GIAC

Exam Questions GSEC

GIAC Security Essentials Certification

NEW QUESTION 1
At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

A. When performing analysis
B. When preparing policy
C. When recovering from the incident
D. When reacting to an incident

Answer: D

NEW QUESTION 2
Where could you go in Windows XP/2003 to configure Automatic Updates?

A. Right click on the Start Menu and choose select Properties in the pop-up Men
B. Open the MMC and choose the Automatic Updates snap-i
C. Right click on your desktop and choose the automatic update
D. Go to the System applet in Control Panel and click on the Automatic Updates ico

Answer: D

NEW QUESTION 3
When Net Stumbler is initially launched, it sends wireless frames to which of the following addresses?

A. Broadcast address
B. Default gateway address
C. Subnet address
D. Network address

Answer: A

NEW QUESTION 4
Which of the following hardware devices prevents broadcasts from crossing over subnets?

A. Bridge
B. Hub
C. Router
D. Modem

Answer: C

NEW QUESTION 5
When trace route fails to get a timely response for a packet after three tries, which action will it take?

A. It will print '* * *' for the attempts and increase the maximum hop count by on
B. It will exit gracefully, and indicate to the user that the destination is unreachabl
C. It will increase the timeout for the hop and resend the packet
D. It will print '* * *' for the attempts, increment the TTL and try again until the maximum hop coun

Answer: D

NEW QUESTION 6
Which of the following works at the network layer and hides the local area network IP address and topology?

A. Network address translation (NAT)
B. Hub
C. MAC address
D. Network interface card (NIC)

Answer: A

NEW QUESTION 7
Which of the following are the types of access controls?
Each correct answer represents a complete solution. Choose three.

A. Physical
B. Administrative
C. Automatic
D. Technical

Answer: ABD

NEW QUESTION 8
If you do NOT have an original file to compare to, what is a good way to identify steganography in potential carrier files?

A. Determine normal properties through methods like statistics and look for changes
B. Determine normal network traffic patterns and look for changes
C. Find files with the extension .stg
D. Visually verify the files you suspect to be steganography messages

Answer: A

NEW QUESTION 9
What is a security feature available with Windows Vista and Windows 7 that was not present in previous Windows operating systems?

A. Data Execution Prevention (DEP)
B. User Account Control (UAC)
C. Encrypting File System (EFS)
D. Built-in IPSec Client

Answer: B

NEW QUESTION 10
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright
B. Trademark
C. Trade secret
D. Patent

Answer: B

NEW QUESTION 10
Which of the below choices should an organization start with when implementing an effective risk management process?

A. Implement an incident response plan
B. Define security policy requirements
C. Conduct periodic reviews
D. Design controls and develop standards for each technology you plan to deploy

Answer: B

NEW QUESTION 15
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You are optimizing performance and security on your Web server. You want to know the ports that are listening to FTP. Which of the following commands will you use?

A. netstat -a | grep FTP
B. FTP netstat -r
C. FTP netstat -a
D. netstat -r | grep FTP

Answer: A

NEW QUESTION 20
Which Host-based IDS (HIDS) method of log monitoring utilizes a list of keywords or phrases that define the events of interest for the analyst, then takes a list of keywords to watch for and generates alerts when it sees matches in log file activity?

A. Passive analysis
B. Retroactive analysis
C. Exclusive analysis
D. Inclusive analysis

Answer: D

NEW QUESTION 25
Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.
This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection
B. Threat-oriented
C. Information-centric
D. Protected enclaves

Answer: A

NEW QUESTION 27
Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

A. RARP
B. ARP
C. DNS
D. RDNS

Answer: A

NEW QUESTION 30
You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering? Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption
B. Ease of maintenance
C. Load balancing
D. Failover

Answer: CD

NEW QUESTION 33
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He is currently working on his C based new traceroute program. Since, many processes are running together on the system, he wants to give the highest priority to the cc command process so that he can test his program, remove bugs, and submit it to the office in time. Which of the following commands will John use to give the highest priority to the cc command process?

A. nice -n 19 cc -c *.c &
B. nice cc -c *.c &
C. nice -n -20 cc -c *.c &
D. nice cc -c *.c

Answer: C

NEW QUESTION 36
You work as a Network Administrator for McNeil Inc. You are installing an application. You want to view the log file whenever a new entry is added to the /var/log/messages log file. Which of the following commands will you use to accomplish this?

A. TAIL -show /var/log/messages
B. TAIL -f /var/log/messages
C. TAIL -50 /var/log/messages
D. TAIL -view /var/log/messages

Answer: B

NEW QUESTION 37
Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

A. Anonymous authentication
B. Mutual authentication
C. Open system authentication
D. Shared key authentication

Answer: CD

NEW QUESTION 40
Which of the following is referred to as Electromagnetic Interference (EMI)?

A. Electrical line noise
B. Spike
C. Transient
D. Brownout

Answer: A

NEW QUESTION 41
Which of the following statements would describe the term "incident" when used in the branch of security known as Incident Handling?

A. Any observable network event
B. Harm to systems
C. Significant threat of harm to systems
D. A and C
E. A, B, and C
F. B and C
G. A and B

Answer: D

NEW QUESTION 42

Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments.
This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection
B. Protected enclaves
C. Vector-oriented
D. Information-centric

Answer: B

NEW QUESTION 43
Which type of risk assessment results are typically categorized as low, medium, or high-risk events?

A. Technical
B. Qualitative
C. Management
D. Quantitative

Answer: B

NEW QUESTION 48
Which of the following protocols implements VPN using IPSec?

A. SLIP
B. PPP
C. L2TP
D. PPTP

Answer: C

NEW QUESTION 53
Which of the following are used to suppress gasoline and oil fires? Each correct answer represents a complete solution. Choose three.

A. Halon
B. CO2
C. Soda acid
D. Water

Answer: ABC

NEW QUESTION 57
Which of the following best describes the level of risk associated with using proprietary crypto algorithms.?

A. Proprietary cryptographic algorithms are required by law to use shorter key lengths in the United States, so the risk is hig
B. Proprietary algorithms have not been subjected to public scrutiny, so they have been checked less throughly for vulnerabilitie
C. Proprietary algorithms are less likely be vulnerable than algorithms that have been publicly disclosed because of enhanced secrecy of the algorith
D. Proprietary algorithms are not known to generally be any more or less vulnerable than publicly scrutinized algorithm

Answer: B

NEW QUESTION 60
Which of the following are the types of intrusion detection systems?
Each correct answer represents a complete solution. Choose all that apply.

A. Host-based intrusion detection system (HIDS)
B. Client-based intrusion detection system (CIDS)
C. Server-based intrusion detection system (SIDS)
D. Network intrusion detection system (NIDS)

Answer: AD

NEW QUESTION 63
Why would someone use port 80 for deployment of unauthorized services?

A. Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue servic
B. If someone were to randomly browse to the rogue port 80 service they could be compromise
C. This is a technique commonly used to perform a denial of service on the local web serve
D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environment

Answer: D

NEW QUESTION 64
What is the process of simultaneously installing an operating system and a Service Pack called?

A. Synchronous Update
B. Slipstreaming
C. Simultaneous Update
D. Synchronizing

Answer: B

NEW QUESTION 67
Which of the following applications would be BEST implemented with UDP instead of TCP?

A. A multicast streaming applicatio
B. A web browse
C. A DNS zone transfe
D. A file transfer applicatio

Answer: A

NEW QUESTION 70
Which aspect of UNIX systems was process accounting originally developed for?

A. Data warehouse
B. Time sharing
C. Process tracking
D. Real time

Answer: C

NEW QUESTION 73
You have reason to believe someone with a domain user account has been accessing and modifying sensitive spreadsheets on one of your application servers. You decide to enable auditing for the files to see who is accessing and changing them. You enable the Audit Object Access policy on the files via Group Policy. Two weeks later, when you check on
the audit logs, you see they are empty. What is the most likely reason this has happened?

A. You cannot enable auditing on files, just folders
B. You did not enable auditing on the files
C. The person modifying the files turned off auditing
D. You did not save the change to the policy

Answer: B

NEW QUESTION 75
You work as a Network Administrator for McNeil Inc. The company has a Linux-based network. David, a Sales Manager, wants to know the name of the shell that he is currently using. Which of the following commands will he use to accomplish the task?

A. mv $shell
B. echo $shell
C. rm $shell
D. ls $shell

Answer: B

NEW QUESTION 76
With regard to defense-in-depth, which of the following statements about network design principles is correct?

A. A secure network design requires that systems that have access to the Internet should not be accessible from the Internet and that systems accessible from the Internet should not have access to the Interne
B. A secure network design requires that networks utilize VLAN (Virtual LAN) implementations to insure that private and semi-public systems are unable to reach each other without going through a firewal
C. A secure network design will seek to provide an effective administrative structure by providing a single choke-point for the network from which all security controls and restrictions will be enforce
D. A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirement

Answer: D

NEW QUESTION 77
You work as a Network Administrator for Secure World Inc. The company has a Linux-based network. You want to run a command with the changed root directory. Which of the following commands will you use?

A. ls <new root> <command>
B. chroot <new root> <command>
C. route <new root> <command>
D. chdir <new root> <command>

Answer: B

NEW QUESTION 81

Who is responsible for deciding the appropriate classification level for data within an organization?

A. Data custodian
B. Security auditor
C. End user
D. Data owner

Answer: B

NEW QUESTION 83
You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

A. PPTP
B. IPSec
C. PGP
D. NTFS

Answer: C

NEW QUESTION 84
Which of the following classes of fire comes under Class C fire?

A. Paper or wood fire
B. Oil fire
C. Combustible metals fire
D. Electronic or computer fire

Answer: D

NEW QUESTION 89
A folder D:\Files\Marketing has the following NTFS permissions:
. Administrators: Full Control
. Marketing: Change and Authenticated
. Users: Read
It has been shared on the server as "MARKETING", with the following share permissions:
. Full Control share permissions for the Marketing group
Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?

A. No access
B. Full Control
C. Read
D. Change

Answer: C

NEW QUESTION 94
What is the key difference between Electronic Codebook mode and other block cipher modes like Cipher Block Chaining, Cipher-Feedback and Output-Feedback?

A. Plaintext patterns are concealed by XO Ring with previous cipher text block but input to the block cipher is not randomize
B. Plaintext patterns are concealed and input to the block cipher is randomized by XO Ring with previous cipher text bloc
C. Plaintext patterns encrypted with the same key will always generate the same Cipher text pattern
D. Plaintext patterns are not concealed but input to the block cipher is randomized by XO Ring with previous cipher text bloc

Answer: C

NEW QUESTION 97
Which of the following commands is used to change file access permissions in Linux?

A. chgrp
B. chperm
C. chmod
D. chown

Answer: C

NEW QUESTION 99
What is the name of the command-line tool for Windows that can be used to manage audit policies on remote systems?

A. SECEDTT.EXE
B. POLCLI.EXE
C. REMOTEAUDIT.EXE
D. AUDITPOL.EXE

Answer: D

NEW QUESTION 101

An attacker gained physical access to an internal computer to access company proprietary
data. The facility is protected by a fingerprint biometric system that records both failed and successful entry attempts. No failures were logged during the time periods of the recent breach. The account used when the attacker entered the facility shortly before each incident belongs to an employee who was out of the area. With respect to the biometric entry system, which of the following actions will help mitigate unauthorized physical access to the facility?

A. Try raising the Crossover Error Rate (CER)
B. Try to lower the False Accept Rate (FAR)
C. Try setting the Equal Error Rate (EER) to zero
D. Try to set a lower False Reject Rate (FRR)

Answer: B

NEW QUESTION 104
How are differences in configuration settings handled between Domain and Local Group Policy Objects (GPOs)?

A. Local and Domain GPOs control different configuration settings, so there will not be conflict
B. Settings in the domain-wide GPO override conflicting settings in the local GPO on each compute
C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applie
D. Precedence depends on which GPO was updated firs

Answer: B

NEW QUESTION 107
You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are required to search for the error messages in the /var/log/messages log file. Which of the following commands will you use to accomplish this?

A. ps /var/log/messages
B. cat /var/log/messages | look error
C. cat /var/log/messages | grep error
D. cat /var/log/messages

Answer: C

NEW QUESTION 108
Which of the following types of computers is used for attracting potential intruders?

A. Files pot
B. Honey pot
C. Data pot
D. Bastion host

Answer: B

NEW QUESTION 112
Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?

A. Ability to detect malicious traffic after it has been decrypted by the host
B. Ability to decrypt network traffic
C. Ability to listen to network traffic at the perimeter
D. Ability to detect malicious traffic before it has been decrypted

Answer: A

NEW QUESTION 113
Which common firewall feature can be utilized to generate a forensic trail of evidence and
to identify attack trends against your network?

A. NAT
B. State Table
C. Logging
D. Content filtering

Answer: C

NEW QUESTION 117
Which of the following Linux commands can change both the username and group name a file belongs to?

A. chown
B. chgrp
C. chmod
D. newgrp

Answer: B

NEW QUESTION 119

Which of the following attack vectors are addressed by Xinetd and TCP Wrappers?

A. Outsider attack from network
B. Outsider attack from a telephone
C. Insider attack from local network
D. Attack from previously installed malicious code
E. A and B
F. A and C
G. B and D
H. C and D

Answer: B

NEW QUESTION 121
Which of the following statements would be seen in a Disaster Recovery Plan?

A. "Instructions for notification of the media can be found in Appendix A"
B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."
C. "The target for restoration of business operations is 72 hours from the declaration of disaster."
D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Answer: D

NEW QUESTION 125
You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. You are configuring an application server. An application named Report, which is owned by the root user, is placed on the server. This application requires superuser permission to write to other files. All sales managers of the company will be using the application. Which of the following steps will you take in order to enable the sales managers to run and use the Report application?

A. Change the Report application to a SUID comman
B. Make the user accounts of all the sales managers the members of the root grou
C. Provide password of root user to all the sales manager
D. Ask each sales manager to run the application as the root use
E. As the application is owned by the root, no changes are require

Answer: A

NEW QUESTION 126
Which of the following is the reason of using Faraday cage?

A. To prevent Denial-of-Service (DoS) attack
B. To prevent shoulder surfing
C. To prevent mail bombing
D. To prevent data emanation

Answer: D

NEW QUESTION 128
What is the motivation behind SYN/FIN scanning?

A. The SYN/FIN combination is useful for signaling to certain Trojan
B. SYN/FIN packets are commonly used to launch denial of service attacks against BSD host
C. The crafted SYN/FIN packet sometimes gets past firewalls and filtering router
D. A SYN/FIN packet is used in session hijacking to take over a sessio

Answer: B

NEW QUESTION 131
You work as a Network Administrator for McNeil 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's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:
The wireless network communication should be secured.
The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps:
Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication. What will happen after you have taken these steps?

A. The laptop users will be able to use smart cards for getting authenticate
B. Both tasks will be accomplishe
C. None of the tasks will be accomplishe
D. The wireless network communication will be secure

Answer: D

NEW QUESTION 134
When an IIS filename extension is mapped, what does this mean?

A. Files with the mapped extensions cannot be interpreted by the web serve

B. The file and all the data from the browser's request are handed off to the mapped interprete
C. The files with the mapped extensions are interpreted by CMD.EX
D. The files with the mapped extensions are interpreted by the web browse

Answer: B

NEW QUESTION 137
You have set up a local area network for your company. Your firewall separates your network into several sections: a DMZ with semi-public servers (web, dns, email) and an intranet with private servers. A penetration tester gains access to both sections and installs sniffers in each. He is able to capture network traffic for all the devices in the private section but only for one device (the device with the sniffer) in the DMZ. What can be inferred about the design of the system?

A. You installed a router in the private section and a switch in the DMZ
B. You installed a hub in the private section and a switch in the DMZ
C. You installed a switch in the private section and a hub in the DMZ
D. You installed a switch in the private section and a router in the DMZ

Answer: B

NEW QUESTION 141
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of emails on the network. Which of the following ports will you open?
Each correct answer represents a complete solution. Choose two.

A. 80
B. 25
C. 20
D. 110

Answer: BD

NEW QUESTION 143
You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.
What will be the key functions of the sensors in such a physical layout?
Each correct answer represents a complete solution. Choose all that apply.

A. To collect data from operating system logs
B. To notify the console with an alert if any intrusion is detected
C. To analyze for known signatures
D. To collect data from Web servers

Answer: BC

NEW QUESTION 144
Why are false positives such a problem with IPS technology?

A. File integrity is not guarantee
B. Malicious code can get into the networ
C. Legitimate services are not delivere
D. Rules are often misinterprete

Answer: D

NEW QUESTION 148
Which of the following is a required component for successful 802.lx network authentication?

A. Supplicant
B. 3rd-party Certificate Authority
C. Ticket Granting Server (TGS)
D. IPSec

Answer: A

NEW QUESTION 152
If the NET_ID of the source and destination address in an IP (Internet Protocol) packet match, which answer BEST describes the routing method the sending host will use?

A. Local (or direct) routing
B. Circuit switch routing
C. Dynamic (or changeable) routing
D. Remote (or indirect) routing

Answer: A

NEW QUESTION 157

You work as a Network Administrator for McRobert Inc. You want to know the NetBIOS name of your computer. Which of the following commands will you use?

A. NETSTAT -s
B. NBTSTAT -s
C. NBTSTAT -n
D. NETSTAT -n

Answer: C

NEW QUESTION 162
Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure
B. Snort
C. StealthWatch
D. Tripwire

Answer: B

NEW QUESTION 164
The Linux command to make the /etc/shadow file, already owned by root, readable only by root is which of the following?

A. chmod 444/etc/shadow
B. chown root: root/etc/shadow
C. chmod 400/etc/shadow
D. chown 400 /etc/shadow

Answer: C

NEW QUESTION 165
Which of the following quantifies the effects of a potential disaster over a period of time?

A. Risk Assessment
B. Business Impact Analysis
C. Disaster Recovery Planning
D. Lessons Learned

Answer: B

NEW QUESTION 168
Which of the following processes is known as sanitization?

A. Assessing the risk involved in discarding particular informatio
B. Verifying the identity of a person, network host, or system proces
C. Physically destroying the media and the information stored on i
D. Removing the content from the media so that it is difficult to restor

Answer: D

NEW QUESTION 170
What is the main reason that DES is faster than RSA?

A. DES is less secur
B. DES is implemented in hardware and RSA is implemented in softwar
C. Asymmetric cryptography is generally much faster than symmetri
D. Symmetric cryptography is generally much faster than asymmetri

Answer: D

NEW QUESTION 175
What defensive measure could have been taken that would have protected the confidentiality of files that were divulged by systems that were compromised by malware?

A. Ingress filtering at the host level
B. Monitoring for abnormal traffic flow
C. Installing file integrity monitoring software
D. Encrypting the files locally when not in use

Answer: D

NEW QUESTION 180
Which of the following is a benefit of using John the Ripper for auditing passwords?

A. John's Blowfish cracking routine uses a complex central computing loop that increases the cost of each hash computatio
B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfis

C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computatio
D. John cannot use the DES bit-slicing technique, so it is much slower than other tools, especially when used against DES-encrypted password

Answer: C

NEW QUESTION 184
When considering ingress filtering, why should all inbound packets be dropped if they contain a source address from within the protected network address space?

A. The packets are probably corrupte
B. The packets may have been accidentally routed onto the Interne
C. The packets may be deliberately spoofed by an attacke
D. The packets are a sign of excess fragmentatio
E. A and B
F. B and C
G. B and D
H. A and D

Answer: B

NEW QUESTION 188
Where are user accounts and passwords stored in a decentralized privilege management environment?

A. On a central authentication serve
B. On more than one serve
C. On each serve
D. On a server configured for decentralized privilege managemen

Answer: C

NEW QUESTION 191
What is the name of the registry key that is used to manage remote registry share permissions for the whole registry?

A. regkey
B. regmng
C. winreg
D. rrsreg

Answer: C

NEW QUESTION 196
During which of the following steps is the public/private key-pair generated for Public Key Infrastructure (PKI)?

A. Key Recovery
B. Initialization
C. Registration
D. Certification

Answer: B

NEW QUESTION 199
The TTL can be found in which protocol header?

A. It is found in byte 8 of the ICMP heade
B. It is found in byte 8 of the IP heade
C. It is found in byte 8 of the TCP heade
D. It is found in byte 8 of the DNS heade

Answer: B

NEW QUESTION 200
Which of the following tools is used to configure, control, and query the TCP/IP network interface parameters?

A. NSLOOKUP
B. IPCONFIG
C. ARP
D. IFCONFIG

Answer: D

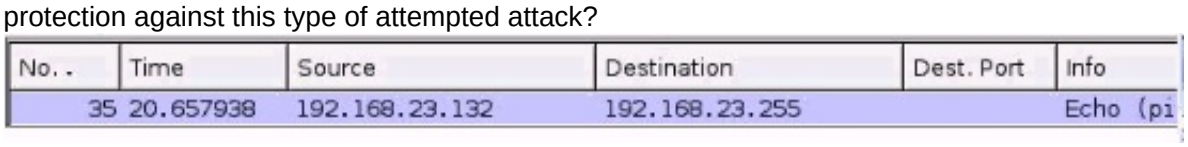
NEW QUESTION 201
If a DNS client wants to look up the IP address for good.news.com and does not receive an authoritative reply from its local DNS server, which name server is most likely to provide an authoritative reply?

A. The news.com domain name server
B. The .com (top-level) domain name server

C. The .(root-level) domain name server
D. The .gov (top-level) domain name server

Answer: A

NEW QUESTION 204
You are examining a packet capture session in Wire shark and see the packet shown in the accompanying image. Based on what you see, what is the appropriate protection against this type of attempted attack?



No. .	Time	Source	Destination	Dest. Port	Info
35	20.657938	192.168.23.132	192.168.23.255		Echo (pi

A. Block DNS traffic across the router
B. Disable forwarding of unsolicited TCP requests
C. Disable IP-directed broadcast requests
D. Block UDP packets at the firewall

Answer: C

NEW QUESTION 207
What is the following sequence of packets demonstrating?

A. telnet.com.telnet > client.com.38060: F 4289:4289(0) ack 92 win 1024
B. client.com.38060 > telnet.com.telnet: .ack 4290 win 8760 (DF)
C. client.com.38060 > telnet.com.telnet: F 92:92(0) ack 4290 win 8760 (DF)
D. telnet.com.telnet > client.com.38060: .ack 93 win 1024

Answer: C

NEW QUESTION 211
In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?

A. Discrete
B. Reporting
C. Promiscuous
D. Alert

Answer: C

NEW QUESTION 213
Which layer of the TCP/IP Protocol Stack Is responsible for port numbers?

A. Network
B. Transport
C. Internet
D. Application

Answer: B

NEW QUESTION 214
Which command would allow an administrator to determine if a RPM package was already installed?

A. rpm -s
B. rpm -q
C. rpm -a
D. rpm -t

Answer: B

NEW QUESTION 216
The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?
STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.
STEP 2 - Do a binary backup if data is being collected.
STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic ba
B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custod
C. Take photographs of all persons who have had access to the compute
D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic ba

Answer: D

NEW QUESTION 219
What would the following IP tables command do?

IP tables -I INPUT -s 99.23.45.1/32 -j DROP

A. Drop all packets from the source address
B. Input all packers to the source address
C. Log all packets to or from the specified address
D. Drop all packets to the specified address

Answer: A

NEW QUESTION 224
Which of the following terms refers to the process in which headers and trailers are added around user data?

A. Encapsulation
B. Authentication
C. Authorization
D. Encryption

Answer: A

NEW QUESTION 229
The previous system administrator at your company used to rely heavily on email lists, such as vendor lists and Bug Traq to get information about updates and patches. While a useful means of acquiring data, this requires time and effort to read through. In an effort to speed things up, you decide to switch to completely automated updates and patching. You set up your systems to automatically patch your production servers using a cron job and a scripted apt-get upgrade command. Of the following reasons, which explains why you may want to avoid this plan?

A. The apt-get upgrade command doesn't work with the cron command because of incompatibility
B. Relying on vendor and 3rd party email lists enables updates via email, for even faster patching
C. Automated patching of production servers without prior testing may result in unexpected behavior or failures
D. The command apt-get upgrade is incorrect, you need to run the apt-get update command

Answer: D

NEW QUESTION 233
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

GSEC Practice Exam Features:

* GSEC Questions and Answers Updated Frequently

* GSEC Practice Questions Verified by Expert Senior Certified Staff

* GSEC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GSEC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year