

GIAC

Exam Questions GSEC

GIAC Security Essentials Certification



NEW QUESTION 1

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 2

Which of the following should be implemented to protect an organization from spam?

- A. Auditing
- B. System hardening
- C. E-mail filtering
- D. Packet filtering

Answer: C

NEW QUESTION 3

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 4

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 5

On which of the following OSI model layers does IPSec operate? A. Physical layer

- A. Network layer
- B. Data-link layer
- C. Session layer

Answer: B

NEW QUESTION 6

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 7

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 8

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 9

When designing wireless networks, one strategy to consider is implementing security mechanisms at all layers of the OSI model. Which of the following protection mechanisms would protect layer 1?

- A. Hardening applications
- B. Limit RF coverage
- C. Employing firewalls
- D. Enabling strong encryption

Answer: B

NEW QUESTION 10

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 10

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 14

Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

- A. Snort
- B. Apache
- C. SSH
- D. SUDO

Answer: D

NEW QUESTION 17

Which of the following is NOT a recommended best practice for securing Terminal Services and Remote Desktop?

- A. Require TLS authentication and data encryption whenever possible
- B. Make sure to allow all TCP 3389 traffic through the external firewall
- C. Group Policy should be used to lock down the virtual desktops of thin-client user
- D. Consider using IPSec or a VPN in addition to the RDP encryption if you are concerned about future RDP vulnerabilities

Answer: B

NEW QUESTION 21

Which choice best describes the line below?

```
alert tcp any any -> 192.168.1.0/24 80 (content: /cgi-bin/test.cgi"; msg: "Attempted CGI-BIN Access!!");
```

- A. Tcpdump filter
- B. IP tables rule
- C. Wire shark filter
- D. Snort rule

Answer: D

NEW QUESTION 26

When discussing access controls, which of the following terms describes the process of determining the activities or functions that an Individual is permitted to perform?

- A. Authentication
- B. Identification
- C. Authorization
- D. Validation

Answer: C

NEW QUESTION 31

In a /24 subnet, which of the following is a valid broadcast address?

- A. 200.11.11.1
- B. 221.10.10.10
- C. 245.20.30.254
- D. 192.10.10.255

Answer: D

NEW QUESTION 34

Which Linux file lists every process that starts at boot time?

- A. inetd
- B. netsrv
- C. initd
- D. inittab

Answer: D

NEW QUESTION 39

What is TRUE about Workgroups and Domain Controllers?

- A. By default all computers running Windows 2008 can only form Domain Controllers not Workgroups
- B. Workgroups are characterized by higher costs while Domain Controllers by lower costs
- C. You cannot have stand-alone computers in the midst of other machines that are members of a domain
- D. Workgroup computers cannot share resources, only computers running on the same domain can
- E. You can have stand-alone computers in the midst of other machines that are members of a domain

Answer: E

NEW QUESTION 40

Which of the following is a type of countermeasure that can be deployed to ensure that a threat vector does not meet a vulnerability?

- A. Prevention controls
- B. Detection controls
- C. Monitoring controls
- D. Subversive controls

Answer: A

NEW QUESTION 44

Which of the following is a term that refers to unsolicited e-mails sent to a large number of e-mail users?

- A. Hotfix
- B. Spam
- C. Biometrics
- D. Buffer overflow

Answer: B

NEW QUESTION 49

Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

- A. Visitors
- B. Customers
- C. Employees
- D. Hackers

Answer: C

NEW QUESTION 54

What would the file permission example "rwsr-sr-x" translate to in absolute mode?

- A. 1755
- B. 6755
- C. 6645
- D. 1644

Answer: B

NEW QUESTION 59

Which of the following statements about the authentication concept of information security management is true?

- A. It ensures the reliable and timely access to resource
- B. It ensures that modifications are not made to data by unauthorized personnel or processes
- C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual
- D. It establishes the users' identity and ensures that the users are who they say they are

Answer: D

NEW QUESTION 62

Which of the following statements about buffer overflow is true?

- A. It manages security credentials and public keys for message encryption
- B. It is a collection of files used by Microsoft for software updates released between major service pack releases
- C. It is a condition in which an application receives more data than it is configured to accept
- D. It is a false warning about a virus

Answer: C

NEW QUESTION 64

In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:

You've notified users that there will be a system test.

You've prioritized and selected your targets and subnets.

You've configured the system to do a deep scan.

You have a member of your team on call to answer questions.

Which of the following is a necessary step to take prior to starting the scan?

- A. Placing the incident response team on call
- B. Clear relevant system log files
- C. Getting permission to run the scan
- D. Scheduling the scan to run before OS update

Answer: C

NEW QUESTION 66

Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

- A. Disaster Recovery Plans
- B. Anticipating all relevant threats
- C. Executive buy-in
- D. Clearly defining roles and responsibilities
- E. Training

Answer: C

NEW QUESTION 69

Which of the following tools is also capable of static packet filtering?

- A. netstat.exe
- B. ipsecpol.exe
- C. ipconfig.exe
- D. net.exe

Answer: B

NEW QUESTION 73

What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

- A. Trojans
- B. Boot infectors
- C. Viruses
- D. Worms

Answer: D

NEW QUESTION 76

What is the term for a game in which for every win there must be an equivalent loss?

- A. Asymmetric
- B. Untenable
- C. Zero-sum
- D. Gain-oriented

Answer: C

NEW QUESTION 78

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 81

While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?

- A. The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating system
- B. The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating system
- C. The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machine
- D. The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating system
- E. The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique IP addresses and then define how much of the system's RAM is available to the guest operating system

Answer: E

NEW QUESTION 83

You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadserver.com so that it can connect to it. There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware to connect to it instead. How do you get the malware to connect to that computer on the test network?

- A. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
- B. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadserver iamabadserver.com
- C. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
- D. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.115 iamabadserver iamabadserver.com

Answer: B

NEW QUESTION 86

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 91

You are reviewing a packet capture file from your network intrusion detection system. In the packet stream, you come across a long series of "no operation" (NOP) commands. In addition to the NOP commands, there appears to be a malicious payload. Of the following, which is the most appropriate preventative measure for this type of attack?

- A. Limits on the number of failed logins
- B. Boundary checks on program inputs
- C. Controls against time of check/time of use attacks
- D. Restrictions on file permissions

Answer: C

NEW QUESTION 96

You have an automated system for patching the operating systems of all your computers. All patches are supposedly current. Yet your automated vulnerability scanner has just reported vulnerabilities that you believe have been patched. Which of the actions below should you take next?

- A. Check some systems manually
- B. Rerun the system patching routine
- C. Contact the incident response team
- D. Ignore the findings as false positive

Answer: A

NEW QUESTION 101

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 102

Which of the following protocols describes the operation of security in H.323? A. H.239

- A. H.245
- B. H.235
- C. H.225

Answer: C

NEW QUESTION 103

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

- A. File pot
- B. Honey pot
- C. Data pot
- D. Bastion host

Answer: B

NEW QUESTION 107

A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?

- A. Power
- B. Smoke
- C. Natural Gas
- D. Water
- E. Toxins

Answer: B

NEW QUESTION 112

Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?

- A. 07:09:43.368615 download.net.39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)
- B. 07:09:43.370302 ftp.com.21 > download.net.39904: S 1192930639:1192930639(0) ack 733381830 win 1024 <mss 1460> (DF)
- C. 09:09:22.346383 ftp.com.21 > download.net.39904: , rst 1 win 2440(DF)
- D. 07:09:43.370355 download.net.39904 > ftp.com.21: , ack 1 win 8760 (DF)

Answer: A

NEW QUESTION 113

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain-based network. The network contains ten Windows 2003 member servers, 150 Windows XP Professional client computers. According to the company's security policy, Mark needs to check whether all the computers in the network have all available security updates and shared folders. He also needs to check the file system type on each computer's hard disk. Mark installs and runs MBSACLI.EXE with the appropriate switches on a server. Which of the following tasks will he accomplish?

- A. None of the tasks will be accomplished
- B. He will be able to check the file system type on each computer's hard disk
- C. He will be able to accomplish all the tasks
- D. He will be able to check all available security updates and shared folders

Answer: C

NEW QUESTION 114

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 119

What is the first thing that should be done during the containment step of incident handling?

- A. Change all the passwords
- B. Secure the area
- C. Prepare the Jump bag
- D. Notify management
- E. Prepare a report

Answer: B

NEW QUESTION 124

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 more commonly used for establishing high-speed backbones that interconnect smaller networks and can carry signals over significant distances?

- A. Bluetooth
- B. Ethernet
- C. Token ring
- D. Asynchronous Transfer Mode (ATM)

Answer: D

NEW QUESTION 130

There is not universal agreement on the names of the layers in the TCP/IP networking model. Which of the following is one of the functions of the bottom layer which is sometimes called the Network Access or Link Layer?

- A. Provides end-to-end data delivery service for user applications
- B. Handles the routing of the data packets over the network
- C. Manages IP addressing and encryption for data packets
- D. Defines the procedures for interfacing with Ethernet devices

Answer: D

NEW QUESTION 135

You work as a Network Administrator for NetTech Inc. When you enter <http://66.111.64.227> in the browser's address bar, you are able to access the site. But, you are unable to access the site when you enter <http://www.uCertify.com>. What is the most likely cause?

- A. DNS entry is not available for the host nam
- B. The site's Web server is offlin
- C. The site's Web server has heavy traffi
- D. WINS server has no NetBIOS name entry for the serve

Answer: A

NEW QUESTION 140

To be considered a strong algorithm, an encryption algorithm must be which of the following?

- A. Secret
- B. Well-known
- C. Confidential
- D. Proprietary

Answer: B

NEW QUESTION 142

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 147

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 150

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 154

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 158

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 deliver
- D. Rules are often misinterpret

Answer: D

NEW QUESTION 159

Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?

- A. Analysis of encrypted traffic
- B. Provide insight into network traffic
- C. Detection of network operations problems
- D. Provide logs of network traffic that can be used as part of other security measure
- E. Inexpensive to manage
- F. B, C, and D
- G. A, C, and E
- H. B, D, and E
- I. A, B, and C

Answer: C

NEW QUESTION 164

Which of the following is a characteristic of hash operations?

- A. Asymmetric
- B. Non-reversible
- C. Symmetric
- D. Variable length output

Answer: D

NEW QUESTION 168

Validating which vulnerabilities in a network environment are able to be exploited by an attacker is called what?

- A. Anomaly detection
- B. Vulnerability scanning
- C. Perimeter assessment
- D. Penetration testing

Answer: B

NEW QUESTION 170

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 174

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 178

What is SSL primarily used to protect you against?

- A. Session modification
- B. SQL injection
- C. Third-patty sniffing
- D. Cross site scripting

Answer: C

NEW QUESTION 182

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 186

When using Pretty Good Privacy (PGP) to digitally sign a message, the signature is created in a two-step process. First, the message to be signed is submitted to PGP's cryptographic hash algorithm. What is one of the hash algorithms used by PGP for this process?

- A. Blowfish
- B. DES
- C. SHA-1
- D. Cast

Answer: C

NEW QUESTION 189

Which of the following are network connectivity devices?

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

- A. Network analyzer
- B. Bridge
- C. Router
- D. Firewall
- E. Repeater
- F. Hub

Answer: BCEF

NEW QUESTION 190

Which of the following protocols are used to provide secure communication between a client and a server over the Internet?

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

- A. SSL
- B. HTTP
- C. TLS
- D. SNMP

Answer: AC

NEW QUESTION 195

Which Windows event log would you look in if you wanted information about whether or not a specific driver was running at start up?

- A. Application
- B. System
- C. Startup
- D. Security

Answer: B

NEW QUESTION 196

Which of the following systems acts as a NAT device when utilizing VMware in NAT mode?

- A. Guest system
- B. Local gateway
- C. Host system
- D. Virtual system

Answer: D

NEW QUESTION 199

A Host-based Intrusion Prevention System (HIPS) software vendor records how the Firefox Web browser interacts with the operating system and other applications, and identifies all areas of Firefox functionality. After collecting all the data about how Firefox should work, a database is created with this information, and it is fed into the HIPS software. The HIPS then monitors Firefox whenever it's in use. What feature of HIPS is being described in this scenario?

- A. Signature Matching
- B. Application Behavior Monitoring
- C. Host Based Sniffing
- D. Application Action Modeling

Answer: B

NEW QUESTION 200

You are examining an IP packet with a header of 40 bytes in length and the value at byte 0 of the packet header is 6. Which of the following describes this packet?

- A. This is an IPv4 packet; the protocol encapsulated in the payload is unspecified
- B. This is an IPv4 packet with a TCP payload
- C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecified
- D. This is an IPv6 packet with a TCP payload

Answer: C

NEW QUESTION 201

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 wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?

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

- A. rm private.txt #11 Nov 2009 02:59:58 am
- B. touch -d "11 Nov 2009 02:59:58 am" private.txt
- C. touch private.txt #11 Nov 2009 02:59:58 am
- D. touch -t 200911110259.58 private.txt

Answer: BD

NEW QUESTION 204

What is the function of the TTL (Time to Live) field in IPv4 and the Hop Limit field in IPv6 In an IP Packet header?

- A. These fields are decremented each time a packet is retransmitted to minimize the possibility of routing loop
- B. These fields are initialized to an initial value to prevent packet fragmentation and fragmentation attack
- C. These fields are recalculated based on the required time for a packet to arrive at its destinatio
- D. These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traverse

Answer: A

NEW QUESTION 205

Which of the following statements best describes where a border router is normally placed?

- A. Between your firewall and your internal network
- B. Between your firewall and DNS server
- C. Between your ISP and DNS server
- D. Between your ISP and your external firewall

Answer: D

NEW QUESTION 209

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 214

You work as a Network Administrator for Tech Perfect Inc. The company has a Linux-based network. You want to kill a process running on a Linux server. Which of the following commands will you use to know the process identification number (PID) of the process?

- A. killall
- B. ps
- C. getpid
- D. kill

Answer: B

NEW QUESTION 217

You work as a Network Administrator for Net World Inc. The company has a Linux-based network. For testing purposes, you have configured a default IP-table with several filtering rules. You want to reconfigure the table. For this, you decide to remove the rules from all the chains in the table. Which of the following commands will you use?

- A. IPTABLES -D
- B. IPTABLES -A
- C. IPTABLES -h
- D. IPTABLES -F

Answer: D

NEW QUESTION 222

Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose two.

- A. It reduces the need for globally unique IP addresse
- B. It allows external network clients access to internal service
- C. It allows the computers in a private network to share a global, ISP assigned address to connect to the Interne
- D. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Hos

Answer: AC

NEW QUESTION 226

Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

- A. Hardening
- B. Authentication
- C. Cryptography
- D. Sanitization

Answer: A

NEW QUESTION 231

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 232

You work as an Administrator for McRoberts Inc. The company has a Linux-based network. You are logged in as a non-root user on your client computer. You want to delete all files from the /garbage directory. You want that the command you will use should prompt for the root user password. Which of the following commands will you use to accomplish the task?

- A. rm -rf /garbage*
- B. del /garbage/*.*
- C. rm -rf /garbage* /SU
- D. su -c "RM -rf /garbage*"

Answer: D

NEW QUESTION 234

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 237

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 bag
- B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody
- C. Take photographs of all persons who have had access to the computer
- D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag

Answer: D

NEW QUESTION 241

When are Group Policy Objects (GPOs) NOT applied automatically to workstations?

- A. At 90-minute intervals
- B. At logon
- C. Every time Windows Explorer is launched
- D. At boot-up

Answer: C

NEW QUESTION 243

While using Wireshark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below. Based on what you see below, which of the following would you recommend to prevent future damage to your database?

```
POST /samplelogin.cfm HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (X11; U; en-US;) Gecko/200910 Ubuntu/8.4
Firefox/2.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/
Cookie: SID=026DCB9CBBF2339C2CBFAEBA8F1DD656;
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
username='a'&password=DROP+TABLE+members;+--
```

- A. Use ssh to prevent a denial of service attack

- B. Sanitize user inputs to prevent injection attacks
- C. Authenticate users to prevent hackers from using your database
- D. Use https to prevent hackers from inserting malware

Answer: D

NEW QUESTION 246

Which of the following are examples of Issue-Specific policies all organizations should address?

- A. Perimeter filtering guides, break times for employees, desktop neatness and backup procedure
- B. Rogue wireless access points, auditing, break time for employees and organizational structur
- C. Audit logs, physical access, mission statements and network protocols use
- D. Backup requirements, employee monitoring, physical access and acceptable us

Answer: D

NEW QUESTION 251

Which of the following statements about policy is FALSE?

- A. A well-written policy contains definitions relating to "what" to d
- B. A well-written policy states the specifics of "how" to do somethin
- C. Security policy establishes what must be done to protect information stored on computer
- D. Policy protects people who are trying to do the right thin

Answer: D

NEW QUESTION 252

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we- are-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?

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

- A. They allow an attacker to conduct a buffer overflo
- B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime acces
- C. They allow an attacker to replace utility programs that can be used to detect the attacker's activit
- D. They allow an attacker to run packet sniffers secretly to capture password

Answer: BCD

NEW QUESTION 257

Which of the following networking topologies uses a hub to connect computers?

- A. Bus
- B. Ring
- C. Star
- D. Cycle

Answer: C

NEW QUESTION 258

Which of the following is a new Windows Server 2008 feature for the Remote Desktop Protocol (RDP)?

- A. The ability to allow the administrator to choose a port other than the default RDP port (TCP 3389)
- B. The ability to support connections from mobile devices like smart phones
- C. The ability to allow clients to authenticate over TLS
- D. The ability to allow clients to execute individual applications rather than using a terminal desktop

Answer: D

NEW QUESTION 261

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The GSEC Practice Test Here](#)