incorrect. The Security Development Lifecycle (SDL) is a software

development security assurance process proposed by Microsoft. It reduces software maintenance costs and increases reliability of software concerning software security related bugs. The Security Development Lifecycle (SDL) includes the following seven phases:

1. Training
2. Requirements
3. Design
4. Implementation
5. Verification
6. Release
7. Response

Answer option B is incorrect. Security Requirements Traceability Matrix (SRTM) is a grid that provides documentation and easy presentation of what is necessary for the security of a system. SRTM is essential in those technical projects that call for security to be incorporated. SRTM can be used for any type of project. It allows requirements and tests to be easily traced back to one another. SRTM ensures that there is accountability for all processes. It also ensures that all work is being completed.

Answer option D is incorrect. Product lifecycle management (PLM) is the process of managing the entire lifecycle of a product from its conception, through design and manufacture, to service and disposal. PLM integrates people, data, processes and business systems and provides a product information backbone for companies and their extended enterprise. Product lifecycle management is very important for a corporation s information technology structure. The core of PLM is in the creations and central management of all product data and the technology used to access this information and knowledge.

QUESTION NO: 78

Which of the following is a flexible set of design principles used during tine phases of systems development and integration?

A. Service-oriented modeling framework (SOMF)
B. Sherwood Applied Business Security Architecture (SABSA)
C. Service-oriented modeling and architecture (SOMA)
D. Service-oriented architecture (SOA)

Answer: D

Explanation:

A service-oriented architecture (SOA) is a flexible set of design principles used during the phases

of systems development and integration. A deployed SOA-based architecture will provide a loosely integrated suite of services that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications- to be aware of available SOA-based services.

Answer option C is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA.
Answer option A is incorrect. The service-oriented modeling framework (SOMF) has been proposed by author Michael 8ell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems.

The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme.

Answer option B is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

QUESTION NO: 79

A user has entered a user name and password at the beginning of the session, and accesses multiple applications. He does not need to re-authenticate for accessing each application. Which of the following authentication processes is he using?

A. File authentication
B. Mutual authentication
C. Biometric authentication
D. SSO authentication

Answer: D
Explanation:
The user is using single sign-on (SSO) authentication process. In this process, he needs one-time authentication to access multiple resources. He is required to enter a user name and password

only at the beginning of the session. He does not need to re-authenticate or maintain separate usernames and passwords for accessing each application.

Answer option B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication.

Answer option A is incorrect. There is no such authentication process as File authentication.
Answer option C is incorrect. Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment.

QUESTION NO: 80

Which of the following helps an employee to access his corporation's network while traveling?

A. Remote access
B. Remote Assistance
C. Task Manager
D. Computer management

Answer: A
Explanation:
In most enterprises, networks secure remote access has become an important component. Remote access helps in accessing a computer or a network from a remote distance. In corporations, people working in branch offices, telecommuters, and people who are traveling may need to access the corporation s network. Home users can access the Internet through remote access to an Internet service provider (ISP).

Answer option B is incorrect. Remote Assistance is a windows feature to enable support personnel (helper) to provide technical support to a remote user (host). Through Remote Assistance a helper can view Windows session of a host on his computer itself.
Remote Assistance works as follows:
• A remote user sends an invitation to an Administrator (or expert) through e-mail or Windows Messenger.
• The Administrator accepts the request and can then view the users desktop.

To maintain privacy and security, all communication is encrypted. Remote Assistance can be used only with the permission of the person who requires the assistance.

Note: If the user has enabled the Allow this computer to be controlled remotely option in Remote control section of Remote Assistance Settings dialog box, an expert can even take control of the keyboard and mouse of a remote computer to guide the user.

Answer option D is incorrect. Computer Management is an administrative tool that allows administrators to manage the local computer in several ways, but it cannot be used to provide remote assistance to a user.

Answer option C is incorrect. The Task Manager utility provides information about programs and processes running on a computer. By using Task Manager, a user can end or run programs, end processes, and display a dynamic overview of his computers performance. Task Manager provides an immediate overview of system activity and performance.

QUESTION NO: 81

You have considered the security of the mobile devices on your corporate network from viruses and malware. Now, you need to plan for remotely enforcing policies for device management and security, which of the following things are includes in the configuration management of mobile devices?

Each correct answer represents a part of the solution. Choose three.

A. Controlling the apps deployed on devices
B. Managing the OS version of devices
C. Supporting other preferred corporate policy
D. Managing application and security patches

Answer: B,D
Explanation:
Configuration management is included in the remote device management policies. It involves deploying IT-approved software versions of supported mobile platforms. Configuration management includes the following things:
• Managing the OS version of devices
• Managing application and security patches
• Supporting other preferred corporate policy

QUESTION NO: 82

Which of the following devices allows telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system?

A. IP phone
B. Laptop
C. IP camera
D. Smartphone

Answer: A
Explanation:
An IP phone uses Voice over IP technologies, allowing telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system. Calls can traverse the Internet, or a private IP Network such as that of a company. The phones use control protocols such as Session Initiation Protocol. Skinny Client Control Protocol, or one of the various proprietary protocols such as Skype. IP phones can be simple software-based Softphones or purpose-built hardware devices that appear much like an ordinary telephone or a cordless phone. Ordinary PSTN phones are used as IP phones with analog telephony adapters (ATA). Following is an image of an IP phone:

C:\Documents and Settings\user-nwz\Desktop\1.JPG

Answer option D is incorrect. A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone. A smartphone is a mobile phone with advanced PC like capabilities. Blackberry and iPhone are the two most popular brands of smartphones. It allows the user to install and run more advanced applications based on a specific platform.

Answer option C is incorrect. An IP camera is a digital camera used for surveillance. It is unlike analog closed circuit television cameras can send and receive data through a computer network and the Internet. There are two types of IP cameras:

Centralized IP camera: It needs a central Network Video Recorder (NVR) to handle the recording, video and alarm management.
Decentralized IP camera: It does not need a central Network Video Recorder (NVR).
Decentralized IP camera has built-in recording functionality and so. it can record directly to digital storage media.

Answer option B is incorrect. A laptop is a type of portable computer. It is designed for mobile use and small and light enough to sit on a person's lap while in use. It integrates most of the typical components of a desktop computer, including a display, a keyboard, a pointing device (touchpad or trackpad, pointing stick), speakers, and often including a battery, into a single small and light unit.

Laptops are usually notebook-shaped with thicknesses between 0,7*1.5 inches (18-38 mm) and dimensions ranging from 10x8 inches (27x22cm, 13" display) to 15x11 inches (39x28cm, 17" display) and up. Modern laptops weigh 3 to 12 pounds (1.4 to 5.4 kg): older laptops were usually heavier. Most laptops are designed in the flip form factor to protect the screen and the keyboard when closed.

QUESTION NO: 83

Juan is working as a Security Administrator for a credit card processing company. He is concerned about PCI compliance and so, he uses network segmentation. How does segmentation help Juan?

A. Segmentation would help prevent viruses.
B. Segmentation reduces the scope of machines that need to be PCI compliant.
C. Segmentation is required by PCI regulations.
D. Segmentation would have no effect.

Answer: B

Explanation:

By segmenting the network, Juan reduces the number of machines that require PCI compliance, and thus makes PCI administration simpler.

Answer option C is incorrect, PCI regulations does not require network segmentation.

Answer option D is incorrect. By reducing the scope of network that requires segmentation, it is easier to maintain compliance.

Answer option A is incorrect. Segmentation may slow down the spread of a virus, but the impact of segmentation on viruses is based on what is done in each segment, not the segmentation itself.

QUESTION NO: 84

Dipen is looking for a method to effectively get security policies read by staff and management, which of the following is the best solution?

A. Printed policies
B. Intranet Website
C. Routine informational meetings
D. Email blast

Answer: B

Explanation:

Dipen should use the Intranet Website. This method puts the security policies in a location that is easy for staff to access, and it is also easy to update. It also does not interfere unnecessarily with employees work processes.

Answer option D is incorrect. An email blast is inconvenient, and must be repeated any time updates to the policies are made. It is also inconvenient for staff members to refer back to.

Answer option A is incorrect. Printed policies are difficult to store and access, generate unnecessary paper, and are difficult to update.

Answer option C is incorrect. Routine meetings are very intrusive and interrupt the normal work flow. They can also be difficult to schedule all the staff at a specific time.

QUESTION NO: 85

Which of the following teams has the responsibility of accounting for personnel and rendering aid?

A. Physical security team
B. Emergency response team
C. Emergency management team
D. Damage assessment team

Answer: B
Explanation:
The emergency response team has the responsibility of accounting for personnel and rendering aid. The emergency response team includes fire wardens for each floor and those persons trained in administering first aid.

Answer option D is incorrect. The damage assessment team assesses the damage of the disaster in order to provide the estimate of time required to recover.

Answer option A is incorrect. The physical security team addresses crowd control and security and operates 24 hours a day to protect individuals and organizational assets.

Answer option C is incorrect. The Emergency management team consists of executives and line managers to make strong decisions at the Emergency Operations Center. This team coordinates with the managers still operating on undamaged areas of the business and makes decisions about the allocation of personnel necessary to support the response and recovery efforts. The leaders of each team report to the emergency management team.

QUESTION NO: 86

You work as a Network Administrator for uCertify Inc. The company has a TCP/IP based network. You have segmented the network in multiple sub networks. Which of the following advantages will you get after segmentation?

Each correct answer represents a complete solution. Choose three.

A. Limited network problems
B. Improved security
C. Reduced congestion
D. Reduced performance

Answer: A,B,C
Explanation:
Network segmentation in computer networking is the act or profession of splitting a computer network into subnetworks, each being a network segment or network layer. The advantages of

such splitting are primarily for boosting performance and improving security.
Advantages:
• Reduced congestion: Improved performance is achieved because on a segmented network, there are fewer hosts per subnetwork, thus minimizing local traffic.
• Improved security: Broadcasts will be contained to the local network. Internal network structure will not be visible from outside.
• Containing network problems: It limits the effect of local failures on other parts of the network.

QUESTION NO: 87

Which of the following is a computer program that is designed to assess computers, computer systems, networks, or applications for weaknesses?

A. Vulnerability scanner
B. Paros
C. Port scanner
D. SYN scan

Answer: A
Explanation:
Vulnerability scanners work on the concept of port scanners. In addition to identifying hosts and open ports, a vulnerability scanner also provides information on the associated vulnerabilities. Vulnerability scanners are very useful to identify out-of-date software versions, applicable patches, system upgrades, etc. The weakness of these scanners is that they can only identify surface vulnerabilities. These scanners are unable to address the overall risk level of a scanned network.

Answer option B is incorrect. Paros is a Web application vulnerability scanner that supports editing /viewing HTTP/HTTPS messages on-the-fly to change items such as cookies and form fields. It also includes various features, such as Web traffic recorder, Web spider, hash calculator, and a scanner for testing common Web application attacks such as SQL injection and cross-site scripting. A SYN scan is a type of TCP scanning. This scan type is also known as 'half-open scanning' because it does not open a full TCP connection. The port scanner generates a SYN packet. If the target port is open, it responds with a SYN-ACK packet. The scanner host responds with an RST packet that causes the connector before the handshake is completed.

Answer option C is incorrect. A port scanner is a software tool that is designed to search a network host for open ports. This tool is often used by administrators to check the security of their networks. It is also used by hackers to compromise the network and systems.

QUESTION NO: 88

Which scanning is one of the more unique scan types, as it does not exactly determine whether the port is open/closed, but whether the port is filtered/unfiltered?

A. UDP scanning
B. TCP SYN scanning
C. TCP FIN scanning
D. ACK scanning

Answer: D
Explanation:
ACK scanning is one of the more unique scan types. It determines whether the port is filtered or unfiltered instead of determining whether the port is open or closed. This is especially good when attempting to explore for the existence of a firewall and its rule-sets. In TCP SYN/ACK scanning, an attacker sends a SYN/ACK packet to the target port. If the port is closed, the victim assumes that this packet was mistakenly sent by the attacker, and sends the RST packet to the attacker. If the port is open, the SYN/ACK packet will be ignored and the port will drop the packet. TCP SYN/ACK scanning is stealth scanning, but some intrusion detection systems can detect TCP SYN/ACK scanning.

Answer option B is incorrect. TCP SYN scanning is also known as half-open scanning because in this type of scanning, a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:
1. The attacker sends a SYN packet to the target port.
2. If the port is open, the attacker receives the SYN/ACK message.
3. Now the attacker breaks the connection by sending an RST packet.
4. If the RST packet is received, it indicates that the port is closed.

This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

Answer option A is incorrect. UDP scan is little difficult to run. UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. Most UDP port scanners use this scanning method, and use the absence of a response to infer that a port is open. However, if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open. This method is also affected by ICMP rate limiting.

Answer option C is incorrect. TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop that packet. TCP FIN scanning is useful only for identifying ports of non-Windows operating systems because Windows operating systems send only RST packets irrespective of whether the port is open or closed.

QUESTION NO: 89

Consider the following scenario.

A user receive an email with a link to a video about a news item, but another valid page, for instance a product page on ebay.com, can be hidden on top underneath the 'Play' button of the news video. The user tries to play' the video but actually buys' the product from ebay.com.

Which malicious technique is used in the above scenario?

A. Malicious add-ons
B. Cross-Site Request Forgery
C. Click-jacking
D. Non-blind spoofing

Answer: C
Explanation:
Click-jacking is a malicious technique that is used to trick Web users into revealing confidential information or sometimes taking control of their computer while clicking on apparently innocuous Web pages. Click-jacking is used to take the form of embedded code/script that can execute without the users' knowledge, such as clicking on a button appearing to execute another function. The term "click-jacking" was invented by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as UI redressing, Click-jacking can be understood as an instance of the confused deputy problem.

Answer option D is incorrect. Non-blind spoofing is a type of IP spoofing attack. This attack occurs when the attacker is on the same subnet as the destination computer, or along the path of the destination traffic. Being on the same subnet, it is easy for the attacker to determine the sequence number and acknowledgement number of the data frames. In a non-blind spoofing attack, the attacker can redirect packets to the destination computer using valid sequence numbers and acknowledge numbers. The result is that the computer's browser session is redirected to a malicious website or compromised legitimate sites that may infect computer with malicious code or

allow the attacker to perform other malicious activities.

Answer option A is incorrect, Add-ons such as browser plug-ins, application add-ons. font packs, and other after-market components can be an attack vector for hackers. Such add-ons are malicious add-ons. These add-ons can be Trojan horses infecting computers. Antivirus software is an obvious form of defense. Security administrators should also establish a corporate security policy prohibiting the installation and use of unapproved add-ons.

Answer option B is incorrect. CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding. CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution.

QUESTION NO: 90

Which of the following concepts are included in the security of a SAN? Each correct answer represents a complete solution. Choose all that apply.

A. Host adapter-based security
B. Storage-controller mapping
C. Switch zoning
D. IDS implementation

Answer: A,B,C
Explanation:
Storage area network (SAN) is a dedicated network that provides access to a consolidated, block level data storage. The security of SAN is completely dependent upon the users authentication or authorization. SAN security includes the following concepts:
• Host adapter-based security: Security measures for the Fibre Channel host bus adapter can be implemented at the driver level.
• Switch zoning: Switch zoning is used in a switch-based Fibre Channel SAN. It refers to the masking of all nodes connected to the switch.
• Storage-controller mapping: By mapping all host adapters against LUNs in the storage system, some storage sub-systems accomplish LUN masking in their storage.

Answer option D is incorrect, IDS is not implemented for the security of a SAN.

QUESTION NO: 91

Which of the following are the reasons to use SAN?

Each correct answer represents a complete solution. Choose all that apply.

A. Faster backup of large amounts of data
B. Fast and extensive disaster recovery
C. Better disk utilization
D. Cost effectiveness
E. Better availability for applications

Answer: A,B,C,E
Explanation:
Reasons to use SAN are as follows:
• Better disk utilization
• Fast and extensive disaster recovery
• Better availability for applications
• Faster backup of large amounts of data

Answer option D is incorrect. Installing SAN is expensive and it is not a reason to use SAN.

QUESTION NO: 92

In which level of threats of the SAN are threats large scale attacks and difficult to prevent?

A. Level three
B. Level one
C. Level four
D. Level two

Answer: A
Explanation:
Storage area network transfers and stores crucial data: often, this makes storage area network vulnerable to risks. There are three different levels of threats faced by the SAN:
• Level one: These types of threats are unintentional and may result in downtime and loss of revenue. However, administrators can prevent these threats.
• Level two: These types of threats are simple malicious attacks that use existing equipments.

• Level three: These types of threats are large scale attacks and are difficult to prevent. These threats come from skilled attackers using uncommon equipments.

QUESTION NO: 93

Which of the following features are provided by SAN for SQL servers? Each correct answer represents a complete solution. Choose all that apply.

A. Faster disaster recovery
B. Non-clustered environment
C. Storage efficiencies
D. Increased database size

Answer: A,C,D
Explanation:
Storage area network (SAN) is a dedicated network that provides access to a consolidated, block level data storage.

SAN provides the following features for SQL servers:
• Increased database size
• Clustered environment
• Performance advantages
• Storage efficiencies
• Faster disaster recovery

QUESTION NO: 94

Which of the following statements are true about distributed computing? Each correct answer represents a complete solution. Choose all that apply.

A. In distributed computing, the computers interact with each other in order to achieve a common goal
B. A distributed system consists of multiple autonomous computers that communicate through a computer network.
C. In distributed computing, a problem is divided into many tasks, each of which is solved by a programmer.
D. Distributed computing refers to the use of distributed systems to solve computational problems.

Answer: A,B,D

Explanation:

Distributed computing is a field of computer science that studies distributed systems. In distributed computing, a problem is divided into many tasks, each of which is solved by one computer. A distributed system consists of multiple autonomous computers that communicate through a computer network. It also refers to the use of distributed systems to solve computational problems. The computers interact with each other in order to achieve a common goal.

QUESTION NO: 95

Interceptor is a pseudo proxy server that performs HTTP diagnostics, which of the following features are provided by HTTP Interceptor? Each correct answer represents a complete solution. Choose all that apply.

A. It controls cookies being sent and received.
B. It allows to browse anonymously by withholding Referrer tag, and user agent.
C. It can view each entire HTTP header.
D. It debugs DOC, DOCX, and JPG file.

Answer: A,B,C

Explanation:

HTTP diagnostics is performed by the HTTP Interceptor which is a pseudo proxy server and it also facilitates viewing the two way communication between the browser and the Internet.

Various features of HTTP Interceptor are as follows:
• View each entire HTTP header.
• Debug your PHP, ASP. CGI or JavaScript and htaccess file.
• Control Cookies being sent and received.
• Find out what sort of URL redirection the site may be using.
• Browse anonymously by withholding Referrer tag, and user agent.

QUESTION NO: 96 CORRECT TEXT

Fill in the blank with the appropriate word.

_____encryption protects a file as it travels over protocols, such as FTPS (SSL), SFTP (SSH), and HTTPS.

Answer: Transport

Explanation: Transport encryption protects a file as it travels over protocols, such as FTPS (SSL). SFTP (SSH), and HTTPS. Leading solutions use encryption strengths up to 256-bit.

File encryption encrypts an individual file so that if it ever ends up in someone else's possession, they will not be able to open it or see the contents. Pretty Good Privacy (PGP) is commonly used to encrypt files. PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

Transport

QUESTION NO: 97

Which of the following refers to an operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements?

A. Trusted OS
B. Distributed operating system
C. Network operating system
D. Real time operating system

Answer: A

Explanation:

Trusted Operating System (TOS) refers to an operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements.

The Common Criteria, combined with the Security Functional Requirements (SFRs) for Labeled Security Protection Profile (LSPP) and Mandatory Access Control(MAC) is the most common set of criteria for trusted operating system design. The Common Criteria is the outcome of a multi-year effort by the governments of the U.S., Canada. United Kingdom, France, Germany- the Netherlands and other countries with an aim to develop a harmonized security criteria for IT products.

Answer option D is incorrect. A real-time operating system (RTOS) is an operating system used to serve real-time application requests. It is an operating system that guarantees a certain capability within a specified time constraint. A key characteristic of an RTOS is the level of its consistency concerning the amount of time it takes to accept and complete an application s task. A real-time OS has an advanced algorithm for scheduling and is more frequently dedicated to a narrow set of applications.

Answer option C is incorrect. The network operating system (NOS) manages resources on a network, offers services to one or more clients, and enables clients to access remote drives as if the drives where on clients own computer. The functions provided by a network operating system are as follows:
• File and print sharing
• Account administration for users
• Security

Answer option B is incorrect. A distributed operating system is the logical aggregation of operating system software over a collection of independent, networked, communicating, and spatially disseminated computational nodes.

QUESTION NO: 98

The Top Level Management contains the Board of Directors (BOD) and the Chief Executive Officer (CEO) or General Manager (GM) or Managing Director (MO) or President. What are the roles of the top level management?

Each correct answer represents a complete solution. Choose all that apply.

A. The Top Level Management decides the objectives, policies, and plans of the organization.
B. The Top Level Management prepares long-term plans of the organization.
C. The Top Level Management has minimum authority and responsibility to take few decisions.
D. The Top Level Management assembles the available resources.

Answer: A,B,D
Explanation:
The Top Level Management contains the Board of Directors (BOD) and the Chief Executive Officer (CEO) or General Manager (GM) or Managing Director (MD) or President. The Board of Directors is the representatives of the Shareholders, i.e. they are selected by the Shareholders of the company. Similarly, the CEO is selected by the Board of Directors of an organization.

Following are the main roles of the top level management:
• The top level management decides the objectives, policies, and plans of the organization.
• The top level management assembles the available resources.
• The top level management does mostly the work of decision making.
• The top level management spends more time in planning and organizing.
• The top level management prepares long-term plans of the organization.
• The top level management has maximum authority and responsibility to take any decision.

QUESTION NO: 99

Compliance is described as dutifulness, obligingness, pliability, tolerance, and tractability. Which of the following are multitude of standards that a project must comply?

Each correct answer represents a complete solution. Choose all that apply.

A. Process compliance
B. Decision oversight
C. Control compliance
D. Standards compliance

Answer: A,B,D
Explanation:
Compliance is described as dutifulness, obligingness, pliability, tolerance, and tractability. Compliance means that an organization must take care of organization's internal regulations, as well as follow the laws of the country and requirements of local legislation and regulations. It may result in conflicts.

Projects must comply with a multitude of standards. Those include the following:
• Standards compliance: Local, state, and federal government
• Process compliance: Audit trails, retention, version control
• Decision oversight: Change Control Board

QUESTION NO: 100

In which of the following level of likelihood is the threat-source highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective?

A. Average
B. Low
C. High
D. Medium

Answer: C
Explanation: Answer option C is correct. Following are the three levels of likelihood:

• High: In this level, the threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
• Medium: In this level the threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
• Low: In this level, the threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

QUESTION NO: 101

John is concerned about internal security threats on the network he administers. He believes that he has taken every reasonable precaution against external threats, but is concerned that he may have gaps in his internal security. Which of the following is the most likely internal threat?

A. Employees not following security policy
B. Privilege Escalation
C. SQL Injection
D. Employees selling sensitive data

Answer: A
Explanation:
Employees may disregard policies, such as policies limiting the use of USB devices or the ability to download programs from the internet. This is the most pervasive internal security threat.
Answer option D is incorrect. Employees selling sensitive data is, of course, possible. However, this scenario is less likely that option A.

Answer option C is incorrect. SQL Injection is most likely accomplished by an external hacker.
Answer option B is incorrect. Privilege escalation can be done by internal or external attackers. However, even with internal attackers, it is far less likely than option B.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

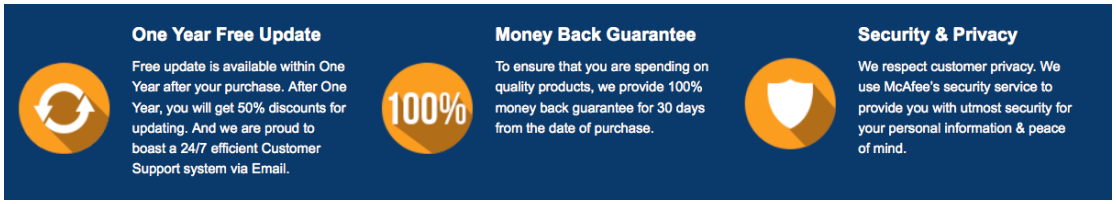
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions