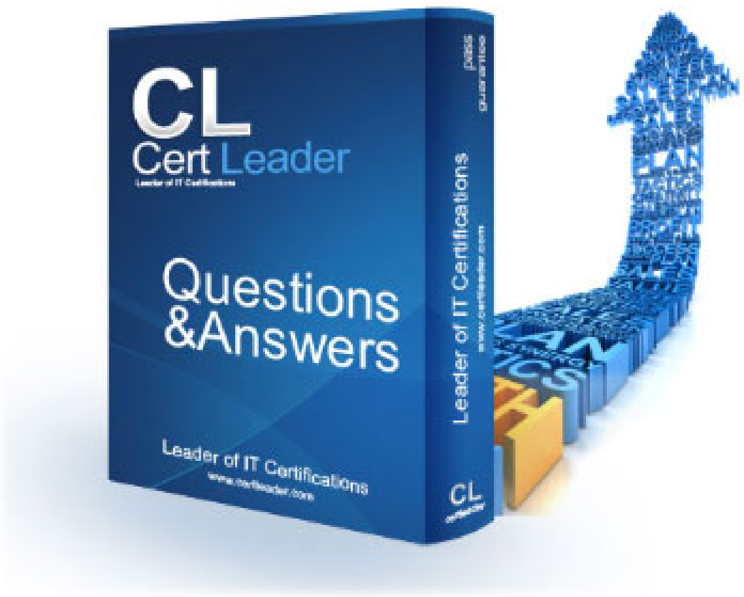
GSEC Dumps

GIAC Security Essentials Certification

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



NEW QUESTION 1
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 2
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 3
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 4
You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an SSH terminal at home to connect to the company's network. You have to configure your company's router for it. By default, which of the following standard ports does the SSH protocol use for connection?

A. 443
B. 22
C. 21
D. 80

Answer: B

NEW QUESTION 5
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 6
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 7
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 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 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 10
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 13
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 16
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 18
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 20
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
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 30
Which of the following statements about Secure Sockets Layer (SSL) are true? Each correct answer represents a complete solution. Choose two.

A. It provides communication privacy, authentication, and message integrit
B. It provides mail transfer servic
C. It uses a combination of public key and symmetric encryption for security of dat
D. It provides connectivity between Web browser and Web serve

Answer: AC

NEW QUESTION 35
Which Linux file lists every process that starts at boot time?

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

Answer: D

NEW QUESTION 37
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 domai

Answer: E

NEW QUESTION 38

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 41
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 45
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 47
Which of the following is a benefit to utilizing Cygwin for Windows?

A. The ability to install a complete Red Hat operating system Install on Window
B. The ability to bring much more powerful scripting capabilities to Window
C. The ability to run a production Apache serve
D. The ability to install a complete Ubuntu operating system install on Window

Answer: A

NEW QUESTION 49
Which of the following proxy servers provides administrative controls over the content?

A. Content filtering web proxy server
B. Caching proxy server
C. Forced proxy server
D. Web proxy server

Answer: A

NEW QUESTION 52
Which of the following is required to be backed up on a domain controller to recover Active Directory?

A. System state data
B. Operating System files
C. User's personal data
D. Installed third party application's folders

Answer: A

NEW QUESTION 56
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 61
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 66
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 67
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 71
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 74
Which of the following is an UDP based protocol?

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

Answer: B

NEW QUESTION 76
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 79
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 80
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 83
What protocol is a WAN technology?

A. 802.11
B. 802.3
C. Ethernet
D. Frame Relay

Answer: D

NEW QUESTION 87
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 92
Which of the following is the reason of using Faraday cage?

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

Answer: D

NEW QUESTION 95
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 96
What technical control provides the most critical layer of defense if an intruder is able to bypass all physical security controls and obtain tapes containing critical data?

A. Camera Recordings
B. Security guards
C. Encryption
D. Shredding
E. Corrective Controls

Answer: C

NEW QUESTION 97
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 100
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 104
Which of the following services resolves host name to IP Address?

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

Answer: C

NEW QUESTION 106
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 108
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 111
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 114
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 119
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 124
Which Windows event log would you look in if you wanted information about whether or not a specific diver was running at start up?

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

Answer: B

NEW QUESTION 125
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 126
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 129
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 132
Which of the following BEST describes the two job functions of Microsoft Baseline Security Analyzer (MBSA)?

A. Vulnerability scanner and auditing tool
B. Auditing tool and alerting system
C. Configuration management and alerting system
D. Security patching and vulnerability scanner

Answer: D

NEW QUESTION 136
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 141
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 146
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 149
The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?
STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.
STEP 2 - Do a binary backup if data is being collected.
STEP 3 - Deliver collected evidence to law enforcement officials.

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

Answer: D

NEW QUESTION 152
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 156
One of your Linux systems was compromised last night. According to change management history and a recent vulnerability scan, the system's patches were up-to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

A. It was a zero-day exploi
B. It was a Trojan Horse exploi
C. It was a worm exploi
D. It was a man-in-middle exploi

Answer: A

NEW QUESTION 158
Which of the following statements about the integrity concept of information security management are true?
Each correct answer represents a complete solution. Choose three.

A. It ensures that unauthorized modifications are not made to data by authorized personnel or processe
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situatio
D. It ensures that modifications are not made to data by unauthorized personnel or processe

Answer: ACD

NEW QUESTION 161
......