

GIAC

Exam Questions GSEC

GIAC Security Essentials Certification



NEW QUESTION 1

Which of the following is a Layer 3 device that will typically drop directed broadcast traffic?

- A. Hubs
- B. Bridges
- C. Routers
- D. Switches

Answer: C

NEW QUESTION 2

Which of the following is a valid password for a system with the default "Password must meet complexity requirements" setting enabled as part of the GPO Password policy requirements?

- A. The Cat Chased its Tail All Night
- B. disk ACCESS failed
- C. SETI@HOME
- D. SaNS2006

Answer: D

NEW QUESTION 3

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 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

Which of the following SIP methods is used to setup a new session and add a caller?

- A. ACK
- B. BYE
- C. REGISTER
- D. INVITE
- E. CANCEL

Answer: D

NEW QUESTION 6

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 7

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 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

Two clients connecting from the same public IP address (for example - behind the same NAT firewall) can connect simultaneously to the same web server on the Internet, provided what condition is TRUE?

- A. The server is not using a well-known port
- B. The server is on a different network
- C. The client-side source ports are different
- D. The clients are on different subnets

Answer: C

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

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 14

Which of the following choices accurately describes how PGP works when encrypting email?

- A. PGP encrypts the message with the recipient's public key, then encrypts this key with a random asymmetric key
- B. PGP creates a random asymmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
- C. PGP creates a random symmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
- D. PGP encrypts the message with the recipient's public key, then encrypts this key with a random symmetric key

Answer: B

NEW QUESTION 15

What is the discipline of establishing a known baseline and managing that condition known as?

- A. Configuration deployment
- B. Observation discipline
- C. Security establishment
- D. Configuration management

Answer: C

NEW QUESTION 19

Which of the following protocols work at the Session layer of the OSI model? Each correct answer represents a complete solution. Choose all that apply.

- A. Border Gateway Multicast Protocol (BGMP)
- B. Internet Security Association and Key Management Protocol (ISAKMP)
- C. Trivial File Transfer Protocol (TFTP)
- D. User Datagram Protocol (UDP)

Answer: AB

NEW QUESTION 20

Which of the following fields CANNOT be hashed by Authentication Header (AH) in transport mode?

- A. Length
- B. Source IP

- C. TTL
- D. Destination IP

Answer: C

NEW QUESTION 23

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 24

You work as a Network Administrator for World Perfect Inc. The company has a Linux-based network. You have configured a Linux Web server on the network. A user complains that the Web server is not responding to requests. The process list on the server shows multiple instances of the HTTPD process. You are required to stop the Web service. Which of the following commands will you use to resolve the issue?

- A. killall httpd
- B. endall httpd
- C. kill httpd
- D. end httpd

Answer: A

NEW QUESTION 27

Which of the following statements about IPSec are true?
Each correct answer represents a complete solution. Choose two.

- A. It uses Internet Protocol (IP) for data integrity
- B. It uses Authentication Header (AH) for data integrity
- C. It uses Password Authentication Protocol (PAP) for user authentication
- D. It uses Encapsulating Security Payload (ESP) for data confidentiality

Answer: BD

NEW QUESTION 31

A US case involving malicious code is brought to trial. An employee had opened a helpdesk ticket to report specific instances of strange behavior on her system. The IT helpdesk representative collected information by interviewing the user and escalated the ticket to the system administrators. As the user had regulated and sensitive data on her computer, the system administrators had the hard drive sent to the company's forensic consultant for analysis and configured a new hard drive for the user. Based on the recommendations from the forensic consultant and the company's legal department, the CEO decided to prosecute the author of the malicious code. During the court case, which of the following would be able to provide direct evidence?

- A. The IT helpdesk representative
- B. The company CEO
- C. The user of the infected system
- D. The system administrator who removed the hard drive

Answer: C

NEW QUESTION 35

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 37

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 38

Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 39

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 41

What is the command-line tool for Windows XP and later that allows administrators the ability to get or set configuration data for a very wide variety of computer and user account settings?

- A. IPCONFIG.EXE
- B. NETSTAT.EXE
- C. WMIC.EXE
- D. C0NF1G.EXE

Answer: C

NEW QUESTION 44

Your IT security team is responding to a denial of service attack against your server. They have taken measures to block offending IP addresses. Which type of threat control is this?

- A. Detective
- B. Preventive
- C. Responsive
- D. Corrective

Answer: D

NEW QUESTION 46

Your customer wants to make sure that only computers he has authorized can get on his Wi-Fi. What is the most appropriate security measure you can recommend?

- A. A firewall
- B. WPA encryption
- C. WEP encryption
- D. Mac filtering

Answer: D

NEW QUESTION 50

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 55

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

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

Answer: D

NEW QUESTION 56

What is the name of the Windows XP/2003 tool that you can use to schedule commands to be executed on remote systems during off-peak hours?

- A. SHTASKS.EXE
- B. SCHEDULETSKS.EXE
- C. SCHEDULR.EXE
- D. SCHRUN.EXE

Answer: A

NEW QUESTION 57

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 59

Which of the following would be a valid reason to use a Windows workgroup?

- A. Lower initial cost
- B. Simplicity of single sign-on
- C. Centralized control
- D. Consistent permissions and rights

Answer: D

NEW QUESTION 60

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 61

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 65

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 processe
- C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individua
- D. It establishes the users' identity and ensures that the users are who they say they ar

Answer: D

NEW QUESTION 68

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 72

You ask your system administrator to verify user compliance with the corporate policies on password strength, namely that all passwords will have at least one

numeral, at least one letter, at least one special character and be 15 characters long. He comes to you with a set of compliance tests for use with an offline password cracker. They are designed to examine the following parameters of the password:

- * they contain only numerals
- * they contain only letters
- * they contain only special characters
- * they contain only letters and numerals
- " they contain only letters and special characters
- * they contain only numerals and special characters

Of the following, what is the benefit to using this set of tests?

- A. They are focused on cracking passwords that use characters prohibited by the password policy
- B. They find non-compliant passwords without cracking compliant password
- C. They are focused on cracking passwords that meet minimum complexity requirements
- D. They crack compliant and non-compliant passwords to determine whether the current policy is strong enough

Answer: B

NEW QUESTION 77

Which of the following monitors program activities and modifies malicious activities on a system?

- A. Back door
- B. HIDS
- C. NIDS
- D. RADIUS

Answer: B

NEW QUESTION 80

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 cal
- B. Clear relevant system log file
- C. Getting permission to run the sca
- D. Scheduling the scan to run before OS update

Answer: C

NEW QUESTION 81

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 85

An employee is currently logged into the corporate web server, without permission. You log into the web server as 'admin" and look for the employee's username: "dmaul" using the "who" command. This is what you get back:

- A. The contents of the /var/log/messages file has been altered
- B. The contents of the bash history file has been altered
- C. The contents of the utmp file has been altered
- D. The contents of the http logs have been altered

Answer: B

NEW QUESTION 86

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as.

- A. False negative
- B. False positive
- C. True positive
- D. True negative

Answer: B

NEW QUESTION 88

Which of the following files contains the shadowed password entries in Linux?

- A. /etc/passwd
- B. /etc/shadow
- C. /etc/profile
- D. /etc/shdpwd

Answer: B

NEW QUESTION 92

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 96

How often is session information sent to the web server from the browser once the session information has been established?

- A. With any change in session data
- B. With every subsequent request
- C. With any hidden form element data
- D. With the initial request to register the session

Answer: A

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 104

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. He is working as a root user on the Linux operating system. He wants to delete his private.txt file from his operating system. He knows that the deleted file can be recovered easily. Hence, he wants to delete the file securely. He wants to hide the shredding, and so he desires to add a final overwrite of the file private.txt with zero. Which of the following commands will John use to accomplish his task?

- A. rmdir -v private.txt
- B. shred -vfu private.txt
- C. shred -vfuz private.txt
- D. rm -vf private.txt

Answer: C

NEW QUESTION 105

CORRECT TEXT

Fill in the blank with the correct answer to complete the statement below.

The permission is the minimum required permission that is necessary for a user to enter a directory and list its contents.

A.

Answer: Read

NEW QUESTION 106

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 107

The process of enumerating all hosts on a network defines which of the following activities?

- A. Port scanning
- B. Vulnerability scanning
- C. GPS mapping
- D. Network mapping

Answer: D

NEW QUESTION 111

Which of the following applications cannot proactively detect anomalies related to a computer?

- A. Firewall installed on the computer
- B. NIDS
- C. HIDS
- D. Anti-virus scanner

Answer: B

NEW QUESTION 116

It is possible to sniff traffic from other hosts on a switched Ethernet network by impersonating which type of network device?

- A. Switch
- B. Bridge
- C. Hub
- D. Router

Answer: D

NEW QUESTION 119

You are implementing wireless access at a defense contractor. Specifications say, you must implement the AES Encryption algorithm. Which encryption standard should you choose?

- A. WPA
- B. TKIP
- C. WEP
- D. WPA 2

Answer: D

NEW QUESTION 121

Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP)?

- A. TCP port 443
- B. UDP port 161
- C. TCP port 110
- D. UDP port 1701

Answer: D

NEW QUESTION 122

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 126

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 accomplishe
- B. He will be able to check the file system type on each computer's hard dis
- C. He will be able to accomplish all the task
- D. He will be able to check all available security updates and shared folder

Answer: C

NEW QUESTION 130

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 133

Which port category does the port 110 fall into?

- A. Well known port
- B. Dynamic port
- C. Private port
- D. Application port

Answer: A

NEW QUESTION 138

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 142

Which of the following areas of a network contains DNS servers and Web servers for Internet users?

- A. VPN
- B. MMZ
- C. VLAN
- D. DMZ

Answer: D

NEW QUESTION 147

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 149

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 152

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 156

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 159

Which of the following is an advantage of an Intrusion Detection System?

- A. It is a mature technolog
- B. It is the best network securit
- C. It never needs patchin
- D. It is a firewall replacemen

Answer: A

NEW QUESTION 163

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 167

Which of the following items are examples of preventive physical controls? Each correct answer represents a complete solution. Choose three.

- A. Biometric access controls
- B. Closed-circuit television monitors
- C. Fire extinguishers
- D. Locks and keys

Answer: ACD

NEW QUESTION 169

Which of the following defines the communication link between a Web server and Web applications?

- A. CGI
- B. PGP
- C. Firewall
- D. IETF

Answer: A

NEW QUESTION 174

What is SSL primarily used to protect you against?

- A. Session modification

- B. SQL injection
- C. Third-party sniffing
- D. Cross site scripting

Answer: C

NEW QUESTION 178

What is the main reason that DES is faster than RSA?

- A. DES is less secure
- B. DES is implemented in hardware and RSA is implemented in software
- C. Asymmetric cryptography is generally much faster than symmetric
- D. Symmetric cryptography is generally much faster than asymmetric

Answer: D

NEW QUESTION 181

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 186

Which of the following is an advantage of private circuits versus VPNs?

- A. Flexibility
- B. Performance guarantees
- C. Cost
- D. Time required to implement

Answer: B

NEW QUESTION 189

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 193

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 194

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 computation
- B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfish
- C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computation
- 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 196

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 corrupt
- B. The packets may have been accidentally routed onto the Internet
- C. The packets may be deliberately spoofed by an attacker

- 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 199

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 204

An employee attempting to use your wireless portal reports receiving the error shown below. Which scenario is occurring?

- A. A denial-of-service attack is preventing a response from the porta
- B. Another access point is deauthenticating legitimate client
- C. The encrypted data is being intercepted and decrypte
- D. Another access point is attempting to intercept the dat

Answer: D

NEW QUESTION 207

Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?

- A. 127.0.0.100
- B. 169.254.1.50
- C. 10.254.1.50
- D. 172.35.1.100

Answer: C

NEW QUESTION 210

IPS devices that are classified as "In-line NIDS" devices use a combination of anomaly analysis, signature-based rules, and what else to identify malicious events on the network?

- A. Firewall compatibility rules
- B. Application analysis
- C. ICMP and UDP active scanning
- D. MAC address filtering

Answer: B

NEW QUESTION 213

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 214

You are the security director for an off-shore banking site. From a business perspective, what is a major factor to consider before running your new vulnerability scanner against the company's business systems?

- A. It may harm otherwise healthy system
- B. It may produce false negative result
- C. It may generate false positive result
- D. It may not return enough benefit for the cos

Answer: C

NEW QUESTION 217

What does the "x" character in the second field of the user account record of the /etc/passwd file indicate?

- A. The user account is using a shadow passwor
- B. The user account is shared by more than one use
- C. The user account is disable
- D. The user account does not exis

Answer: A

NEW QUESTION 218

Which of the following statements about DMZ are true?

Each correct answer represents a complete solution. Choose two.

- A. It is the boundary between the Internet and a private networ
- B. It is an anti-virus software that scans the incoming traffic on an internal network
- C. It contains company resources that are available on the Internet, such as Web servers and FTP server
- D. It contains an access control list (ACL).

Answer: AC

NEW QUESTION 221

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 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

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 230

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 232

Which of the following is used to allow or deny access to network resources?

- A. Spoofing
- B. ACL
- C. System hardening

D. NFS

Answer: B

NEW QUESTION 235

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 240

Included below is the output from a resource kit utility run against local host.
Which command could have produced this output?

- A. Schtasks
- B. Task kill
- C. SC
- D. Task list

Answer: D

NEW QUESTION 244

An IT security manager is trying to quickly assess the risks associated with not implementing a corporate firewall system. What sort of risk assessment is most appropriate?

- A. Annualized Risk Assessment
- B. Qualitative risk assessment
- C. Quantitative risk assessment
- D. Technical Risk Assessment
- E. Iterative Risk Assessment

Answer: B

NEW QUESTION 249

In trace route results, what is the significance of an * result?

- A. A listening port was identified
- B. A reply was returned in less than a second
- C. The target host was successfully reached
- D. No reply was received for a particular host

Answer: D

NEW QUESTION 250

.....

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](#)