

GIAC

Exam Questions GSEC

GIAC Security Essentials Certification



NEW QUESTION 1

At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

- A. When performing analysis
- B. When preparing policy
- C. When recovering from the incident
- D. When reacting to an incident

Answer: D

NEW QUESTION 2

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 3

Which of the following hardware devices prevents broadcasts from crossing over subnets?

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

Answer: C

NEW QUESTION 4

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 5

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 6

Which of the following are the types of access controls?

Each correct answer represents a complete solution. Choose three.

- A. Physical
- B. Administrative
- C. Automatic
- D. Technical

Answer: ABD

NEW QUESTION 7

During a scheduled evacuation training session the following events took place in this order:

- * 1. Evacuation process began by triggering the building fire alarm.
- * 2a. The meeting point leader arrived first at the designated meeting point and immediately began making note of who was and was not accounted for.
- * 2b. Stairwell and door monitors made it to their designated position to leave behind a box of flashlights and prop the stairway doors open with a garbage can so employees can find exits and dispose of food and beverages.
- 2c. Special needs assistants performed their assigned responsibility to help employees out that require special assistance.
- * 3. The safety warden communicated with the meeting point leader via walkie talkie to collect a list of missing personnel and communicated this information back to the searchers.
- * 4. Searchers began checking each room and placing stick-it notes on the bottom of searched doors to designate which areas were cleared.
- * 5. All special need assistants and their designated wards exited the building.
- * 6. Searchers complete their assigned search pattern and exit with the Stairwell/door monitors.

Given this sequence of events, which role is in violation of its expected evacuation tasks?

- A. Safety warden
- B. Stairwell and door monitors
- C. Meeting point leader
- D. Searchers
- E. Special needs assistants

Answer: B

NEW QUESTION 8

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 9

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 10

Which Host-based IDS (HIDS) method of log monitoring utilizes a list of keywords or phrases that define the events of interest for the analyst, then takes a list of keywords to watch for and generates alerts when it sees matches in log file activity?

- A. Passive analysis
- B. Retroactive analysis
- C. Exclusive analysis
- D. Inclusive analysis

Answer: D

NEW QUESTION 10

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 12

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 14

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 16

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 17

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 19

Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

- A. Anonymous authentication
- B. Mutual authentication
- C. Open system authentication
- D. Shared key authentication

Answer: CD

NEW QUESTION 20

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 22

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 27

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 30

Where is the source address located in an IPv4 header?

- A. At an offset of 20 bytes
- B. At an offset of 8 bytes
- C. At an offset of 16 bytes
- D. At an offset of 12 bytes

Answer: D

NEW QUESTION 35

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 36

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 37

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 38

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 40

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

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

Answer: B

NEW QUESTION 45

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 service
- B. If someone were to randomly browse to the rogue port 80 service they could be compromised
- C. This is a technique commonly used to perform a denial of service on the local web server
- D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environments

Answer: D

NEW QUESTION 48

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 servers
- B. These attacks rely on a modified TCP/IP stack to function
- C. These attacks can be easily traced back to the source
- D. These attacks only work against Linux/Unix hosts

Answer: A

NEW QUESTION 53

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

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

Answer: D

NEW QUESTION 56

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

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

Answer: A

NEW QUESTION 60

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 63

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 67

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 72

Which Defense-in-Depth principle starts with an awareness of the value of each section of information within an organization?

- A. Information centric defense
- B. Uniform information protection
- C. General information protection
- D. Perimeter layering

Answer: A

NEW QUESTION 74

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 75

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 78

Which of the following statements about buffer overflow is true?

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

Answer: C

NEW QUESTION 83

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 88

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 92

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 96

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 97

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 100

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

- A. PPTP
- B. IPSec
- C. PGP
- D. NTFS

Answer: C

NEW QUESTION 104

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 109

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 111

Which of the following is a backup strategy?

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

Answer: A

NEW QUESTION 115

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 119

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 124

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 129

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 132

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 134

Which of the following tools is used to query the DNS servers to get detailed information about IP addresses, MX records, and NS servers?

- A. NBTSTAT
- B. NSLOOKUP
- C. PING
- D. NETSTAT

Answer: B

NEW QUESTION 139

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 144

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 148

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 152

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 153

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

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

Answer: B

NEW QUESTION 156

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 160

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 162

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

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

Answer: B

NEW QUESTION 166

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 170

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 172

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 174

Which of the following statements would be seen in a Disaster Recovery Plan?

- A. "Instructions for notification of the media can be found in Appendix A"
- B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."
- C. "The target for restoration of business operations is 72 hours from the declaration of disaster."
- D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Answer: D

NEW QUESTION 176

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 177

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 181

Which of the following languages enable programmers to store cookies on client computers? Each correct answer represents a complete solution. Choose two.

- A. DHTML
- B. Perl
- C. HTML
- D. JavaScript

Answer: BD

NEW QUESTION 185

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 189

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

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

Answer: B

NEW QUESTION 192

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 197

Analyze the screenshot below. What is the purpose of this message?

- A. To gather non-specific vulnerability information
- B. To get the user to download malicious software
- C. To test the browser plugins for compatibility
- D. To alert the user to infected software on the compute

Answer: D

NEW QUESTION 200

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 205

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 206

What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?

- A. Non-zero sum game
- B. Win-win situation
- C. Zero-sum game
- D. Symmetric warfare

Answer: D

NEW QUESTION 208

Why are false positives such a problem with IPS technology?

- A. File integrity is not guarantee
- B. Malicious code can get into the network
- C. Legitimate services are not delivered
- D. Rules are often misinterpreted

Answer: D

NEW QUESTION 213

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 215

There are three key factors in selecting a biometric mechanism. What are they?

- A. Reliability, encryption strength, and cost
- B. Encryption strength, authorization method, and cost
- C. Reliability, user acceptance, and cost
- D. User acceptance, encryption strength, and cost

Answer: C

NEW QUESTION 220

You work as a Network Administrator for McRobert Inc. You want to know the NetBIOS name of your computer. Which of the following commands will you use?

- A. NETSTAT -s
- B. NBTSTAT -s
- C. NBTSTAT -n
- D. NETSTAT -n

Answer: C

NEW QUESTION 223

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 225

Which of the following heights of fence deters only casual trespassers?

- A. 8 feet
- B. 2 to 2.5 feet
- C. 6 to 7 feet
- D. 3 to 4 feet

Answer: D

NEW QUESTION 229

Which of the following features of Windows 7 allows an administrator to both passively review installed software and configure policies to prevent out-of-date or insecure software from running?

- A. Direct Access
- B. Software Restriction Policies
- C. App Locker
- D. User Account Control

Answer: C

NEW QUESTION 233

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 238

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 241

What is SSL primarily used to protect you against?

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

Answer: C

NEW QUESTION 246

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

- A. DES is less secur

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

Answer: D

NEW QUESTION 251

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 space
- C. Deploy the honey pot hosts to only respond to attack
- D. Deploy the honey pot hosts on used address space

Answer: B

NEW QUESTION 254

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 257

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

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

Answer: C

NEW QUESTION 258

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 263

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 267

When a packet leaving the network undergoes Network Address Translation (NAT), which of the following is changed?

- A. TCP Sequence Number
- B. Source address
- C. Destination port
- D. Destination address

Answer: B

NEW QUESTION 270

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 274

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 278

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 281

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

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

Answer: C

NEW QUESTION 282

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 fragmentation
- E. A and B
- F. B and C
- G. B and D
- H. A and D

Answer: B

NEW QUESTION 286

Where are user accounts and passwords stored in a decentralized privilege management environment?

- A. On a central authentication server
- B. On more than one server
- C. On each server
- D. On a server configured for decentralized privilege management

Answer: C

NEW QUESTION 288

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 292

Regarding the UDP header below, what is the length in bytes of the UDP datagram?

04 1a 00 a1 00 55 db 51

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

Answer: D

NEW QUESTION 297

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 301

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 304

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 309

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 313

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 317

When should you create the initial database for a Linux file integrity checker?

- A. Before a system is patched
- B. After a system has been compromised
- C. Before a system has been compromised
- D. During an attack

Answer: C

NEW QUESTION 319

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 322

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 325

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 addresses
- 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 Internet
- D. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host

Answer: AC

NEW QUESTION 330

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 333

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 337

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 340

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag

B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody

C. Take photographs of all persons who have had access to the computer

D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag

Answer: D

NEW QUESTION 342

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 346

Which of the following books deals with confidentiality?

A. Purple Book

B. Orange Book

C. Red Book

D. Brown Book

Answer: B

NEW QUESTION 347

What would the following IP tables command do?

IP tables -I INPUT -s 99.23.45.1/32 -j DROP

A. Drop all packets from the source address

B. Input all packets to the source address

C. Log all packets to or from the specified address

D. Drop all packets to the specified address

Answer: A

NEW QUESTION 352

Which of the following statements about policy is FALSE?

A. A well-written policy contains definitions relating to "what" to do

B. A well-written policy states the specifics of "how" to do something

C. Security policy establishes what must be done to protect information stored on computer

D. Policy protects people who are trying to do the right thing

Answer: D

NEW QUESTION 357

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

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

A. They allow an attacker to conduct a buffer overflow

B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access

C. They allow an attacker to replace utility programs that can be used to detect the attacker's activities

D. They allow an attacker to run packet sniffers secretly to capture passwords

Answer: BCD

NEW QUESTION 360

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

A. Bus

B. Ring

- C. Star
- D. Cycle

Answer: C

NEW QUESTION 362

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 364

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 365

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 367

.....

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](#)