GIAC

Exam Questions GSEC

GIAC Security Essentials Certification

NEW QUESTION 1
Which of the following protocols is used to send e-mails on the Internet?

A. SMTP
B. IMAP4
C. POP3
D. HTTP

Answer: A

NEW QUESTION 2
Which class of IDS events occur when the IDS fails to alert on malicious data?

A. True Negative
B. True Positive
C. False Positive
D. False Negative

Answer: D

NEW QUESTION 3
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 4
The Windows 'tracert' begins by sending what type of packet to the destination host?

A. A UDP packet with a TTL of 1
B. An ICMP Echo Request
C. An ICMP Router Discovery
D. An ICMP Echo Reply

Answer: A

NEW QUESTION 5
Which Defense-in-Depth model involves identifying various means by which threats can become manifest and providing security mechanisms to shut them down?

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

Answer: A

NEW QUESTION 6
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 7
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 8
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 9
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 10
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 10
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 11
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 integrit
B. It uses Authentication Header (AH) for data integrit
C. It uses Password Authentication Protocol (PAP) for user authenticatio
D. It uses Encapsulating Security Payload (ESP) for data confidentialit

Answer: BD

NEW QUESTION 12
Your software developer comes to you with an application that controls a user device. The application monitors its own behavior and that of the device and creates log files. The log files are expected to grow steadily and rapidly. Your developer currently has the log files stored in the /bin folder with the application binary.
Where would you suggest that the developer store the log files?

A. /var/log
B. /etc/log
C. /usr/log
D. /tmp/log
E. /dev/log

Answer: A

NEW QUESTION 13
Which of the following statements about Microsoft's VPN client software is FALSE?

A. The VPN interface can be figured into the route tabl
B. The VPN interface has the same IP address as the interface to the network it's been specified to protec
C. The VPN client software is built into the Windows operating syste
D. The VPN tunnel appears as simply another adapte

Answer: B

NEW QUESTION 17
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 startup shell of Maria from bash to tcsh. Which of the following commands will John use to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. usermod -s
B. chage
C. usermod -u
D. useradd -s

Answer: AD

NEW QUESTION 22
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 25
For most organizations, which of the following should be the highest priority when it comes to physical security concerns?

A. Controlling ingress and egress
B. Controlling access to workstations
C. Ensuring employee safety
D. Controlling access to servers
E. Protecting physical assets

Answer: C

NEW QUESTION 27
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 28
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 33
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 37
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 40
In PKI, when someone wants to verify that the certificate is valid, what do they use to decrypt the signature?

A. Receiver's digital signature
B. X.509 certificate CA's private key
C. Secret passphrase
D. CA's public key

Answer: D

NEW QUESTION 45
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 50
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. SCHTASKS.EXE
B. SCHEDULETSKS.EXE
C. SCHEDULR.EXE
D. SCHRUN.EXE

Answer: A

NEW QUESTION 54
You are going to upgrade your hard disk's file system from FAT to NTFS. What are the major advantages of the NTFS file system over FAT16 and FAT32 file systems?
Each correct answer represents a complete solution. Choose all that apply.

A. NTFS gives better file security than FAT16 and FAT32.
B. Automatic backu
C. NTFS file system supports for larger hard disk
D. NTFS give improved disk compression than FAT16 and FAT32.

Answer: ACD

NEW QUESTION 58
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 61
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 66
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 70
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 72
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 73
Which of the following is generally practiced by the police or any other recognized governmental authority?

A. Spoofing
B. SMB signing
C. Wiretapping
D. Phishing

Answer: C

NEW QUESTION 76
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 priontized 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 80
Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

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

Answer: C

NEW QUESTION 83
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 87
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You want to mount an SMBFS share from a Linux workstation. Which of the following commands can you use to accomplish the task?
Each correct answer represents a complete solution. Choose two.

A. smbmount
B. mount smb
C. smbfsmount
D. mount -t smbfs

Answer: AD

NEW QUESTION 91
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 syste
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 syste
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 machin
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 syste
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 systems RAM is available to the guest operating syste

Answer: E

NEW QUESTION 93
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 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 iamabadserveriamabadserver.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 96
Which of the following statements regarding the Secure Sockets Layer (SSL) security model are true?
Each correct answer represents a complete solution. Choose two.

A. The client can optionally authenticate the serve
B. The client always authenticates the serve
C. The server always authenticates the clien
D. The server can optionally authenticate the clien

Answer: BD

NEW QUESTION 100
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 101
Which of the following is a backup strategy?

A. Differential
B. Integrational
C. Recursive
D. Supplemental

Answer: A

NEW QUESTION 103
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 105
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 107
When you log into your Windows desktop what information does your Security Access Token (SAT) contain?

A. The Security ID numbers (SIDs) of all the groups to which you belong
B. A list of cached authentications
C. A list of your domain privileges
D. The Security ID numbers (SIDs) of all authenticated local users

Answer: C

NEW QUESTION 111
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 manuall
B. Rerun the system patching routine
C. Contact the incident response tea
D. Ignore the findings as false positive

Answer: A

NEW QUESTION 114
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 117
Which access control mechanism requires a high amount of maintenance since all data must be classified, and all users granted appropriate clearance?

A. Mandatory
B. Discretionary
C. Rule set-based
D. Role-Based

Answer: A

NEW QUESTION 122
What is the maximum number of connections a normal Bluetooth device can handle at one time?

A. 2
B. 4
C. 1
D. 8
E. 7

Answer: E

NEW QUESTION 125
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 126
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 130
You have implemented a firewall on the company's network for blocking unauthorized network connections. Which of the following types of security control is implemented in this case?

A. Detective
B. Preventive
C. Directive
D. Corrective

Answer: B

NEW QUESTION 135
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 136
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 139
You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

A. Take a full backup daily with the previous night's tape taken offsit
B. Take a full backup daily and use six-tape rotatio
C. Take a full backup on Monday and an incremental backup on each of the following weekday
D. Keep Monday's backup offsit
E. Take a full backup on alternate days and keep rotating the tape
F. Take a full backup on Monday and a differential backup on each of the following weekday
G. Keep Monday's backup offsit
H. Take a full backup daily with one tape taken offsite weekl

Answer: A

NEW QUESTION 142
Which of the following is the FIRST step in performing an Operational Security (OP5EC) Vulnerabilities Assessment?

A. Assess the threat
B. Assess vulnerabilities of critical information to the threat
C. Conduct risk versus benefit analysis
D. Implement appropriate countermeasures
E. Identification of critical information

Answer: E

NEW QUESTION 144
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
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 150
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 152
Which of the following is TRUE regarding the ability of attackers to eavesdrop on wireless communications?

A. Eavesdropping attacks cannot be performed through concrete wall
B. Eavesdropping attacks can take place from miles awa
C. Eavesdropping attacks are easily detected on wireless network
D. Eavesdropping attacks require expensive device

Answer: B

NEW QUESTION 155
What type of attack can be performed against a wireless network using the tool Kismet?

A. IP spoofing
B. Eavesdropping
C. Masquerading
D. Denial of Service

Answer: B

NEW QUESTION 158
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 161
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 162
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 165
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 166
How is a Distributed Denial of Service (DDOS) attack distinguished from a regular DOS attack?

A. DDOS attacks are perpetrated by many distributed host
B. DDOS affects many distributed target
C. Regular DOS focuses on a single route
D. DDOS affects the entire Interne

Answer: A

NEW QUESTION 169
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 174
Against policy, employees have installed Peer-to-Peer applications on their workstations and they are using them over TCP port 80 to download files via the company network from other Peer-to-Peer users on the Internet. Which of the following describes this threat?

A. Firewall subversion
B. Backdoor installation
C. Malicious software infection
D. Phishing attempt

Answer: A

NEW QUESTION 177
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 180
Many IIS servers connect to Microsoft SQL databases. Which of the following statements about SQL server security is TRUE?

A. SQL Server patches are part of the operating system patche
B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web applicatio
C. It is good practice to never use integrated Windows authentication for SQL Serve
D. It is good practice to not allow users to send raw SQL commands to the SQL Serve

Answer: D

NEW QUESTION 184
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 189
A new data center is being built where customer credit information will be processed and stored. Which of the following actions will help maintain the confidentiality of the data?

A. Environmental sensors in the server room
B. Access control system for physical building
C. Automated fire detection and control systems
D. Frequent off-site backup of critical databases

Answer: B

NEW QUESTION 190
In addition to securing the operating system of production honey pot hosts, what is recommended to prevent the honey pots from assuming the identities of production systems that could result in the denial of service for legitimate users?

A. Deploy the honey pot hosts as physically close as possible to production system
B. Deploy the honey pot hosts in an unused part of your address spac
C. Deploy the honey pot hosts to only respond to attack
D. Deploy the honey pot hosts on used address spac

Answer: B

NEW QUESTION 191
Which of the following TCP packet flags indicates that host should IMMEDIATELY terminate the connection containing the packet?

A. FIN
B. URG
C. SYN
D. RST

Answer: D

NEW QUESTION 196
What is the most secure way to address an unused Windows service so it cannot be exploited by malware?

A. Firewall it
B. Set to manual startup
C. Disable it
D. Uninstall it

Answer: D

NEW QUESTION 200
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 203
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 204
Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

A. IMAP
B. SNMP
C. POP3
D. SMTP

Answer: A

NEW QUESTION 205
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 206
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 211
Regarding the UDP header below, what is the length in bytes of the UDP datagrarn?
04 1a 00 a1 00 55 db 51

A. 161
B. 81
C. 219
D. 85

Answer: D

NEW QUESTION 213
You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based
network. You have created a folder named Report. You have made David the owner of the folder. The members of a group named JAdmin can access the folder and have Read, Write, and Execute permissions. No other user can access the folder. You want to ensure that the members of the JAdmin group do not have Write permission on the folder. Also, you want other users to have Read permission on the Report folder.
Which of the following commands will you use to accomplish the task?

A. chmod 777 report
B. chown david.jadmin report
C. chmod 555 report
D. chmod 754 report

Answer: D

NEW QUESTION 218
Which of the following is TRUE regarding Ethernet?

A. Stations are not required to monitor their transmission to check for collision
B. Several stations are allowed to be transmitting at any given time within a single collision domai
C. Ethernet is shared medi
D. Stations are not required to listen before they transmi

Answer: C

NEW QUESTION 220
Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

A. It uses TCP port 443 as the default por
B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure sit
C. It is a protocol used to provide security for a database server in an internal networ
D. It uses TCP port 80 as the default por

Answer: AB

NEW QUESTION 222
How many bytes does it take to represent the hexadecimal value OxFEDCBA?

A. 12
B. 2
C. 3
D. 6

Answer: C

NEW QUESTION 227
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 229
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 234
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 235
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?

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 240
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 244
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 247
While using Wire shark 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?

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 248
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 249
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 254
.....

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