Question #1 *Topic 1*

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

A. Risk acceptance

B. Risk transfer

C. Risk avoidance

D. Risk mitigation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

You have successfully installed an IRM server into your environment. This IRM server will be utilized to protect the company's videos, which are available to all employees but contain sensitive data. You log on to the WSS 3.0 server with administrator permissions and navigate to the Operations section. What option should you now choose so that you can input the RMS server name for the WSS 3.0 server to use?

A. Self-service site management

B. Content databases

C. Information Rights Management

D. Define managed paths

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

You work as a security manager for Qualxiss Inc. Your Company involves OODA loop for resolving and deciding over company issues. You have detected a security breach issue in your company.
Which of the following procedures regarding the breach is involved in the observe phase of the OODA loop?

A. Follow the company security guidelines.

B. Decide an activity based on a hypothesis.

C. Implement an action practically as policies.

D. Consider previous experiences of security breaches.

Suggested Answer: *A*

Community vote distribution

D (100%)

Scorpionking 2 years, 5 months ago

Selected Answer: D

In the OODA loop, the "Observe" phase involves gathering data, information, and intelligence about the situation or issue at hand. It is about comprehending the current state and understanding what is happening.

Out of the given options, the procedure involved in the "Observe" phase is:

D. Consider previous experiences of security breaches.

upvoted 1 times

Question #4 *Topic 1*

How long are cookies in effect if no expiration date is set?

A. Fifteen days

B. Until the session ends.

C. Forever

D. One year

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

You work as a Network Administrator for ABC Inc. The company has a secure wireless network.
However, in the last few days, an attack has been taking place over and over again. This attack is taking advantage of ICMP directed broadcast. To stop this attack, you need to disable ICMP directed broadcasts. Which of the following attacks is taking place?

A. Smurf attack

B. Sniffer attack

C. Cryptographic attack

D. FMS attack

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Which of the following statements are true about Dsniff?
Each correct answer represents a complete solution. Choose two.

A. It is a virus.

B. It contains Trojans.

C. It is antivirus.

D. It is a collection of various hacking tools.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Which of the following are the goals of the cryptographic systems?
Each correct answer represents a complete solution. Choose three.

A. Availability

B. Authentication

C. Confidentiality

D. Integrity

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

John works as an Exchange Administrator for Apple Inc. The company has a Windows 2003 Active Directory domain-based network. The network contains several Windows Server 2003 servers. Three of them have been configured as domain controllers. John complains to the Network Administrator that he is unable to manage group memberships. Which of the following operations master roles is responsible for managing group memberships?

A. PDC emulator

B. Infrastructure master

C. Schema master

D. RID master

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

You are the project manager of SST project. You are in the process of collecting and distributing performance information including status report, progress measurements, and forecasts. Which of the following process are you performing?

A. Perform Quality Control

B. Verify Scope

C. Report Performance

D. Control Scope

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning: nmap -PN -p- -sI
IP_Address_of_Company_Server
He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.
Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

A. Audit policy

B. Antivirus policy

C. Non-disclosure agreement

D. Acceptable use policy

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which of the following protocols provides secured transaction of data between two computers?

A. SSH

B. FTP

C. Telnet

D. RSH

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #12

Topic 1

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. IPChains

B. OpenSSH

C. Stunnel

D. IPTables

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Which of the following concepts represent the three fundamental principles of information security?
Each correct answer represents a complete solution. Choose three.

A. Privacy

B. Availability

C. Integrity

D. Confidentiality

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

You work as a Software Developer for Mansoft Inc. You create an application. You want to use the application to encrypt data. You use the HashAlgorithmType enumeration to specify the algorithm used for generating Message Authentication Code (MAC) in Secure Sockets Layer (SSL) communications.

Which of the following are valid values for HashAlgorithmType enumeration?

Each correct answer represents a part of the solution. Choose all that apply.

A. MD5

B. None

C. DES

D. RSA

E. SHA1

F. 3DES

Suggested Answer: *ABE*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John?
Each correct answer represents a complete solution. Choose all that apply.

A. The virus, used by John, is not in the database of the antivirus program installed on the ser ver.

B. The mutation engine of the virus is generating a new encrypted code.

C. John has created a new virus.

D. John has changed the signature of the virus.

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Which of the following types of virus is capable of changing its signature to avoid detection?

A. Stealth virus

B. Boot sector virus

C. Macro virus

D. Polymorphic virus

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Which of the following protocols can help you get notified in case a router on a network fails?

A. SMTP

B. SNMP

C. TCP

D. ARP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Computer networks and the Internet are the prime mode of Information transfer today. Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Cryptography

B. OODA loop

C. Risk analysis

D. Firewall security

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

In a complex network, Router transfers data packets by observing some form of parameters or metrics provided in the routing table. Which of the following metrics is NOT included in the routing table?

A. Bandwidth

B. Load

C. Delay

D. Frequency

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Mark is implementing security on his e-commerce site. He wants to ensure that a customer sending a message is really the one he claims to be. Which of the following techniques will he use to ensure this?

A. Packet filtering

B. Authentication

C. Firewall

D. Digital signature

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

You work as a Network Administrator for Net World Inc. The company has a TCP/IP-based network.
You have configured an Internet access router on the network. A user complains that he is unable to access a resource on the Web. You know that a bad NAT table entry is causing the issue. You decide to clear all the entries on the table. Which of the following commands will you use?

A. show ip dhcp binding

B. ipconfig /flushdns

C. ipconfig /all

D. clear ip nat translation *

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

You are a Consumer Support Technician. You are helping a user troubleshoot computer-related issues. While troubleshooting the user's computer, you find a malicious program similar to a virus or worm. The program negatively affects the privacy and security of the computer and is capable of damaging the computer. Which of the following alert levels of Windows Defender is set for this program?

A. Low

B. High

C. Severe

D. Medium

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Which of the following provides a credential that can be used by all Kerberos-enabled servers and applications?

A. Remote Authentication Dial In User Service (RADIUS)

B. Internet service provider (ISP)

C. Network Access Point (NAP)

D. Key Distribution Center (KDC)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

You work as an Exchange Administrator for TechWorld Inc. The company has a Windows 2008 Active Directory-based network. The network contains an Exchange Server 2010 organization. The messaging organization contains one Hub Transport server, one Client Access server, and two Mailbox servers.

You are planning to deploy an Edge Transport server in your messaging organization to minimize the attack surface. At which of the following locations will you deploy the Edge Transport server?

A. Active Directory site

B. Intranet

C. Behind the inner firewall of an organization

D. Perimeter network

Suggested Answer: *D*

WillAvery 2 years, 7 months ago

Windows 2008?👀

upvoted 1 times

Question #25 *Topic 1*

You are a Product manager of Marioxiss Inc. Your company management is having a conflict with another company Texasoftg Inc. over an issue of security policies. Your legal advisor has prepared a document that includes the negotiation of views for both the companies. This solution is supposed to be the key for conflict resolution. Which of the following are the forms of conflict resolution that have been employed by the legal advisor?
Each correct answer represents a complete solution. Choose all that apply.

A. Orientation

B. Mediation

C. Negotiation

D. Arbitration

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

A. Physical configuration audit

B. Configuration control

C. Functional configuration audit

D. Configuration identification

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Availability Management allows organizations to sustain the IT service availability to support the business at a justifiable cost. Which of the following elements of Availability Management is used to perform at an agreed level over a period of time?
Each correct answer represents a part of the solution. Choose all that apply.

A. Maintainability

B. Resilience

C. Error control

D. Recoverability

E. Reliability

F. Security

G. Serviceability

Suggested Answer: *ABDEFG*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

Your company is going to add wireless connectivity to the existing LAN. You have concerns about the security of the wireless access and wish to implement encryption. Which of the following would be the best choice for you to use?

A. WAP

B. WEP

C. DES

D. PKI

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Which of the following tools can be used to perform tasks such as Windows password cracking Windows enumeration, and VoIP session sniffing?

A. John the Ripper

B. Obiwan

C. Cain

D. L0phtcrack

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

A. NetBus

B. EliteWrap

C. Trojan Man

D. Tiny

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

What does a firewall check to prevent certain ports and applications from getting the packets into an Enterprise?

A. The application layer port numbers and the transport layer headers

B. The presentation layer headers and the session layer port numbers

C. The network layer headers and the session layer port numbers

D. The transport layer port numbers and the application layer headers

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

A. Install a DMZ firewall

B. Enable verbose logging on the firewall

C. Install a host-based IDS

D. Install a network-based IDS

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

The SALES folder has a file named XFILE.DOC that contains critical information about your company. This folder resides on an NTFS volume. The company's Senior Sales Manager asks you to provide security for that file. You make a backup of that file and keep it in a locked cupboard, and then you deny access on the file for the Sales group. John, a member of the Sales group, accidentally deletes that file. You have verified that John is not a member of any other group.

Although you restore the file from backup, you are confused how John was able to delete the file despite having no access to that file.

What is the most likely cause?

A. The Sales group has the Full Control permission on the SALES folder.

B. The Deny Access permission does not work on files.

C. The Deny Access permission does not restrict the deletion of files.

D. John is a member of another group having the Full Control permission on that file.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want to the information security policies.
Which of the following are its significant steps?
Each correct answer represents a complete solution. Choose two.

A. Awareness and Training Material Effectiveness

B. Awareness and Training Material Development

C. Awareness and Training Material Implementation

D. Awareness and Training Program Design

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

You are the project manager of the HHH Project. The stakeholders for this project are scattered across the world and you need a method to promote interaction. You determine that a Web conferencing software would be the most cost effective solution. The stakeholders can watch a slide show while you walk them through the project details. The stakeholders can hear you, ask questions via a chat software, and post concerns. What is the danger in this presentation?

A. 55 percent of all communication is nonverbal and this approach does not provide non-verbal communications.

B. The technology is not proven as reliable.

C. The stakeholders won't really see you.

D. The stakeholders are not required to attend the entire session.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

A Cisco Unified Wireless Network has an AP that does not rely on the central control device of the network. Which type of AP has this characteristic?

A. Lightweight AP

B. Rogue AP

C. LWAPP

D. Autonomous AP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Which of the following monitors program activities and modifies malicious activities on a system?

A. Back door

B. HIDS

C. RADIUS

D. NIDS

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Which of the following statements is not true about a digital certificate?

A. It is used with both public key encryption and private key encryption.

B. It is used with private key encryption.

C. It is neither used with public key encryption nor with private key encryption.

D. It is used with public key encryption.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Cross-Site Request Forgery

B. Code injection attack

C. Cross-Site Scripting attack

D. Command injection attack

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

A. Electronic Communications Privacy Act of 1986

B. Economic Espionage Act of 1996

C. Computer Fraud and Abuse Act

D. Wiretap Act

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Which of the following does an anti-virus program update regularly from its manufacturer's Web site?

A. Hotfixes

B. Definition

C. Service packs

D. Permissions

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 domainbased network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company's security policy, you apply Windows firewall setting to the computers on the network. Now, you are troubleshooting a connectivity problem that might be caused by Windows firewall. What will you do to identify connections that Windows firewall allows or blocks?

A. Configure Network address translation (NAT).

B. Disable Windows firewall logging.

C. Configure Internet Protocol Security (IPSec).

D. Enable Windows firewall logging.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #43

Topic 1

Hardening a system is one of the practical methods of securing a computer system. Which of the following techniques is used for hardening a computer system?

A. Disabling all user accounts

B. Applying egress filtering

C. Applying Access Control List (ACL)

D. Applying a patch to the OS kernel

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #44

Topic 1

You work as a security manager in Mariotiss Inc. Your enterprise has been facing network and software security threats since a few months. You want to renew your current security policies and management to enhance the safety of your information systems. Which of the following is the best practice to initiate the renewal process from the lowest level with the least managerial effort?

A. Start the Incident handling process.

B. Change the entire security policy.

C. Perform an IT audit.

D. Switch to a new network infrastructure.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. A risk probability-impact matrix

B. Quantitative risk analysis

C. Qualitative risk analysis

D. Seven risk responses

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

You are concerned about outside attackers penetrating your network via your company Web server.
You wish to place your Web server between two firewalls
One firewall between the Web server and the outside world
The other between the Web server and your network
What is this called?

A. IDS

B. SPI firewall

C. DMZ

D. Application Gateway firewall

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

A. Discretionary Access Control (DAC)

B. Role Based Access Control (RBAC)

C. Access Control List (ACL)

D. Mandatory Access Control (MAC)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

Which of the following types of authentications supported by OSPF?
Each correct answer represents a complete solution. Choose three.

A. MD5 authentication

B. Simple password authentication

C. Null authentication

D. Kerberos v5 authentication

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Which of the following are the differences between routed protocols and routing protocols?
Each correct answer represents a complete solution. Choose two.

A. A routing protocol is configured on an interface and decides the method of packet delivery.

B. A routing protocol decides the path for a packet through the network.

C. A routed protocol is configured on an interface and decides how a packet will be delivered.

D. A routed protocol works on the transport layer of the OSI model.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #50

Topic 1

Which of the following algorithms produce 160-bit hash values?
Each correct answer represents a complete solution. Choose two.

A. MD2

B. MD5

C. SHA-1

D. SHA-0

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #51

Topic 1

Your Company is receiving false and abusive e-mails from the e-mail address of your partner company. When you complain, the partner company tells you that they have never sent any such e-mails. Which of the following types of cyber crimes involves this form of network attack?

A. Cyber squatting

B. Cyber Stalking

C. Man-in-the-middle attack

D. Spoofing

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

SIMULATION -
Fill in the blank with the appropriate layer name.
The Network layer of the OSI model corresponds to the______ layer of the TCP/IP model.

Suggested Answer: *Internet*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

You switch on your mobile Bluetooth device to transfer data to another Bluetooth device. Which of the following Information assurance pillars ensures that the data transfer is being performed with the targeted authorized Bluetooth device and not with any other or unauthorized device?

A. Data integrity

B. Confidentiality

C. Authentication

D. Non-repudiation

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #54

Topic 1

Which of the following statements about asymmetric encryption are true?
Each correct answer represents a complete solution. Choose two.

A. Asymmetric encryption is faster as compared to symmetric encryption.

B. Asymmetric encryption uses a public key and a private key pair for data encryption.

C. In asymmetric encryption, only one key is needed to encrypt and decrypt data.

D. In asymmetric encryption, the public key is distributed and the private key is available only to the recipient of the message.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #55 Topic 1

Which of the following terms is used for a router that filters traffic before it is passed to the firewall?

A. Screened host

B. Demilitarized zone (DMZ)

C. Honey pot

D. Bastion host

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #56

Topic 1

Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?

A. F936.28A1.5BCD.DEFA

B. A3-07-B9-E3-BC-F9

C. 1011-0011-1010-1110-1100-0001

D. 132.298.1.23

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

Which of the following provide data confidentiality services by encrypting the data sent between wireless systems?
Each correct answer represents a complete solution. Choose two.

A. MS-CHAP v2

B. WEP

C. PAP

D. WPA

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

You have decided to implement an intrusion detection system on your network. You primarily are interested in the IDS being able to recognized known attack techniques. Which type of IDS should you choose?

A. Signature Based

B. Passive

C. Active

D. Anomaly Based

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #59

Topic 1

You want to ensure that everyone who sends you an email should encrypt it. However you do not wish to exchange individual keys with all people who send you emails. In order to accomplish this goal which of the following should you choose?

A. DES

B. AES

C. Symmetric Encryption

D. Public Key encryption

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #60

Topic 1

You have been assigned the task of selecting a hash algorithm. The algorithm will be specifically used to ensure the integrity of certain sensitive files. It must use a 128 bit hash value. Which of the following should you use?

A. SHA

B. AES

C. MD5

D. DES

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

Which of the following are some of the parts of a project plan?
Each correct answer represents a complete solution. Choose all that apply.

A. Risk identification

B. Project schedule

C. Team members list

D. Risk analysis

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

Which of the following are core TCP/IP protocols that can be implemented with Windows NT to connect computers and internetworks?
Each correct answer represents a complete solution. Choose all that apply.

A. Address Resolution Protocol (ARP)

B. Network Link Protocol (NWLink)

C. User Datagram Protocol (UDP)

D. Internet Control Message Protocol (ICMP)

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

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 the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Windows

B. Red Hat

C. Solaris

D. Knoppix

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

Which of the following protocols are used by Network Attached Storage (NAS)?
Each correct answer represents a complete solution. Choose all that apply.

A. Apple Filing Protocol (AFP)

B. Server Message Block (SMB)

C. Network File System (NFS)

D. Distributed file system (Dfs)

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

A. Containment

B. Identification

C. Preparation

D. Eradication

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

You are working on your computer system with Linux Operating system. After working for a few hours, the hard disk goes to the inactive state (sleep). You try to restart the system and check the power circuits. You later discover that the hard disk has crashed. Which of the following precaution methods should you apply to keep your computer safe from such issues?

A. Use Incident handling

B. Use OODA loop

C. Use Information assurance

D. Use SMART model.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

A. Containment

B. Preparation

C. Recovery

D. Identification

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

You are the security manager of Microliss Inc. Your enterprise uses a wireless network infrastructure with access points ranging 150-350 feet. The employees using the network complain that their passwords and important official information have been traced. You discover the following clues:
The information has proved beneficial to another company.
The other company is located about 340 feet away from your office.
The other company is also using wireless network.
The bandwidth of your network has degraded to a great extent.
Which of the following methods of attack has been used?

A. A piggybacking attack has been performed.

B. The information is traced using Bluebugging.

C. A DOS attack has been performed.

D. A worm has exported the information.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

Which of the following options cannot be accessed from Windows Update?

A. Restore Hidden Updates

B. Check for Updates

C. View Update History

D. View AntiVirus Software Update

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

A. Denial-of-Service

B. Eavesdropping

C. Spoofing

D. Packet manipulation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

John works as a security manager in Mariotx.Inc. He has been tasked to resolve a network attack issue. To solve the problem, he first examines the critical information about the attacker's interaction to the network environment. He prepares a past record and behavioral document of the attack to find a direction of the solution. Then he decides to perform an action based on the previous hypothesis and takes the appropriate action against the attack. Which of the following strategies has John followed?

A. Maneuver warfare

B. Control theory

C. SWOT Analysis

D. OODA loop

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

Which of the following service provider classes is used to create a digital signature?

A. RC2CryptoServiceProvider

B. RNGCryptoServiceProvider

C. DESCryptoServiceProvider

D. SHA1CryptoServiceProvider

E. MD5CryptoServiceProvider

F. DSACryptoServiceProvider

Suggested Answer: *F*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

Which of the following is a pillar of Information Assurance CIA triad?

A. Integrity

B. Affiliation

C. Accessibility

D. Isolation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

Adam, a novice Web user is getting large amount of unsolicited commercial emails on his email address. He suspects that the emails he is receiving are the Spam. Which of the following steps will he take to stop the Spam?
Each correct answer represents a complete solution. Choose all that apply.

A. Forward a copy of the spam to the ISP to make the ISP conscious of the spam.

B. Send an email to the domain administrator responsible for the initiating IP address.

C. Report the incident to the FTC (The U.S. Federal Trade Commission) by sending a copy of the spam message.

D. Close existing email account and open new email account.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

Computer networks and the Internet are the prime mode of Information transfer today. Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Risk analysis

B. Firewall security

C. OODA loop

D. Cryptography

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #76

Topic 1

You work as an executive manager for Mariotx.Inc. You entered into a business contract with a firm called Helfixnet.Inc. You passed on the contract details to Helfixnet.Inc and also got an acceptance approval. You later find that Helfixnet.Inc is violating the rules of the contract and they claim that they had never entered into any contract with Mariotx.Inc when asked. Which of the following directives of Information Assurance can you apply to ensure prevention from such issues?

A. Confidentiality

B. Non-repudiation

C. Data integrity

D. Data availability

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #77

Topic 1

You work in an enterprise as a Network Engineer. Your enterprise has a secure internal network.
You want to apply an additional network packet filtering device that is intermediate to your enterprise's internal network and the outer network (internet). Which of the following network zones will you create to accomplish this task?

A. Autonomous system area (AS)

B. Demilitarized zone (DMZ)

C. Border network area

D. Site network area

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

The security of a computer against the unauthorized usage largely depends upon the efficiency of the applied access control method. Which of the following statements are true about a computer access control method?
Each correct answer represents a complete solution. Choose all that apply.

A. It can be based upon fingerprint or eye recognition.

B. It can be time-synchronous.

C. It provides security against the virus attacks.

D. It provides security against Eavesdropping.

E. It checks the authenticity of a person.

F. It is used to encrypt a message before transmitting it on a network.

Suggested Answer: *ABE*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer?

A. IPLog

B. Snort

C. Timbersee

D. Swatch

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

Which of the following factors determine the strength of the encryption?

A. Character-set encoding

B. Length of the key

C. Operating system

D. Ease of use

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #81

Topic 1

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Public key

B. Digital certificates

C. Twofish

D. RSA

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

You work as a SharePoint Administrator for TechWorld Inc. You must protect your SharePoint server farm from viruses that are accidentally uploaded to the SharePoint libraries. You have installed antivirus software that is designed for use with Windows SharePoint server. You have logged on to the Central Administration site.
How can you configure the SharePoint site so that the document libraries are protected?

A. SharePoint does not support antivirus solutions.

B. Restrict users to read only on document libraries.

C. Choose the Scan documents on upload option in the antivirus settings.

D. Require all documents to be scanned on the local PC before uploading to the SharePoint sit e.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #83

Topic 1

Which of the following are application layer protocols of Internet protocol (IP) suite?
Each correct answer represents a complete solution. Choose two.

A. IGP

B. IGRP

C. Telnet

D. SMTP

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

You are the Security Consultant and have been contacted by a client regarding their encryption and hashing algorithms. Their in-house network administrator tells you that their current hashing algorithm is an older one with known weaknesses and is not collision resistant. Which algorithm are they most likely using for hashing?

A. PKI

B. MD5

C. SHA

D. Kerberos

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

Which of the following processes is accountable for monitoring an IT Service and detecting when the performance drops beneath adequate limits?

A. Service Asset and Configuration Management

B. Service Request Management

C. Event Management

D. Service Level Management

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #86

Topic 1

What does Wireless Transport Layer Security (WTLS) provide for wireless devices?
Each correct answer represents a complete solution. Choose all that apply.

A. Data integrity

B. Authentication

C. Encryption

D. Bandwidth

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

You work as a project manager for TYU project. You are planning for risk mitigation. You need to identify the risks that will need a more in-depth analysis. Which of the following activities will help you in this?

A. Quantitative analysis

B. Qualitative analysis

C. Estimate activity duration

D. Risk identification

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

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

A. A stub is a program that simulates a calling unit, and a driver is a program that simulates a called unit.

B. In unit testing, each independent unit of an application is tested separately.

C. In integration testing, a developer combines two units that have already been tested into a component.

D. The bottom-up approach to integration testing helps minimize the need for stubs.

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 1*

Which of the following protocols is used to provide remote monitoring and administration to network management machines on the network? The management machines will use this protocol to collect information for network monitoring. At times, the protocol can also be used for remote configuration.

A. NNTP

B. Telnet

C. SSH

D. SNMP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 1*

In which type of access control do user ID and password system come under?

A. Physical

B. Power

C. Technical

D. Administrative

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

You are the project manager of a new project in your organization. You and the project team have identified the project risks, completed risk analysis, and are planning the most appropriate risk responses. Which of the following tools is most effective to choose the most appropriate risk response?

A. Project network diagrams

B. Delphi Technique

C. Decision tree analysis

D. Cause-and-effect diagrams

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

Which of the following protocols work at the Network layer of the OSI model?

A. Internet Group Management Protocol (IGMP)

B. Simple Network Management Protocol (SNMP)

C. Routing Information Protocol (RIP)

D. File Transfer Protocol (FTP)

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

A. The Configuration Manager

B. The Supplier Manager

C. The IT Service Continuity Manager

D. The Service Catalogue Manager

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 1*

Andrew works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network contains five Windows 2008 member servers and 120 Windows XP Professional client computers. Andrew is concerned about the member servers that are not meeting the security requirements as mentioned in the security policy of the company. Andrew wants to compare the current security settings of the member servers with the security template that is configured according to the security policy of the company. Which of the following tools will Andrew use to accomplish this?

A. Security Configuration and Analysis Tool

B. Active Directory Migration Tool (ADMT)

C. Task Manager

D. Group Policy Management Console (GPMC)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #95 *Topic 1*

Sam is creating an e-commerce site. He wants a simple security solution that does not require each customer to have an individual key. Which of the following encryption methods will he use?

A. S/MIME

B. PGP

C. Asymmetric encryption

D. Symmetric encryption

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

Which of the following are the examples of administrative controls?
Each correct answer represents a complete solution. Choose all that apply.

A. Data Backup

B. Security policy

C. Security awareness training

D. Auditing

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #97 *Topic 1*

Which of the following statements about Secure Shell (SSH) are true?
Each correct answer represents a complete solution. Choose three.

A. It was designed as a replacement for TELNET and other insecure shells.

B. It is a network protocol used primarily on Linux and Unix based systems.

C. It allows data to be exchanged using a secure channel between two networked devices.

D. It is the core routing protocol of the Internet.

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #98 *Topic 1*

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions, which is available to the Internet. Which of the following security threats may occur if DMZ protocol attacks are performed?
Each correct answer represents a complete solution. Choose all that apply.

A. Attacker can exploit any protocol used to go into the internal network or intranet of the com pany.

B. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

C. Attacker can gain access to the Web server in a DMZ and exploit the database.

D. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 1*

You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

A. Quantitative risk analysis

B. Risk audits

C. Qualitative risk analysis

D. Requested changes

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 1*

Security is responsible for well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security?
Each correct answer represents a complete solution. Choose all that apply.

A. Availability

B. Confidentiality

C. Confidentiality

D. Authenticity

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 1*

Which of the following techniques allows an attacker to take network traffic coming towards a host at one port and redirect it from that host to another host?

A. Blackbox testing

B. Firewalking

C. Brainstorming

D. Port redirection

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 1*

Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?

A. Disaster Invocation Guideline

B. Business Continuity Strategy

C. Index of Disaster-Relevant Information

D. Availability/ ITSCM/ Security Testing Schedule

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 1*

Your network utilizes a coax cable for connections between various network segments. Your predecessor made sure none of the coax cables were in an exposed area that could easily be accessed. This caused the use of significant extra cabling. Why do you think this was done?

A. This was an error you should correct. It wastes the cable and may make maintenance more difficult.

B. He was concerned about wireless interception of data.

C. He was concerned about electromagnetic emanation being used to gather data.

D. He was concerned about vampire taps.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #104 *Topic 1*

Which of the following is used to authenticate asymmetric keys?

A. Digital signature

B. MAC Address

C. Password

D. Demilitarized zone (DMZ)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #105

Topic 1

Tom works as the project manager for BlueWell Inc. He is working with his project to ensure timely and appropriate generation, retrieval, distribution, collection, storage, and ultimate disposition of project information. What is the process in which Tom is working?

A. Stakeholder expectation management

B. Stakeholder analysis

C. Work performance measurement

D. Project communication management

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #106 *Topic 1*

Which of the following is a remote access protocol that supports encryption?

A. PPP

B. SLIP

C. UDP

D. SNMP

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #107 *Topic 1*

Which of the following processes is described in the statement below?
"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Perform Quantitative Risk Analysis

B. Perform Qualitative Risk Analysis

C. Monitor and Control Risks

D. Identify Risks

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #108 *Topic 1*

Which of the following objects in an Active Directory serve as security principles?
Each correct answer represents a part of the solution. Choose all that apply.

A. User accounts

B. Organizational units (OUs)

C. Computer accounts

D. Groups

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #109 *Topic 1*

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication

B. Confidentiality

C. Integrity

D. Non-repudiation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #110 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. On the We-are-secure login page, he enters ='or''=' as a username and successfully logs in to the user page of the Web site. The We-are-secure login page is vulnerable to a __________.

A. Social engineering

B. Smurf DoS

C. Brute force

D. Ping flood attack

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #111 *Topic 1*

Which of the following is an organization that defines standards for anti-virus software?

A. ICSA

B. IETF

C. IIS

D. IEEE

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #112 *Topic 1*

Which of the following types of attacks cannot be prevented by technical measures only?

A. Social engineering

B. Smurf DoS

C. Brute force

D. Ping flood attack

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #113

Topic 1

Which of the following cryptographic algorithms uses a single key to encrypt and decrypt data?

A. Asymmetric

B. Symmetric

C. Numeric

D. Hashing

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #114 *Topic 1*

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

A. Corrective controls

B. Detective controls

C. Safeguards

D. Preventive controls

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #115 *Topic 1*

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

A. UDP is an unreliable protocol.

B. FTP uses a UDP port for communication.

C. UDP is a connectionless protocol.

D. TFTP uses a UDP port for communication.

E. UDP works at the data-link layer of the OSI model.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #116 *Topic 1*

You have an antivirus program for your network. It is dependent upon using lists of known viruses. What is this type of scan called?

A. Heuristic

B. Fixed List

C. Dictionary

D. Host Based

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #117 *Topic 1*

Which Wireless network standard operates at 2.4 GHz and transfers data at a rate of 54 Mbps?

A. 802.11a

B. 802.11n

C. 802.11b

D. 802.11g

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #118 *Topic 1*

Which U.S. government agency is responsible for establishing standards concerning cryptography for nonmilitary use?

A. American Bankers Association

B. Central Security Service (CSS)

C. National Institute of Standards and Technology (NIST)

D. International Telecommunications Union

E. Request for Comments (RFC)

F. National Security Agency (NSA)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #119 *Topic 1*

Which of the following is the most secure place to host a server that will be accessed publicly through the Internet?

A. A DNS Zone

B. An Intranet

C. A demilitarized zone (DMZ)

D. A stub zone

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #120 *Topic 1*

Which of the following tools are used to determine the hop counts of an IP packet?
Each correct answer represents a complete solution. Choose two.

A. Netstat

B. Ping

C. TRACERT

D. IPCONFIG

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #121 *Topic 1*

Under the SMART scheme, the Predictive Failure Analysis Technology is used to determine the failure or crash for which of the following parts of a computer system?

A. Operating System

B. Hard Disc drive

C. Software

D. Internet Browser

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #122 *Topic 1*

Which of the following books is used to examine integrity and availability?

A. Brown Book

B. Red Book

C. Purple Book

D. Orange Book

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #123 *Topic 1*

The Project Risk Management knowledge area focuses on which of the following processes?
Each correct answer represents a complete solution. Choose all that apply.

A. Risk Management Planning

B. Quantitative Risk Analysis

C. Potential Risk Monitoring

D. Risk Monitoring and Control

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #124 *Topic 1*

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system. He wants to sniff the weare- secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?

A. Hunt

B. IPChains

C. Ethercap

D. Tripwire

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #125

Topic 1

Which of the following cryptographic algorithm uses public key and private key to encrypt or decrypt data?

A. Symmetric

B. Numeric

C. Hashing

D. Asymmetric

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #126 *Topic 1*

You work as a Security manager for Qualoxizz Inc. Your company has number of network switches in the site network infrastructure. Which of the following actions will you perform to ensure the security of the switches in your company?

A. Set long session timeouts.

B. Open up all the unused management ports.

C. Set similar passwords for each management port.

D. Ignore usage of the default account settings.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #127 *Topic 1*

Key Distribution Center is used in which authentication method?

A. Multi-factor

B. Smart cards

C. Biometrics

D. Security tokens

E. Kerberos

F. Challenge Handshake Authentication Protocol

Suggested Answer: *E*

Currently there are no comments in this discussion, be the first to comment!

Question #128 *Topic 1*

Which of the following statements about digital signature is true?

A. Digital signature is required for an e-mail message to get through a firewall.

B. Digital signature verifies the identity of the person who applies it to a document.

C. Digital signature decrypts the contents of documents.

D. Digital signature compresses the message to which it is applied.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #129 *Topic 1*

Which of the following is a valid IP address for class B Networks?

A. 172.157.88.3

B. 80.33.5.7

C. 212.136.45.8

D. 225.128.98.7

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #130 *Topic 1*

The MBR of a hard disk is a collection of boot records that contain disk information such as disk architecture, cluster size, and so on. The main work of the MBR is to locate and run necessary operating system files that are required to run a hard disk. In the context of the operating system, MBR is also known as the boot loader. Which of the following viruses can infect the MBR of a hard disk?
Each correct answer represents a complete solution. Choose two.

A. Boot sector

B. Multipartite

C. File

D. Stealth

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #131 *Topic 1*

You work as a security manager for hackoxiss Inc. The company consists of a perimeter network as its internal network. A number of ethical hackers are employed in the company. You are getting complaints that some employees of the company are trying to intrude other systems on the outer network (Internet). In which of the following ways will you secure the internal as well as the outer network?

A. Deny the access of outer users to internal network.

B. Use distributed firewalls.

C. Deny the access of internal users to outer network.

D. Configure ACL on your company's router.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #132 *Topic 1*

Which project management risk event would you be using if you changed the sequence of activities to reduce the probability of the project being delayed?

A. Enhancing

B. Withdrawal

C. Exploiting

D. Avoidance

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #133

Topic 1

You work as a Software Developer for Mansoft Inc. You have participated in the customization of a previously developed Configuration Management Application Block (CMAB) that manages an application configuration setting in multiple data stores. Based on requirements, you have extended the CMAB to read and write configuration data to and from an Oracle database. You need to create a unit test strategy. Which of the following steps would you include in a unit test of the CMAB?

Each correct answer represents a part of the solution. Choose all that apply.

A. Perform White box testing

B. Regression test the existing functionality

C. Execute Use cases of the application

D. Perform Stress testing

E. Review the implementation

Suggested Answer: *ABE*

Currently there are no comments in this discussion, be the first to comment!

Question #134 *Topic 1*

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer?
Each correct answer represents a complete solution. Choose two.

A. Attacker can use the Ping Flood DoS attack if WZC is used.

B. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.

C. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #135 *Topic 1*

Which of the following is not needed for effective procurement planning?

A. Activity resource management

B. Project schedule

C. Cost baseline

D. Quality risk analysis

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #136 *Topic 1*

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

A. By examining your firewall logs.

B. By examining your domain controller server logs.

C. By setting up a DMZ.

D. You cannot, you need an IDS.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #137 *Topic 1*

Which of the following network connectivity devices translates one protocol into another and is used to connect dissimilar network technologies?

A. Hub

B. Firewall

C. Bridge

D. Gateway

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #138

Topic 1

Kelly is the project manager of the NNQ Project for her company. This project will last for one year and has a budget of $350,000. Kelly is working with her project team and subject matter experts to begin the risk response planning process. When the project manager begins the plan risk response process, what two inputs will she need?

A. Risk register and the results of risk analysis

B. Risk register and the risk response plan

C. Risk register and the risk management plan

D. Risk register and power to assign risk responses

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #139 *Topic 1*

You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus.

Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

A. Recovery

B. Identification

C. Containment

D. Eradication

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #140 *Topic 1*

Which of the following statements are TRUE regarding asymmetric encryption and symmetric encryption? Each correct answer represents a complete solution. Choose all that apply.

A. Data Encryption Standard (DES) is a symmetric encryption key algorithm.

B. In symmetric encryption, the secret key is available only to the recipient of the message.

C. Symmetric encryption is commonly used when a message sender needs to encrypt a large amount of data.

D. Asymmetric encryption uses a public key and a private key pair for data encryption.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #141 *Topic 1*

The ATM of a bank is robbed by breaking the ATM machine. Which of the following physical security devices can now be used for verification and historical analysis of the ATM robbery?

A. Biometric devices

B. Intrusion detection systems

C. Key card

D. CCTV Cameras

Suggested Answer: *D -*

Currently there are no comments in this discussion, be the first to comment!

Question #142 *Topic 2*

What is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.

B. A CI that has the same essential functionality as another CI but a bit different in some small manner.

C. A CI that particularly refers to a hardware specification.

D. A CI that particularly refers to a software version.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #143 *Topic 2*

SIMULATION -

Fill in the blank with the appropriate value. SHA-1 produces a ______-bit message digest.

Suggested Answer: *SHA-1 produces a 160 -bit message digest*

Currently there are no comments in this discussion, be the first to comment!

Question #144 *Topic 2*

Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Trademark laws

B. Patent laws

C. Copyright laws

D. Code Security law

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #145 *Topic 2*

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory domain-based network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company's security policy, you want to apply Windows firewall setting to all the computers in the domain to improve security.
Which of the following is the fastest and the most effective way to accomplish the task?

A. Apply firewall settings manually.

B. Apply firewall settings on the domain controller of the domain.

C. Use group policy to apply firewall settings.

D. Use a batch file to apply firewall setting.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #146 *Topic 2*

You work as a Network Administrator for Infosec Inc. You find that not only have security applications running on the server, including software firewalls, anti-virus programs, and anti-spyware programs been disabled, but anti-virus and anti-spyware definitions have also been deleted. You suspect that this situation has arisen due to malware infection. Which of the following types of malware is the most likely cause of the issue?

A. Whack-A-Mole

B. FireKiller 2000

C. Beast

D. SubSeven

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #147 *Topic 2*

Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?
Each correct answer represents a complete solution. Choose all that apply.

A. Slack space

B. Unused Sectors

C. Dumb space

D. Hidden partition

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #148 *Topic 2*

Firekiller 2000 is an example of a _________.

A. DoS attack Trojan

B. Data sending Trojan

C. Remote access Trojan

D. Security software disabler Trojan

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #149 Topic 2

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

A. Availability

B. Integrity

C. Confidentiality

D. Non-repudiation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #150 *Topic 2*

You work as a Computer Hacking Forensic Investigator for SecureNet Inc. You want to investigate Cross-Site Scripting attack on your company's Website. Which of the following methods of investigation can you use to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.

B. Look at the Web servers logs and normal traffic logging.

C. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.

D. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #151 *Topic 2*

You work as a Software Developer for Mansoft Inc. You, together with a team, develop a distributed application that processes orders from multiple types of clients. The application uses SQL Server to store data for all orders. The application does not implement any custom performance counters. After the application is deployed to production, it must be monitored for performance spikes. What will you do to monitor performance spikes in the application in a deployment environment?
Each correct answer represents a part of the solution. Choose all that apply.

A. Use SQL Profiler

B. Use CLR Profiler

C. Use Windows System Monitor

D. Use Microsoft Operations Manager

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #152

Topic 2

Which of the following tools can be used for stress testing of a Web server?
Each correct answer represents a complete solution. Choose two.

A. Internet bots

B. Spyware

C. Scripts

D. Anti-virus software

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #153 *Topic 2*

You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project?
Each correct answer represents a complete solution. Choose all that apply.

A. It provides the risk analysis of project configurations.

B. It provides object, orient, decide and act strategy.

C. It provides the versions for network devices.

D. It provides a live documentation of the project.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #154

Topic 2

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He analyzes that the company has blocked all ports except port 80.
Which of the following attacking methods can he use to send the dangerous software protocols?

A. HTTP tunneling

B. URL obfuscation

C. Banner grabbing

D. MAC spoofing

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #155 *Topic 2*

You work as a Consumer Support Technician for ABC Inc. The company provides troubleshooting support to users. You are troubleshooting a computer of a user who is working on Windows Vista.

He reports that his sensitive data is being accessed by someone because of security vulnerability in the component of Windows Vista. Which of the following features of Windows Security Center will you configure to save the user's data?

A. Malware protection

B. Automatic updating

C. Firewall

D. Other security settings

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #156 *Topic 2*

Which of the following types of cipher encrypts alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword?

A. Block cipher

B. Transposition cipher

C. Vigen re cipher

D. Stream cipher

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #157 *Topic 2*

You work as a Network Administrator for McRoberts Inc. You are required to upgrade a client computer on the company's network to Windows Vista Ultimate. During installation, the computer stops responding, and the screen does not change. What is the most likely cause?

A. Antivirus software is running on the computer.

B. You have provided an improper product key.

C. The computer is running a driver that is incompatible with Vista.

D. The computer has a hardware device that is incompatible with Vista.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #158 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. John wants to redirect all TCP port 80 traffic to UDP port 40, so that he can bypass the firewall of the We-are-secure server. Which of the following tools will John use to accomplish his task?

A. PsList

B. Fpipe

C. Cain

D. PsExec

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!