GIAC

Exam GSLC

GIAC Security Leadership Certification (GSLC)

Version: 6.0

[Total Questions: 567]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	139
Topic 2: Volume B	149
Topic 3: Volume C	144
Topic 4: Volume D	135

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following domains of the DNS hierarchy consists of categories found at the end of domain names, such as .com or .uk and divides the domains into organizations (.org), businesses (.com), countries (.uk), and other categories?

A. Top-level domain
B. Root-level domain
C. Second level domain
D. Name server

Answer: A

Question No : 2 - (Topic 1)

John is a merchant. He has set up a LAN in his office. Some important files are deleted as a result of virus attack. John wants to ensure that it does not happen again. What will he use to protect his data from virus?

A. Backup
B. Symmetric encryption
C. Firewall
D. Antivirus

Answer: D

Question No : 3 - (Topic 1)

Which of the following are the examples of administrative controls?

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

A. Security policy
B. Auditing
C. Security awareness training
D. Data Backup

Answer: A,C

Question No : 4 - (Topic 1)

Which of the following viruses/worms uses the buffer overflow attack?

A. Code red worm
B. Klez worm
C. Nimda virus
D. Chernobyl (CIH) virus

Answer: A

Question No : 5 - (Topic 1)

John works as a Website Administrator in ABC Inc. The company has to set a privacy policy on all the computers. The policy requires John to restrict only third party cookies that do not have a compact private policy or that use personally identifiable information without a user's implicit consent. He reports to the Technical Support Executive that he wants to set the policy. The Technical Support Executive asks him to configure the settings in the Privacy tab page. Which of the following privacy settings will John use to accomplish the task?

A. High
B. Low
C. Block All Cookies
D. The policy cannot be set.

Answer: B

Question No : 6 - (Topic 1)

Which of the following tools works both as an encryption-cracking tool and as a keylogger?

A. Magic Lantern
B. KeyGhost Keylogger
C. Alchemy Remote Executor

D. SocketShield

Answer: A

Question No : 7 - (Topic 1)

Which of the following statements about Encapsulating Security Payload (ESP) are true?

Each correct answer represents a complete solution. Choose two.

A. It is an IPSec protocol.
B. It is a text-based communication protocol.
C. It uses TCP port 22 as the default port and operates at the application layer.
D. It can also be nested with the Layer Two Tunneling Protocol (L2TP).

Answer: A,D

Question No : 8 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate word.

A_____ is a computer system on the Internet that is expressly set up to attract and trap people who attempt to penetrate other people's computer systems.

Answer: honeypot

Question No : 9 - (Topic 1)

In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?

A. Polymorphic shell code attack
B. IP address spoofing
C. Cross-site request forgery
D. Rainbow attack

Answer: B

Question No : 10 - (Topic 1)

Adrian knows the host names of all the computers on his network. He wants to find the IP addresses of these computers. Which of the following TCP/IP utilities can he use to find the IP addresses of these computers?

Each correct answer represents a complete solution. Choose two.

A. IPCONFIG
B. PING
C. NETSTAT
D. TRACERT

Answer: B,D

Question No : 11 - (Topic 1)

Which of the following can provide security against man-in-the-middle attack?

A. Strong data encryption during travel
B. Firewall
C. Anti-virus programs
D. Strong authentication method

Answer: A

Question No : 12 - (Topic 1)

You are a project manager of a construction project. You are documenting project purchasing decisions, specifying the approach, and identifying potential sellers. You are in which of the following processes?

A. Plan Procurements
B. Administer Procurements

C. Close Procurements
D. Conduct Procurements

Answer: A

Question No : 13 - (Topic 1)

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security equivalent to wired networks for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. Which of the following statements are true about WEP?

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

A. WEP uses the RC4 encryption algorithm.
B. Automated tools such as AirSnort are available for discovering WEP keys.
C. It provides better security than the Wi-Fi Protected Access protocol.
D. The Initialization Vector (IV) field of WEP is only 24 bits long.

Answer: A,B,D

Question No : 14 - (Topic 1)

Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

A. Stick
B. ADMutate
C. Absinthe
D. Fragroute

Answer: C

Question No : 15 - (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. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.
C. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.
D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Answer: B,C

Question No : 16 - (Topic 1)

You are the program manager for your organization. You have proposed a program that will cost $750,000 and will last for four years. Management is concerned with the cost of the program in relation to the return your program will bring. If the rate of return is six percent what is the minimum value your project should return in four years based on the investment of the program?

A. $795,000
B. $750,001
C. $946,857
D. $750,000

Answer: C

Question No : 17 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate type of router.

A _____ router performs packet-filtering and is used as a firewall.

Answer: screening

Question No : 18 - (Topic 1)

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user. You are also required to prevent the sales team members from communicating directly to one another.

Which of the following actions will you perform to accomplish the task?

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

A. Implement the IEEE 802.1X authentication for the wireless network.
B. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.
C. Implement the open system authentication for the wireless network.
D. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.
E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

Answer: A,B,D

Question No : 19 - (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. Qualitative analysis
B. Quantitative analysis
C. Risk identification
D. Estimate activity duration

Answer: A

Question No : 20 - (Topic 1)

Tomas is the project manager of the QWS Project and is worried that the project

stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution of the issues may lead to additional project changes. On what document are Tomas and the stakeholders working in this scenario?

A. Change management plan
B. Communications management plan
C. Issue log
D. Risk management plan

Answer: A

Question No : 21 - (Topic 1)

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP
B. Don't broadcast SSID
C. Implement MAC filtering
D. Implement WPA

Answer: B

Question No : 22 - (Topic 1)

Which of the following tools is based on Linux and used to carry out the Penetration Testing?

A. JPlag
B. BackTrack
C. Vedit
D. Ettercap

Answer: B

Question No : 23 - (Topic 1)

Which of the following are the goals of risk management?

Each correct answer represents a complete solution. Choose three.

A. Identifying the risk
B. Finding an economic balance between the impact of the risk and the cost of the countermeasure
C. Identifying the accused
D. Assessing the impact of potential threats

Answer: A,B,D

Question No : 24 - (Topic 1)

Which of the following features of IE prevent users from a type of scam that entice a user to disclose personal information such as social security number, bank account details, or credit card number?

A. Pop-up blocker
B. Cookie
C. Content Advisor
D. Phishing Filter

Answer: D

Question No : 25 - (Topic 1)

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to use Kismet as a wireless sniffer to sniff the We-are-secure network. Which of the following IEEE-based traffic can be sniffed with Kismet?

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

A. 802.11g
B. 802.11a
C. 802.11b
D. 802.11n

Answer: A,B,C,D

Question No : 26 - (Topic 1)

Which of the following protocols does IPsec use to perform various security functions in the network?

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

A. Internet Key Exchange
B. Encapsulating Security Payload
C. Authentication Header
D. Skinny Client Control Protocol

Answer: A,B,C

Question No : 27 - (Topic 1)

Which of the following provides the best protection against a man-in-the-middle attack?

A. Strong encryption
B. Fiber-optic cable
C. Firewall
D. Strong password

Answer: A

Question No : 28 - (Topic 1)

John works as a professional Ethical Hacker. He has been assigned the task of testing the security of www.we-are-secure.com. He installs a sniffer on the We-are-secure server thinking that the following protocols of the We-are-secure server are being used in the network:

HTTP

SSL

SSH

IPSec

Considering the above factors, which of the following types of packets can he expect to see captured in encrypted form when he checks the sniffer's log file?

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

A. SSH
B. SSL
C. HTTP
D. IPSec

Answer: A,B,D

Question No : 29 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate word.

_____ is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols in general, and not just encryption.

Answer: Cryptanalysis

Question No : 30 - (Topic 1)

Which of the following provides security by implementing authentication and encryption on Wireless LAN (WLAN)?

A. WEP
B. WAP
C. L2TP
D. IPSec

Answer: A

Question No : 31 - (Topic 1)

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He wants to test the response of a DDoS attack on the we-are-secure server. To accomplish this, he takes the following steps:

Instead of directly attacking the target computer, he first identifies a less secure network named Infosecure that contains a network of 100 computers.

He breaks this less secure network and takes control of all its computers. After completing this step, he installs a DDoS attack tool on each computer of the Infosecure network.

Finally, he uses all the computers of the less secure network to carry out the DDoS attack on the we-are-secure server.

Which of the following tools can John use to accomplish the task?

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

A. Stacheldraht
B. Trin00
C. TFN
D. BackOfficer Friendly

Answer: A,B,C

Question No : 32 - (Topic 1)

You are taking over the security of an existing network. You discover a machine that is not being used as such, but has software on it that emulates the activity of a sensitive database server. What is this?

A. A Virus
B. A reactive IDS.
C. A Honey Pot
D. A Polymorphic Virus

Answer: C

Question No : 33 - (Topic 1)

You are the project manager for your organization and are trying to determine which

vendor your organization will use. You have determined that any vendor that would like to bid on your project work will need to have a Microsoft Certified System Engineer on staff, have eight years of Cisco experience, and have at least two references from similar projects. What have you created in this scenario?

A. Screening system for the vendors
B. Weighting system for the vendors
C. Preferred vendors list
D. Bidders conference

Answer: A

Question No : 34 - (Topic 1)

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

A. The network layer headers and the session layer port numbers
B. The presentation layer headers and the session layer port numbers
C. The transport layer port numbers and the application layer headers
D. The application layer port numbers and the transport layer headers

Answer: C

Question No : 35 - (Topic 1)

Mark works as a Network Administrator for Infonet Inc. The company has a Windows 2000 Active Directory domain-based network. The domain contains one hundred Windows XP Professional client computers. Mark is deploying an 802.11 wireless LAN on the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all the connections. According to the company's security policy, the client computers must be able to automatically connect to the wireless LAN. However, the unauthorized computers must not be allowed to connect to the wireless LAN and view the wireless network. Mark wants to configure all the wireless access points and client computers to act in accordance with the company's security policy. What will he do to accomplish this?

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

A. Configure the authentication type for the wireless LAN to Open system.
B. Install a firewall software on each wireless access point.