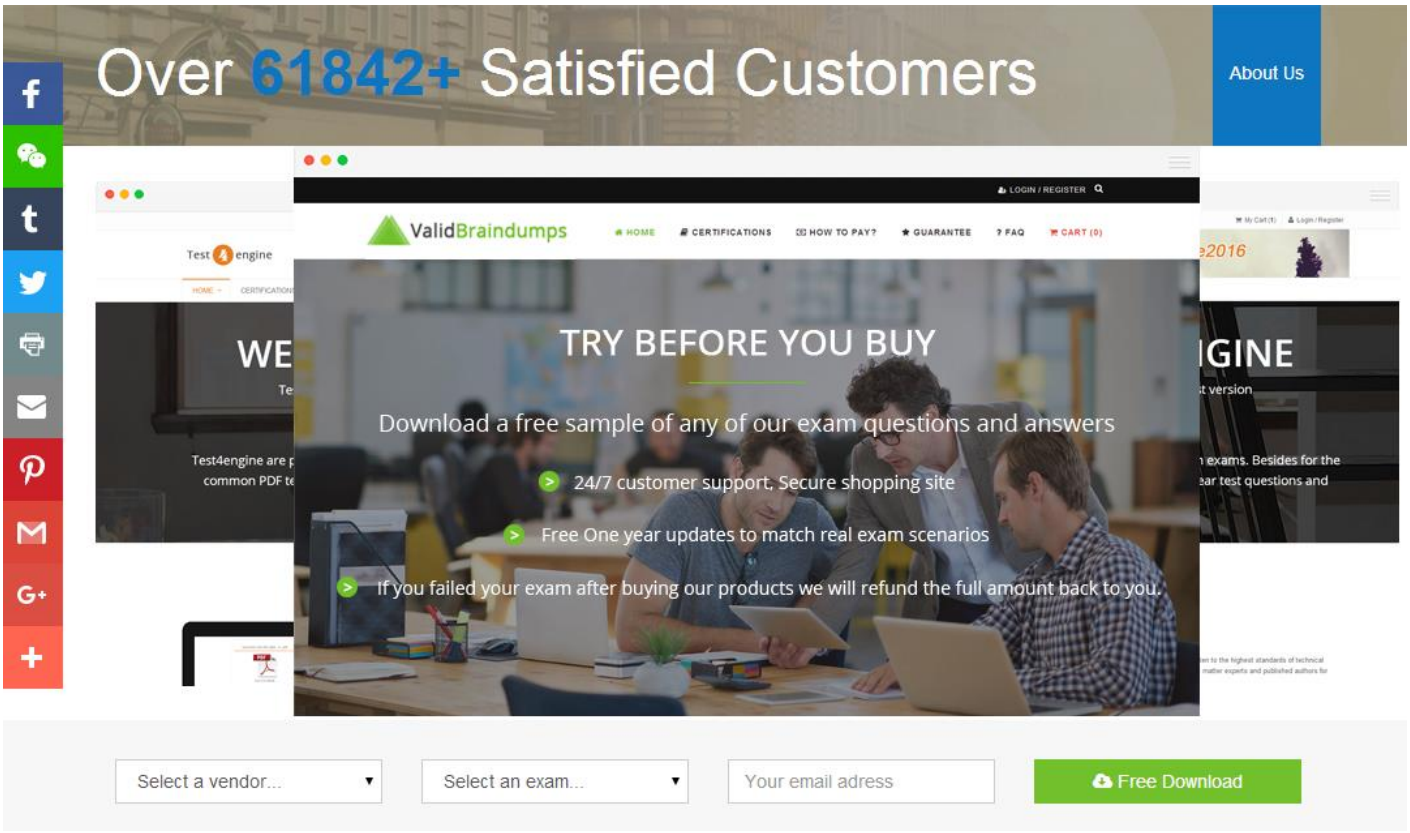
ValidBraindumps



Try Before You Buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

http://www.validbraindumps.com

Free valid test braindumps for IT certification valid exam

Exam : **GSLC**

Title : GIAC Security Leadership Certification (GSLC)

Vendor : GIAC

Version : DEMO

NO.1 Which of the following is the practice of a domain name registrant using the five-day "grace period" (the Add Grace Period or AGP) at the beginning of the registration of an ICANN-regulated second- level domain to test the marketability of the domain?
A. NMap
B. Domain tasting
C. Proxy server
D. PsPasswd
Answer: B

NO.2 Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?
A. Reconnaissance
B. File integrity auditing
C. Shoulder surfing
D. Spoofing
Answer: B

NO.3 You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. You install access points for enabling a wireless network. The sales team members and the managers in the company will be using laptops to connect to the LAN through wireless connections. Therefore, you install WLAN network interface adapters on their laptops. However, you want to restrict the sales team members and managers from communicating directly to each other. Instead, they should communicate through the access points on the network. Which of the following topologies will you use to accomplish the task?
A. Infrastructure
B. Star
C. Ad hoc
D. Mesh
Answer: A

NO.4 Which of the following terms refers to a prolonged loss of power?
A. Spike
B. Brownout
C. Surge
D. Blackout
Answer: D

NO.5 You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2008. The company's headquarters is located at Los Angeles. A branch office of the company is located at Denver. You are about to send a message to Rick who is a Network Administrator at Denver. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys will you use to encrypt the message?

A. Your public key
B. The recipient's private key
C. The recipient's public key
D. Your private key
Answer: C

NO.6 Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account (not administrative) that has permission to remotely access the network. What is this most likely?
A. An example of IP spoofing.
B. A backdoor the intruder created so that he can re-enter the network.
C. A normal account you simply did not notice before. Large networks have a number of accounts; it is hard to track them all.
D. An example of privilege escalation.
Answer: B

NO.7 This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:
- It displays the signal strength of a wireless network, MAC address,
SSID, channel details, etc.
- It is commonly used for the following purposes:
a. War driving
b. Detecting unauthorized access points
c. Detecting causes of interference on a WLAN
d. WEP ICV error tracking
e. Making Graphs and Alarms on 802.11 Data, including Signal Strength
This tool is known as _____.
A. THC-Scan
B. Kismet
C. Absinthe
D. NetStumbler
Answer: D

NO.8 You work as the Network Administrator for a company that does a large amount of defense contract business. A high level of security, particularly regarding sensitive documents, is required. Which of the following are the steps you should take to secure network printers?
Each correct answer represents a complete solution. Choose two.
A. Remove the printers from the network and do not allow remote printing.
B. Ensure that the printers hard drive is scanned for spyware.
C. Secure all remote administrative protocols such as telnet.
D. Do not allow duplicate print jobs.
E. Limit the size of print jobs on the printer.
Answer: BC

NO.9 John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - =
- = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?
Each correct answer represents a complete solution. Choose all that apply.
A. The countermeasure to 'printenv' vulnerability is to remove the CGI script.
B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
C. This vulnerability helps in a cross site scripting attack.
D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.
Answer: ACD

NO.10 Which of the following devices would MOST likely have a DMZ interface?
A. Firewall
B. Switch
C. Load balancer
D. Proxy
Answer: A

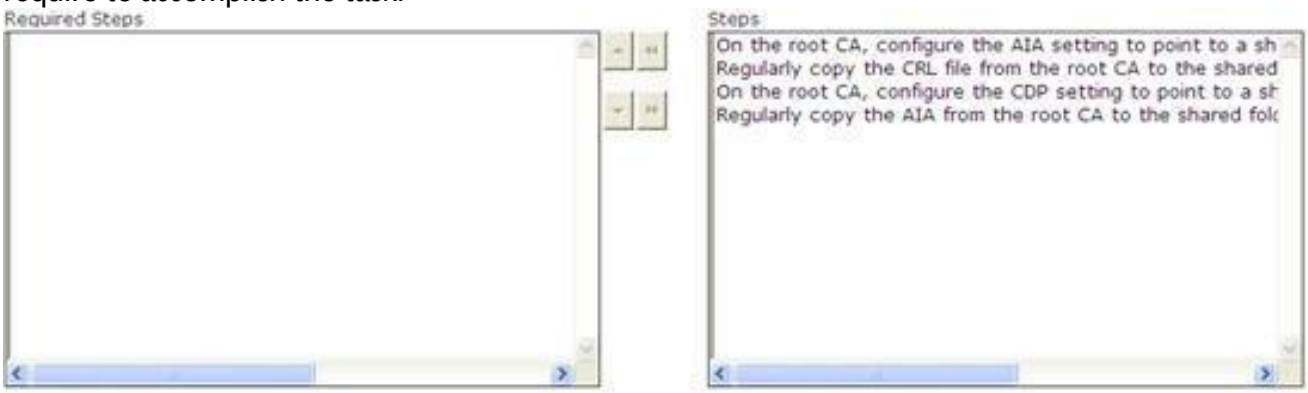
NO.11 Against which of the following does SSH provide protection?
Each correct answer represents a complete solution. Choose two.
A. Broadcast storm
B. DoS attack
C. Password sniffing
D. IP spoofing
Answer: CD

NO.12 John works as a network security officer in Gentech Inc. The company uses a TCP/IP network. While working on the network, a problem occurs related to the DNS resolution. Which of the following utilities can he use to diagnose the problem?
A. IPConfig
B. Ping
C. Tracert
D. nslookup

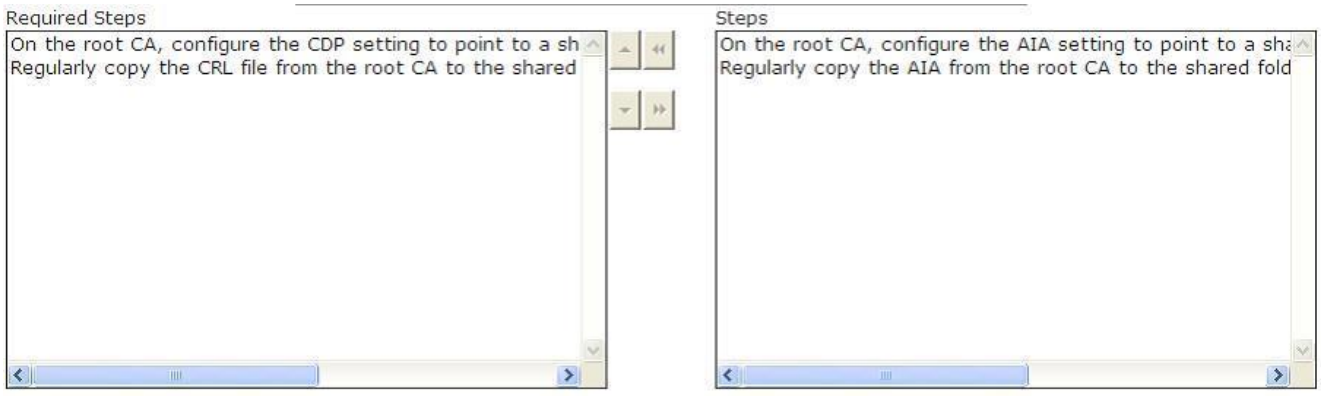
Answer: D

NO.13 Which of the following are the countermeasures against WEP cracking?
Each correct answer represents a part of the solution. Choose all that apply.
A. Changing keys often.
B. Using the longest key supported by hardware.
C. Using a 16 bit SSID.
D. Using a non-obvious key.
Answer: ABD

NO.14 You work as a Network Administrator for Net World International. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. All client computers on the network run Windows XP Professional. You configure a public key infrastructure (PKI) on the network. You configure a root CA and a subordinate CA on the network. For security reasons, you want to take the root CA offline. You are required to configure the CA servers to support for certificate revocation. Choose the steps you will require to accomplish the task.



Answer:



NO.15 Which of the following features is used to generate spam on the Internet by spammers and worms?
A. AutoFill
B. SMTP relay
C. Server Message Block (SMB) signing
D. AutoComplete

Answer: B

NO.16 You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company's headquarters is located at Los Angeles. A branch office of the company is located at Denver. You are about to send a message to Rick who is a Network Administrator at Denver. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys will you use to encrypt the message?

A. The recipient's public key

B. Your private key

C. The recipient's private key

D. Your public key

Answer: A

NO.17 These are false reports about non-existent viruses. In these reports, the writer often claims to do impossible things. Due to these false reports, the network administrator shuts down his network, which in turn affects the work of the company. These reports falsely claim to describe an extremely dangerous virus, and declare that the report is issued by a reputed company. These reports are known as _____.

A. Spambots

B. Logic bombs

C. Chain letters

D. Virus hoaxes

E. Time bombs

Answer: D

NO.18 You are working in a functional organization and are managing the IHH Project. Your project will likely last for six months and has a budget constraint of $1,876,000. You'll be dealing with a functional manager to manage costs and resources in the project. Who will have authority over assigning the project team members to activities?

A. Customers

B. Project sponsor

C. Functional manager

D. Team leader

Answer: C

NO.19 Which of the following files must be configured to enable hostname lookups to use the Domain Name Service (DNS)?

A. libnss_ldap

B. /etc/pam.d

C. /etc/nsswitch.conf

D. /etc/pam.d/sshd

Answer: C

NO.20 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. Border network area
B. Autonomous system area (AS)
C. Demilitarized zone (DMZ)
D. Site network area
Answer: A

NO.21 Which of the following statements are true about worms?
Each correct answer represents a complete solution. Choose all that apply.
A. Worms can exist inside files such as Word or Excel documents.
B. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
C. Worms replicate themselves from one system to another without using a host file.
D. One feature of worms is keystroke logging.
Answer: B,C

NO.22 Which of the following attacks does Management Frame Protection help to mitigate?
Each correct answer represents a complete solution. Choose two.
A. Replay attack
B. DoS attack
C. DDoS attack
D. Man-in-the-middle attack
Answer: BD

NO.23 You work as a technician for Secure Net Inc. You receive an e-mail from your software vendor.
The e-mail contains information about a critical fix that needs to be installed on your computer. It further states that if this patch is not installed right away, your system will crash and you will lose all your data. Now they require your maintenance account password.
Which of the following types of security attacks do you think it is?
A. Social engineering
B. Man-in-the-middle
C. Hacking
D. Spoofing
Answer: A

NO.24 Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?
A. Intrusion detection system (IDS)
B. Demilitarized zone (DMZ)

C. Packet filtering
D. Firewall
Answer: A

NO.25 Which of the following activities result in change requests?
Each correct answer represents a complete solution. Choose all that apply.
A. Preventive actions
B. Inspection
C. Defect repair
D. Corrective actions
Answer: ACD

NO.26 Which of the following are used as a cost estimating technique during the project planning stage?
Each correct answer represents a complete solution. Choose three.
A. Expert judgment
B. Function point analysis
C. Program Evaluation Review Technique (PERT)
D. Delphi technique
Answer: ABD

NO.27 An IPS sensor triggers an alarm known as "signature firing". What events may occur in response? Each correct answer represents a complete solution. Choose all that apply.
A. Attacker's IP address is blocked
B. Unauthorized packets are dropped
C. A log entry is Created
D. TCP connection is reset
Answer: ABCD

NO.28 Which of the following is a popular replacement for halon gas?
A. FM-200
B. CO2
C. SO2
D. Ozone
Answer: A

NO.29 Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 Active Directory domain-based network. The domain consists of four domain controllers, six Windows 2003 member servers, and 500 Windows XP Professional client computers. The PKI infrastructure is already configured on the network. The current configuration of the network allows only managers to use EFS on local computers. Sometimes Mark faces problems when managers lose their private keys due to the user profile becoming corrupt or being lost. Due to this, the files that were persistently encrypted by using the corresponding public key are inaccessible. He wants to restore access to the encrypted files as quickly as possible. What will he do to accomplish the task?

A. Ask the managers to log on to the network with a new user account.
B. Rename all the encrypted files and ask the managers to open the files.
C. Configure key archival on certificate authority (CA).
D. Ask the managers to use the Distributed file system (Dfs) to encrypt important files.
Answer: C

NO.30 You work as a Network Administrator for Perfect Labs Inc. The company has a TCP/IP-based network, which is connected to the Internet. You want to provide Internet access to users. You are concerned about virus threats and want to protect the network against potential virus attacks from the Internet.
Which of the following steps will you take to minimize potential virus attacks?
A. Install a virus protection program on each workstation.
B. Run SCANDISK on each workstation.
C. Configure a firewall in the network.
D. Install a proxy server in the network.
Answer: A

NO.31 Which of the following relies on a physical characteristic of the user to verify his identity?
A. Kerberos v5
B. Social Engineering
C. CHAP
D. Biometrics
Answer: D

NO.32 You work as a Network Administrator for Infosec Inc. Nowadays, you are facing an unauthorized access in your Wi-Fi network. Therefore, you analyze a log that has been recorded by your favorite sniffer, Ethereal. You are able to discover the cause of the unauthorized access after noticing the following string in the log file:
(Wlan.fc.type_subtype eq 32 and llc.oui eq 0x00601d and llc.pid eq
0x0001)
When you find All your 802.11b are belong to us as the payload string, you are convinced about which tool is being used for the unauthorized access.
Which of the following tools have you ascertained?
A. NetStumbler
B. AiroPeek
C. Kismet
D. AirSnort
Answer: A

NO.33 Which of the following are symptoms of a virus attack on your computer?
Each correct answer represents a complete solution. Choose two.
A. Corrupted or missing files.
B. Sudden reduction in system resources.
C. Faster read/write access of the CD-ROM drive.

D. Unclear monitor display.
Answer: AB

NO.34 Which of the following is used for high-level or comprehensive analysis, as well as for root cause analysis?
A. Assumptions analysis
B. Delphi method
C. Brainstorming
D. Checklist analysis
Answer: D

NO.35 Which of the following is an input of the close procurements process?
A. Organizational process asset updates
B. Procurement credentials
C. Project management plan
D. Closed procurements
Answer: C