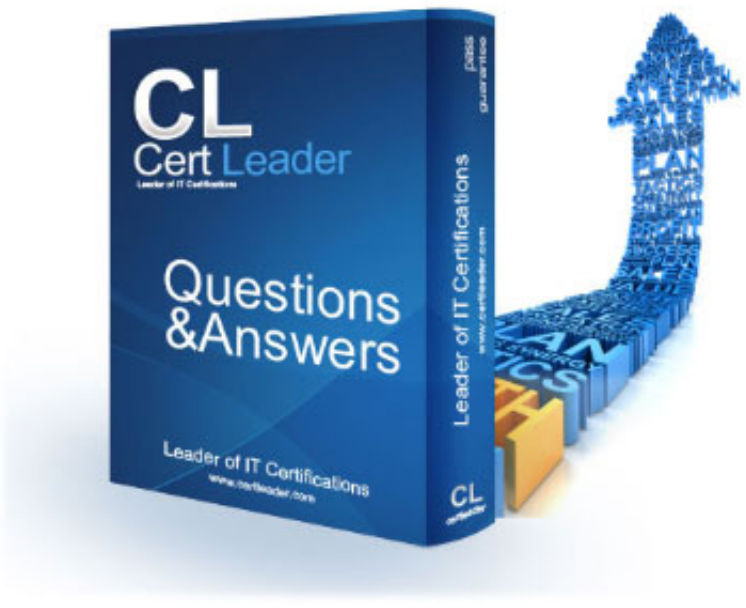
GSEC Dumps

GIAC Security Essentials Certification

https://www.certleader.com/GSEC-dumps.html



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
What is the maximum passphrase length in Windows 2000/XP/2003?

A. 255 characters
B. 127 characters
C. 95 characters
D. 63 characters

Answer: B

NEW QUESTION 3
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 4
Which of the following radio frequencies is used by the IEEE 802.11a wireless network?

A. 3.7 GHz
B. 7.0 GHz
C. 2.4 GHz
D. 5.0 GHz

Answer: D

NEW QUESTION 5
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 6
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 7
You work as a Network Administrator for McNeil Inc. You are installing an application. You want to view the log file whenever a new entry is added to the /var/log/messages log file. Which of the following commands will you use to accomplish this?

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

Answer: B

NEW QUESTION 8
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 9
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 10
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 10
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 11
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 possibl
B. Make sure to allow all TCP 3389 traffic through the external firewal
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 vulnerabilitie

Answer: B

NEW QUESTION 15
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 16
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 20
What does an attacker need to consider when attempting an IP spoofing attack that relies on guessing Initial Sequence Numbers (ISNs)?

A. These attacks work against relatively idle server
B. These attacks rely on a modified TCP/IP stack to functio
C. These attacks can be easily traced back to the sourc
D. These attacks only work against Linux/Unix host

Answer: A

NEW QUESTION 22
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 26
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 29
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 33
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 34
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Privacy policy
B. Backup policy
C. User password policy
D. Network security policy

Answer: A

NEW QUESTION 38
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 42
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 44
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 47
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 52
What type of formal document would include the following statement?
Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal application of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies, and if there is any uncertainty, employees should consult their supervisor or manager.

A. Company privacy statement
B. Remote access policy
C. Acceptable use policy
D. Non-disclosure agreement

Answer: C

NEW QUESTION 53
SSL session keys are available in which of the following lengths?

A. 40-bit and 128-bi
B. 64-bit and 128-bi
C. 128-bit and 1,024-bi
D. 40-bit and 64-bi

Answer: A

NEW QUESTION 56
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 57
Which of the following is a backup strategy?

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

Answer: A

NEW QUESTION 61
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 62
Your CIO has found out that it is possible for an attacker to clone your company's RFID (Radio Frequency ID) based key cards. The CIO has tasked you with finding a way to ensure that anyone entering the building is an employee. Which of the following authentication types would be the appropriate solution to this problem?

A. Mandatory Access Controls
B. Bell-LaPadula
C. Two-Factor
D. TACACS

Answer: C

NEW QUESTION 67
Which of the following describes software technologies that improve portability, manageability, and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?

A. System registry
B. Group Policy
C. Application virtualization
D. System control

Answer: C

NEW QUESTION 72
When a host on a remote network performs a DNS lookup of www.google.com, which of the following is likely to provide an Authoritative reply?

A. The local DNS server
B. The top-level DNS server for .com
C. The DNS server for google.com
D. The root DNS server

Answer: A

NEW QUESTION 73
Which of the following is an UDP based protocol?

A. telnet
B. SNMP
C. IMAP
D. LDAP

Answer: B

NEW QUESTION 76
Which of the following protocols provides maintenance and error reporting function?

A. UDP
B. ICMP
C. PPP
D. IGMP

Answer: B

NEW QUESTION 79
Which of the following Linux commands can change both the username and group name a file belongs to?

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

Answer: B

NEW QUESTION 81
Which of the following attack vectors are addressed by Xinetd and TCP Wrappers?

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

Answer: B

NEW QUESTION 83
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 86
What file instructs programs like Web spiders NOT to search certain areas of a site?

A. Robots.txt
B. Restricted.txt
C. Spider.txt
D. Search.txt

Answer: A

NEW QUESTION 90
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 93
What is the motivation behind SYN/FIN scanning?

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

Answer: B

NEW QUESTION 97
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 101
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 105
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 109
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 111
Which of the following is a required component for successful 802.lx network authentication?

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

Answer: A

NEW QUESTION 114
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 118
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 123
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 125
Which of the following services resolves host name to IP Address?

A. Computer Browser
B. DHCP
C. DNS
D. WINS

Answer:

C

NEW QUESTION 128
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 131
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 134
What is the main problem with relying solely on firewalls to protect your company's sensitive data?

A. Their value is limited unless a full-featured Intrusion Detection System is use
B. Their value is limited because they cannot be changed once they are configure
C. Their value is limited because operating systems are now automatically patche
D. Their value is limited because they can be bypassed by technical and non-technical mean

Answer: D

NEW QUESTION 139
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 144
Your system has been infected by malware. Upon investigation, you discover that the malware propagated primarily via email. The malware attacked known vulnerabilities for which patches are available, but due to problems with your configuration management system you have no way to know which systems have been patched and which haven't, slowing your progress in patching your network. Of the following, which solution would you use to protect against this propagation vector?

A. Encrypt the emails on the server
B. Scan and block suspect email attachments at the email server
C. Install a firewall between the email server and the Internet
D. Separate the email server from the trusted portions of the network

Answer: B

NEW QUESTION 149
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 152
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 155
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 157
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 162
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 167
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 168
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 networ
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 173
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 174
If Linux server software is a requirement in your production environment which of the following should you NOT utilize?

A. Debian
B. Mandrake
C. Cygwin
D. Red Hat

Answer: C

NEW QUESTION 178
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 182
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 183
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 186

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 189
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 194
The previous system administrator at your company used to rely heavily on email lists, such as vendor lists and Bug Traq to get information about updates and patches. While a useful means of acquiring data, this requires time and effort to read through. In an effort to speed things up, you decide to switch to completely automated updates and patching. You set up your systems to automatically patch your production servers using a cron job and a scripted apt-get upgrade command. Of the following reasons, which explains why you may want to avoid this plan?

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

Answer: D

NEW QUESTION 198
In trace route results, what is the significance of an * result?

A. A listening port was identifie
B. A reply was returned in less than a secon
C. The target host was successfully reache
D. No reply was received for a particular ho

Answer: D

NEW QUESTION 203
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GSEC Exam with Our Prep Materials Via below:

https://www.certleader.com/GSEC-dumps.html