GIAC

Exam GISF

GIAC Information Security Fundamentals

Version: 6.1

[Total Questions: 333]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	149
Topic 2: Volume B	150
Topic 3: Volume C	34

Topic 1, Volume A

Question No : 1 - (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

Answer: A,B,C

Question No : 2 - (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)

Answer: A

Question No : 3 - (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

Answer: C

Question No : 4 - (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

Answer: B,D

Question No : 5 - (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.

Answer: A,C,D

Question No : 6 - (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

Answer: B

Question No : 7 - (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

Answer: C

Question No : 8 - (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.

Answer: D

Question No : 9 - (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

Answer: D

Question No : 10 - (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

Answer: B,C

Question No : 11 - (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

Answer: B,C,D

Question No : 12 - (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.

Answer: B,C

Question No : 13 - (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

Answer: D

Question No : 14 - (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.

Answer: A,C,D

Question No : 15 - (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

Answer: A,B,D,E,F,G

Question No : 16 - (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

Answer: D

Question No : 17 - (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

Answer: A

Question No : 18 - (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

Answer: B

Question No : 19 - (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.

Answer: D

Question No : 20 - (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

Answer: D

Question No : 21 - (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

Answer: D

Question No : 22 - (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

Answer: C

Question No : 23 - (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

Answer: D

Question No : 24 - (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)

Answer: A,C,D

Question No : 25 - (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)

Answer: A,B,C

Question No : 26 - (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.

Answer: B

Question No : 27 - (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

Answer: A,B

Question No : 28 - (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.

Answer: B,D

Question No : 29 - (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

Answer: D

Question No : 30 - (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

Answer: C

Question No : 31 - (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

Answer: D

Question No : 32 - (Topic 1)

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

A. SSH
B. FTP
C. Telnet
D. RSH

Answer: A

Question No : 33 - (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.

Answer: C

Question No : 34 - (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

Answer: A

Question No : 35 - (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.