GIAC

Exam Questions GSEC

GIAC Security Essentials Certification

NEW QUESTION 1
You work as a Linux technician for Tech Perfect Inc. You have lost the password of the root. You want to provide a new password. Which of the following steps will you take to accomplish the task?

A. The password of the root user cannot be change
B. Use the PASSWD root comman
C. Reboot the compute
D. Reboot the computer in run level 0. Use INIT=/bin/sh as a boot optio
E. At the bash# prompt, run the PASSWD root comman
F. Reboot the computer in run level 1. Use INIT=/bin/sh as a boot optio
G. At the bash# prompt, run the PASSWD root comman

Answer: D

NEW QUESTION 2
Which of the following is a Layer 3 device that will typically drop directed broadcast traffic?

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

Answer: C

NEW QUESTION 3
Which of the following is a valid password for a system with the default "Password must meet complexity requirements" setting enabled as part of the GPO Password policy requirements?

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

Answer: D

NEW QUESTION 4
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 5
When Net Stumbler is initially launched, it sends wireless frames to which of the following addresses?

A. Broadcast address
B. Default gateway address
C. Subnet address
D. Network address

Answer: A

NEW QUESTION 6
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 7
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 8
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 9
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 10
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 10
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 14
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 15
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 18
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 21
Which of the following fields CANNOT be hashed by Authentication Header (AH) in transport mode?

A. Length
B. Source IP
C. TTL
D. Destination IP

Answer: C

NEW QUESTION 23
Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

A. RARP
B. ARP
C. DNS
D. RDNS

Answer: A

NEW QUESTION 25
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 28
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 29
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 33
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 34
Which of the following is referred to as Electromagnetic Interference (EMI)?

A. Electrical line noise
B. Spike
C. Transient
D. Brownout

Answer: A

NEW QUESTION 38
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 39
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 40
Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments.
This style of defense-in-depth protection is best described as which of the following?

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

Answer: B

NEW QUESTION 45
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 48
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 49
Which of the following best describes the level of risk associated with using proprietary crypto algorithms.?

A. Proprietary cryptographic algorithms are required by law to use shorter key lengths in the United States, so the risk is hig
B. Proprietary algorithms have not been subjected to public scrutiny, so they have been checked less throughly for vulnerabilitie
C. Proprietary algorithms are less likely be vulnerable than algorithms that have been publicly disclosed because of enhanced secrecy of the algorith
D. Proprietary algorithms are not known to generally be any more or less vulnerable than publicly scrutinized algorithm

Answer: B

NEW QUESTION 50
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 53
You are responsible for technical support at a company. One of the employees complains that his new laptop cannot connect to the company wireless network. You have verified that he is entering a valid password/passkey. What is the most likely problem?

A. A firewall is blocking hi
B. His laptop is incompatibl
C. MAC filtering is blocking hi
D. His operating system is incompatibl

Answer: C

NEW QUESTION 54
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 58
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 62
Which of the following applications would be BEST implemented with UDP instead of TCP?

A. A multicast streaming applicatio
B. A web browse
C. A DNS zone transfe
D. A file transfer applicatio

Answer: A

NEW QUESTION 64
Which Linux file lists every process that starts at boot time?

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

Answer: D

NEW QUESTION 65
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 69
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 73
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 78
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 80
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 83
Which of the following Unix syslog message priorities is the MOST severe?

A. err
B. emerg
C. crit
D. alert

Answer: B

NEW QUESTION 88
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 89
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 94
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 95
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 99
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 104
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:

```
[user@localhost ~]$ who
admin :0 2010-09-11 06:49
dvader pts/3 2010-09-11 08:07 (localhost.localdomain)
hsolo pts/4 2010-09-11 08:14 (192.168.54.3)
cdooku pts/4 2010-09-11 08:14 (192.168.54.5)
```

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 109
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 113
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 114
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 118
Which of the following is a backup strategy?

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

Answer: A

NEW QUESTION 122
Which of the following is a standard Unix command that would most likely be used to copy raw file system data for later forensic analysis?

A. dd
B. backup
C. cp
D. gzip

Answer: A

NEW QUESTION 127
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 135
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 137
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 141
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 143
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 146
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 149
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 154
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 156
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 157
Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?

A. Ability to detect malicious traffic after it has been decrypted by the host
B. Ability to decrypt network traffic
C. Ability to listen to network traffic at the perimeter
D. Ability to detect malicious traffic before it has been decrypted

Answer: A

NEW QUESTION 159
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 164

What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 165
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 168
What is the first thing that should be done during the containment step of incident handling?

A. Change all the passwords
B. Secure the area
C. Prepare the Jump bag
D. Notify management
E. Prepare a report

Answer: B

NEW QUESTION 173
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 176
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 177
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 182
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 186

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 188
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 190
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 191
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 193
You work as a Network Administrator for McNeil Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:
The wireless network communication should be secured.
The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps:
Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication. What will happen after you have taken these steps?

A. The laptop users will be able to use smart cards for getting authenticate
B. Both tasks will be accomplishe
C. None of the tasks will be accomplishe
D. The wireless network communication will be secure

Answer: D

NEW QUESTION 194
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 196
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 201
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 203
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 204
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 206
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 210
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 214
Which of the following items are examples of preventive physical controls? Each correct answer represents a complete solution. Choose three.

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

Answer: ACD

NEW QUESTION 218
Which of the following quantifies the effects of a potential disaster over a period of time?

A. Risk Assessment
B. Business Impact Analysis
C. Disaster Recovery Planning
D. Lessons Learned

Answer: B

NEW QUESTION 221
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 223
Which of the following defines the communication link between a Web server and Web applications?

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

Answer: A

NEW QUESTION 226
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 230
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 232
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 233
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 237
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 unspecifie
B. This is an IPv4 packet with a TCP payloa
C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecifie
D. This is an IPv6 packet with a TCP payloa

Answer: C

NEW QUESTION 242
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 243
Where are user accounts and passwords stored in a decentralized privilege management environment?

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

Answer: C

NEW QUESTION 247
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 250
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 254
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 modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?
Each correct answer represents a complete solution. Choose all that apply.

A. rm private.txt #11 Nov 2009 02:59:58 am
B. touch -d "11 Nov 2009 02:59:58 am" private.txt
C. touch private.txt #11 Nov 2009 02:59:58 am
D. touch -t 200911110259.58 private.txt

Answer: BD

NEW QUESTION 257
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 258
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 262
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 267
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?

No. .	Time	Source	Destination	Dest. Port	Info
35	20.657938	192.168.23.132	192.168.23.255		Echo (pi

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 268
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 271
Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

A. Hardening
B. Authentication
C. Cryptography
D. Sanitization

Answer: A

NEW QUESTION 273
What is the following sequence of packets demonstrating?

A. telnet.com.telnet > client.com.38060: F 4289:4289(0) ack 92 win 1024
B. client.com.38060 > telnet.com.telnet: .ack 4290 win 8760 (DF)
C. client.com.38060 > telnet.com.telnet: F 92:92(0) ack 4290 win 8760 (DF)
D. telnet.com.telnet > client.com.38060: .ack 93 win 1024

Answer: C

NEW QUESTION 274
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 279
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 284
Which command would allow an administrator to determine if a RPM package was already installed?

A. rpm -s
B. rpm -q
C. rpm -a
D. rpm -t

Answer: B

NEW QUESTION 286
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 287
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 288
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 overflo
B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime acces
C. They allow an attacker to replace utility programs that can be used to detect the attacker's activit
D. They allow an attacker to run packet sniffers secretly to capture password

Answer: BCD

NEW QUESTION 291
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 294
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 298
What are the two actions the receiver of a PGP email message can perform that allows establishment of trust between sender and receiver?

A. Decode the message by decrypting the asymmetric key with his private key, then using the asymmetric key to decrypt the messag
B. Decode the message by decrypting the symmetric key with his private key, then using the symmetric key to decrypt the messag
C. Decode the message by decrypting the symmetric key with his public key, then using the symmetric key to decrypt the messag
D. Decrypt the message by encrypting the digital signature with his private key, then using the digital signature to decrypt the messag

Answer: A

NEW QUESTION 299
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 304
.....

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