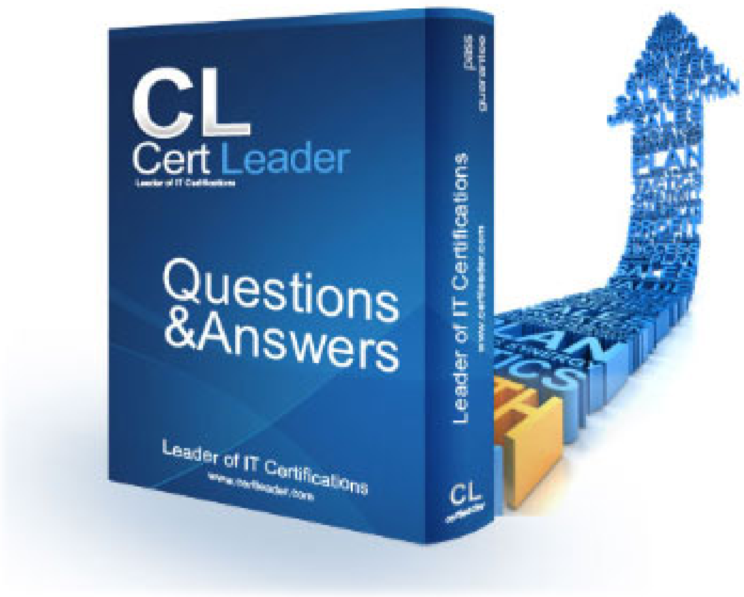
GSEC Dumps

GIAC Security Essentials Certification

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



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 protocols is used to send e-mails on the Internet?

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

Answer: A

NEW QUESTION 3
Which of the following is an Implementation of PKI?

A. SSL
B. 3DES
C. Kerberos
D. SHA-1

Answer: A

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 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 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
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 8
If you do NOT have an original file to compare to, what is a good way to identify steganography in potential carrier files?

A. Determine normal properties through methods like statistics and look for changes
B. Determine normal network traffic patterns and look for changes
C. Find files with the extension .stg
D. Visually verify the files you suspect to be steganography messages

Answer: A

NEW QUESTION 9
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 por
B. The server is on a different networ
C. The client-side source ports are differen
D. The clients are on different subnet

Answer: C

NEW QUESTION 10
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 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 15
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 19
Which of the following choices accurately describes how PGP works when encrypting email?

A. PGP encrypts the message with the recipients public key, then encrypts this key with a random asymmetric ke
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 recipients public key, then encrypts this key with a random symmetric ke

Answer: B

NEW QUESTION 22
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 24
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 27
You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?
Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption
B. Ease of maintenance
C. Load balancing
D. Failover

Answer: CD

NEW QUESTION 28
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 33
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 35
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 37
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 38
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 42
Which of the following protocols implements VPN using IPSec?

A. SLIP
B. PPP
C. L2TP
D. PPTP

Answer: C

NEW QUESTION 43
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 53
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 54
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 55
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 60
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 62
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 66
Which of the following is NOT a recommended best practice for securing Terminal Services and Remote Desktop?

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

Answer: B

NEW QUESTION 70
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 74
In a /24 subnet, which of the following is a valid broadcast address?

A. 200.11.11.1
B. 221.10.10.10
C. 245.20.30.254
D. 192.10.10.255

Answer: D

NEW QUESTION 78
Why would someone use port 80 for deployment of unauthorized services?

A. Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue servic
B. If someone were to randomly browse to the rogue port 80 service they could be compromise
C. This is a technique commonly used to perform a denial of service on the local web serve
D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environment

Answer: D

NEW QUESTION 79
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 80
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 85

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

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

Answer: D

NEW QUESTION 87
Users at the Marketing department are receiving their new Windows XP Professional workstations. They will need to maintain local work files in the first logical volume, and will use a second volume for the information shared between the area group. Which is the best file system design for these workstations?

A. Both volumes should be converted to NTFS at install tim
B. First volume should be FAT32 and second volume should be NTF
C. First volume should be EFS and second volume should be FAT32.
D. Both volumes should be converted to FAT32 with NTFS DACL

Answer: A

NEW QUESTION 89
In PKI, when someone wants to verify that the certificate is valid, what do they use to decrypt the signature?

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

Answer: D

NEW QUESTION 93
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 94
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 96
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 100
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 103
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 106
Which of the following would be a valid reason to use a Windows workgroup?

A. Lower initial cost
B. Simplicity of single sign-on
C. Centralized control
D. Consistent permissions and rights

Answer: D

NEW QUESTION 108
You have reason to believe someone with a domain user account has been accessing and modifying sensitive spreadsheets on one of your application servers. You decide to enable auditing for the files to see who is accessing and changing them. You enable the Audit Object Access policy on the files via Group Policy. Two weeks later, when you check on
the audit logs, you see they are empty. What is the most likely reason this has happened?

A. You cannot enable auditing on files, just folders
B. You did not enable auditing on the files
C. The person modifying the files turned off auditing
D. You did not save the change to the policy

Answer: B

NEW QUESTION 113
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 117
With regard to defense-in-depth, which of the following statements about network design principles is correct?

A. A secure network design requires that systems that have access to the Internet should not be accessible from the Internet and that systems accessible from the Internet should not have access to the Interne
B. A secure network design requires that networks utilize VLAN (Virtual LAN) implementations to insure that private and semi-public systems are unable to reach each other without going through a firewal
C. A secure network design will seek to provide an effective administrative structure by providing a single choke-point for the network from which all security controls and restrictions will be enforce
D. A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirement

Answer: D

NEW QUESTION 118
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 122
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 126

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 128
Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

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

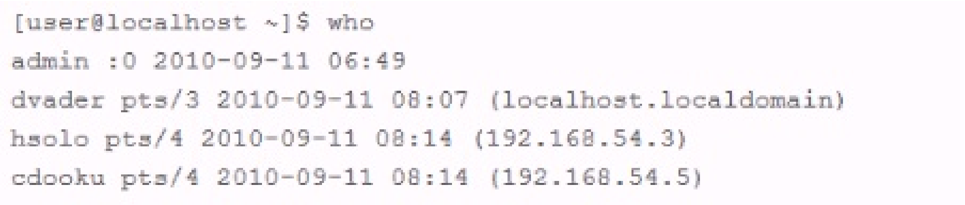
Answer: C

NEW QUESTION 130
Which of the following tools is also capable of static packet filtering?

A. netstat.exe
B. ipsecpol.exe
C. ipconfig.exe
D. net.exe

Answer: B

NEW QUESTION 134
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 135
What type of formal document would include the following statement?
Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal application of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies, and if there is any uncertainty, employees should consult their supervisor or manager.

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

Answer: C

NEW QUESTION 140
Which of the following classes of fire comes under Class C fire?

A. Paper or wood fire
B. Oil fire
C. Combustible metals fire
D. Electronic or computer fire

Answer: D

NEW QUESTION 144

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 148
You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

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

Answer: A

NEW QUESTION 150
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 153
Which of the following is a backup strategy?

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

Answer: A

NEW QUESTION 155
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 159
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 163
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 164
An attacker gained physical access to an internal computer to access company proprietary
data. The facility is protected by a fingerprint biometric system that records both failed and successful entry attempts. No failures were logged during the time periods of the recent breach. The account used when the attacker entered the facility shortly before each incident belongs to an employee who was out of the area. With respect to the biometric entry system, which of the following actions will help mitigate unauthorized physical access to the facility?

A. Try raising the Crossover Error Rate (CER)
B. Try to lower the False Accept Rate (FAR)
C. Try setting the Equal Error Rate (EER) to zero
D. Try to set a lower False Reject Rate (FRR)

Answer: B

NEW QUESTION 167
How are differences in configuration settings handled between Domain and Local Group Policy Objects (GPOs)?

A. Local and Domain GPOs control different configuration settings, so there will not be conflict
B. Settings in the domain-wide GPO override conflicting settings in the local GPO on each compute
C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applie
D. Precedence depends on which GPO was updated firs

Answer: B

NEW QUESTION 169
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 174
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 177
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 182
Which of the following is NOT typically used to mitigate the war dialing threat?

A. Setting up monitored modems on special phone numbers
B. Setting modems to auto-answer mode
C. Proactively scanning your own phone numbers
D. Monitoring call logs at the switch

Answer: B

NEW QUESTION 185
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 190
Which of the following types of computers is used for attracting potential intruders?

A. Files pot
B. Honey pot
C. Data pot
D. Bastion host

Answer: B

NEW QUESTION 192
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 193
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 195
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain- based network. The network contains ten Windows 2003 member servers, 150 Windows XP Professional client computers. According to the company's security policy, Mark needs to check whether all the computers in the network have all available security updates and shared folders. He also needs to check the file system type on each computer's hard disk. Mark installs and runs MBSACLI.EXE with the appropriate switches on a server. Which of the following tasks will he accomplish?

A. None of the tasks will be accomplishe
B. He will be able to check the file system type on each computer's hard dis
C. He will be able to accomplish all the task
D. He will be able to check all available security updates and shared folder

Answer: C

NEW QUESTION 199
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 203
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 204
Which of the following is the FIRST step in performing an Operational Security (OP5EC) Vulnerabilities Assessment?

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

Answer: E

NEW QUESTION 209
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 214
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 218
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 221
You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. You are configuring an application server. An application named Report, which is owned by the root user, is placed on the server. This application requires superuser permission to write to other files. All sales managers of the company will be using the application. Which of the following steps will you take in order to enable the sales managers to run and use the Report application?

A. Change the Report application to a SUID comman
B. Make the user accounts of all the sales managers the members of the root grou
C. Provide password of root user to all the sales manager
D. Ask each sales manager to run the application as the root use
E. As the application is owned by the root, no changes are require

Answer: A

NEW QUESTION 226
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 227
What is the motivation behind SYN/FIN scanning?

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

Answer: B

NEW QUESTION 228
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

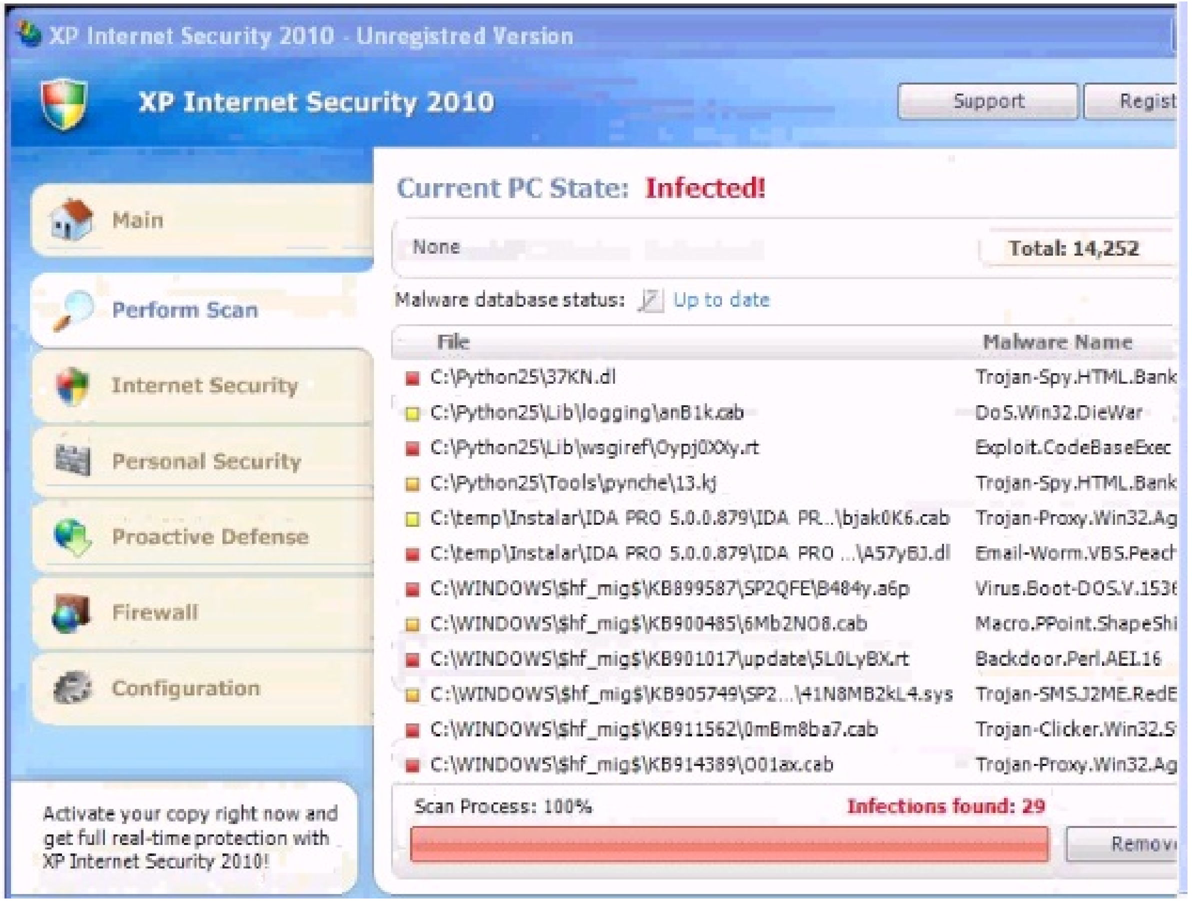
NEW QUESTION 229
You work as a Network Administrator for McNeil Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company's management has decided to provide laptops to its sales team members. 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 232
Analyze the screenshot below. What is the purpose of this message?



Current PC State: Infected!

None | Total: 14,252

Malware database status: Up to date

File	Malware Name
🟥 C:\Python25\37KN.dl	Trojan-Spy.HTML.Bank
🟨 C:\Python25\Lib\logging\anB1k.cab	DoS.Win32.DieWar
🟥 C:\Python25\Lib\wsgiref\Oypj0XXy.rt	Exploit.CodeBaseExec
🟨 C:\Python25\Tools\pynche\13.kj	Trojan-Spy.HTML.Bank
🟨 C:\temp\Instalar\IDA PRO 5.0.0.879\IDA PR...\bjak0K6.cab	Trojan-Proxy.Win32.Ag
🟥 C:\temp\Instalar\IDA PRO 5.0.0.879\IDA PRO ...\A57yBJ.dl	Email-Worm.VBS.Peach
🟥 C:\WINDOWS\hf_mig\KB899587\SP2QFE\B484y.a6p	Virus.Boot-DOS.V.153
🟨 C:\WINDOWS\hf_mig\KB900485\6Mb2NO8.cab	Macro.PPoint.ShapeShi
🟥 C:\WINDOWS\hf_mig\KB901017\update\5L0LyBX.rt	Backdoor.Perl.AEI.16
🟨 C:\WINDOWS\hf_mig\KB905749\SP2...\41N8MB2kL4.sys	Trojan-SMS.J2ME.RedE
🟥 C:\WINDOWS\hf_mig\KB911562\0mBm8ba7.cab	Trojan-Clicker.Win32.S
🟥 C:\WINDOWS\hf_mig\KB914389\O01ax.cab	Trojan-Proxy.Win32.Ag

Scan Process: 100% Infections found: 29

Activate your copy right now and get full real-time protection with XP Internet Security 2010!

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 236
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 240
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of emails on the network. Which of the following ports will you open?
Each correct answer represents a complete solution. Choose two.

A. 80
B. 25
C. 20
D. 110

Answer: BD

NEW QUESTION 243
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 245
The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

A. ROI = (gain - expenditure)/(expenditure) X 100%
B. ROI = (gain + expenditure)/(expenditure) X 100%
C. ROI = (loss + expenditure)/(expenditure) X 100%
D. ROI = (loss - expenditure)/(expenditure) X 100%

Answer: A

NEW QUESTION 247
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 248
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 250
How is a Distributed Denial of Service (DDOS) attack distinguished from a regular DOS attack?

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

Answer: A

NEW QUESTION 252
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 256
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 261
Validating which vulnerabilities in a network environment are able to be exploited by an attacker is called what?

A. Anomaly detection
B. Vulnerability scanning
C. Perimeter assessment

D. Penetration testing

Answer: B

NEW QUESTION 265
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 268
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 271
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 272
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 277
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 278
What is the most secure way to address an unused Windows service so it cannot be exploited by malware?

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

Answer: D

NEW QUESTION 279
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 284
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 285
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 286
Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

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

Answer: A

NEW QUESTION 289
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 294
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 298
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 302
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
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 306
You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using Encrypting File System (EFS).
You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy disk. What will you do to accomplish this?

A. Copy the files to a network share on an NTFS volum
B. Copy the files to a network share on a FAT32 volum
C. Place the files in an encrypted folde
D. Then, copy the folder to a floppy dis
E. Copy the files to a floppy disk that has been formatted using Windows 2000 Professiona

Answer: A

NEW QUESTION 308
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 313
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 317
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 322
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 325
How many bytes does it take to represent the hexadecimal value OxFEDCBA?

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

Answer: C

NEW QUESTION 326
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 330
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 333
If a DNS client wants to look up the IP address for good.news.com and does not receive an authoritative reply from its local DNS server, which name server is most likely to provide an authoritative reply?

A. The news.com domain name server
B. The .com (top-level) domain name server
C. The .(root-level) domain name server
D. The .gov (top-level) domain name server

Answer: A

NEW QUESTION 335
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 338
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 341
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 343
Which of the following books deals with confidentiality?

A. Purple Book
B. Orange Book
C. Red Book
D. Brown Book

Answer: B

NEW QUESTION 346
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 350
Which of the following statements about policy is FALSE?

A. A well-written policy contains definitions relating to "what" to d
B. A well-written policy states the specifics of "how" to do somethin
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 thin

Answer: D

NEW QUESTION 355
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 357
Which of the following networking topologies uses a hub to connect computers?

A. Bus
B. Ring
C. Star
D. Cycle

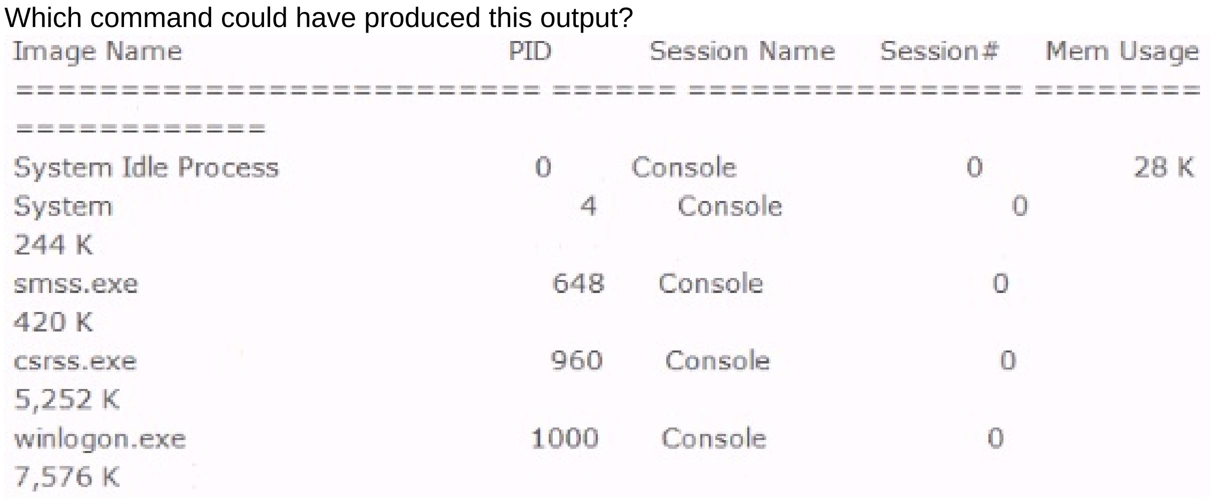
Answer: C

NEW QUESTION 358
The previous system administrator at your company used to rely heavily on email lists, such as vendor lists and Bug Traq to get information about updates and patches. While a useful means of acquiring data, this requires time and effort to read through. In an effort to speed things up, you decide to switch to completely automated updates and patching. You set up your systems to automatically patch your production servers using a cron job and a scripted apt-get upgrade command. Of the following reasons, which explains why you may want to avoid this plan?

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

Answer: D

NEW QUESTION 359
Included below is the output from a resource kit utility run against local host.
Which command could have produced this output?



```
Image Name                    PID    Session Name     Session#   Mem Usage
========================= ====== ================ ========
============
System Idle Process             0    Console              0         28 K
System                            4    Console              0
244 K
smss.exe                        648    Console              0
420 K
csrss.exe                       960    Console              0
5,252 K
winlogon.exe                   1000    Console              0
7,576 K
```

A. Schtasks
B. Task kill
C. SC
D. Task list

Answer: D

NEW QUESTION 361
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 363
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 366
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 370
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 372
......

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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