GIAC

Exam Questions GSEC

GIAC Security Essentials Certification

NEW QUESTION 1
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 2
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 3
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 4
Which of the following SIP methods is used to setup a new session and add a caller?

A. ACK
B. BYE
C. REGISTER
D. INVITE
E. CANCEL

Answer: D

NEW QUESTION 5
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 6
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 7
Which Defense-in-Depth model involves identifying various means by which threats can become manifest and providing security mechanisms to shut them down?

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

Answer: A

NEW QUESTION 8

Which of the following works at the network layer and hides the local area network IP address and topology?

A. Network address translation (NAT)
B. Hub
C. MAC address
D. Network interface card (NIC)

Answer: A

NEW QUESTION 9
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 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 13
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright
B. Trademark
C. Trade secret
D. Patent

Answer: B

NEW QUESTION 15
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 19
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 22
Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.
This style of defense-in-depth protection is best described as which of the following?

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

Answer: A

NEW QUESTION 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 30
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 31
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 34
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 37
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 42
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 45
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 46
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 51
For most organizations, which of the following should be the highest priority when it comes to physical security concerns?

A. Controlling ingress and egress
B. Controlling access to workstations
C. Ensuring employee safety
D. Controlling access to servers
E. Protecting physical assets

Answer: C

NEW QUESTION 54
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 58
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 61
When discussing access controls, which of the following terms describes the process of determining the activities or functions that an Individual is permitted to perform?

A. Authentication

B. Identification
C. Authorization
D. Validation

Answer: C

NEW QUESTION 65
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 68
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 69
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 71
Which Linux file lists every process that starts at boot time?

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

Answer: D

NEW QUESTION 74
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 79
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 81
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 83
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 85
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 87
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 92
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

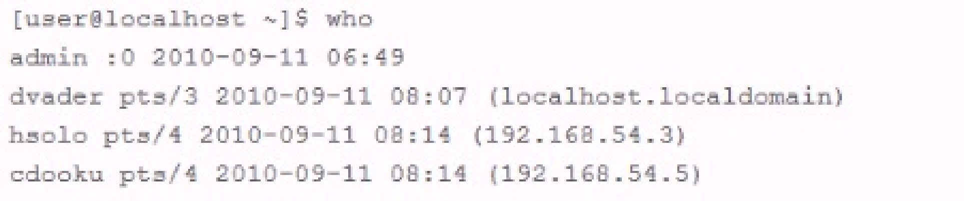
Answer: C

NEW QUESTION 95
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
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 100

What is the term for a game in which for every win there must be an equivalent loss?

A. Asymmetric
B. Untenable
C. Zero-sum
D. Gain-oriented

Answer: C

NEW QUESTION 104
Which of the following proxy servers provides administrative controls over the content?

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

Answer: A

NEW QUESTION 107
While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?

A. The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating syste
B. The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating syste
C. The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machin
D. The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating syste
E. The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique IP addresses and then define how much of the systems RAM is available to the guest operating syste

Answer: E

NEW QUESTION 111
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 113
You have been hired to design a TCP/IP-based network that will contain both Unix and Windows computers. You are planning a name resolution strategy. Which of the following services will best suit the requirements of the network?

A. APIPA
B. LMHOSTS
C. DNS
D. DHCP
E. WINS

Answer: C

NEW QUESTION 114
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 118
You are reviewing a packet capture file from your network intrusion detection system. In the packet stream, you come across a long series of "no operation" (NOP) commands. In addition to the NOP commands, there appears to be a malicious payload. Of the following, which is the most appropriate preventative measure for this type of attack?

A. Limits on the number of failed logins
B. Boundary checks on program inputs

C. Controls against time of check/time of use attacks
D. Restrictions on file permissions

Answer: C

NEW QUESTION 123
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 127
Your CIO has found out that it is possible for an attacker to clone your company's RFID (Radio Frequency ID) based key cards. The CIO has tasked you with finding a way to ensure that anyone entering the building is an employee. Which of the following authentication types would be the appropriate solution to this problem?

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

Answer: C

NEW QUESTION 129
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 132
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 133
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 135
What is the maximum number of connections a normal Bluetooth device can handle at one time?

A. 2
B. 4
C. 1
D. 8
E. 7

Answer: E

NEW QUESTION 136
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 138
It is possible to sniff traffic from other hosts on a switched Ethernet network by impersonating which type of network device?

A. Switch
B. Bridge
C. Hub
D. Router

Answer: D

NEW QUESTION 140
You are implementing wireless access at a defense contractor. Specifications say, you must implement the AES Encryption algorithm. Which encryption standard should you choose?

A. WPA
B. TKIP
C. WEP
D. WPA 2

Answer: D

NEW QUESTION 141
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 145
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 149
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 153
What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 154
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 155
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 160
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 165
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 166
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 168
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 173
When an IIS filename extension is mapped, what does this mean?

A. Files with the mapped extensions cannot be interpreted by the web serve
B. The file and all the data from the browser's request are handed off to the mapped interprete
C. The files with the mapped extensions are interpreted by CMD.EX
D. The files with the mapped extensions are interpreted by the web browse

Answer: B

NEW QUESTION 175
You have set up a local area network for your company. Your firewall separates your network into several sections: a DMZ with semi-public servers (web, dns, email) and an intranet with private servers. A penetration tester gains access to both sections and installs sniffers in each. He is able to capture network traffic for all the devices in the private section but only for one device (the device with the sniffer) in the DMZ. What can be inferred about the design of the system?

A. You installed a router in the private section and a switch in the DMZ

B. You installed a hub in the private section and a switch in the DMZ
C. You installed a switch in the private section and a hub in the DMZ
D. You installed a switch in the private section and a router in the DMZ

Answer: B

NEW QUESTION 180
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 182
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 183
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 187
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 189
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 193
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 195
Against policy, employees have installed Peer-to-Peer applications on their workstations and they are using them over TCP port 80 to download files via the

company network from other Peer-to-Peer users on the Internet. Which of the following describes this threat?

A. Firewall subversion
B. Backdoor installation
C. Malicious software infection
D. Phishing attempt

Answer: A

NEW QUESTION 199
Which of the following services resolves host name to IP Address?

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

Answer: C

NEW QUESTION 201
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 203
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 205
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 208
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 softwar
C. Asymmetric cryptography is generally much faster than symmetri
D. Symmetric cryptography is generally much faster than asymmetri

Answer: D

NEW QUESTION 209
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 214
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 218
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

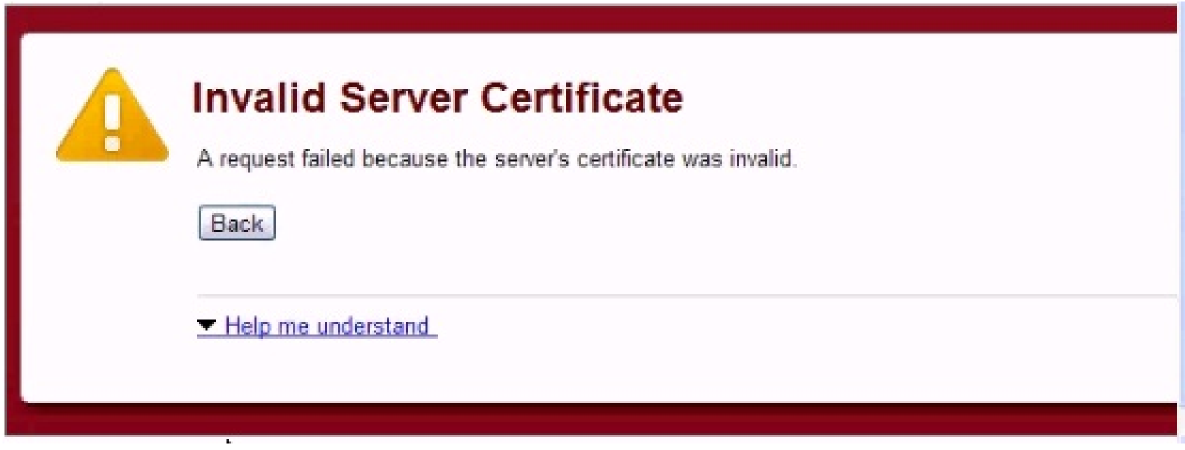
Answer: C

NEW QUESTION 220
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 corrupte
B. The packets may have been accidentally routed onto the Interne
C. The packets may be deliberately spoofed by an attacke
D. The packets are a sign of excess fragmentatio
E. A and B
F. B and C
G. B and D
H. A and D

Answer: B

NEW QUESTION 224
An employee attempting to use your wireless portal reports receiving the error shown below. Which scenario is occurring?



Invalid Server Certificate

A request failed because the server's certificate was invalid.

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 227
You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based
network. You have created a folder named Report. You have made David the owner of the folder. The members of a group named JAdmin can access the folder and have Read, Write, and Execute permissions. No other user can access the folder. You want to ensure that the members of the JAdmin group do not have Write permission on the folder. Also, you want other users to have Read permission on the Report folder.
Which of the following commands will you use to accomplish the task?

A. chmod 777 report
B. chown david.jadmin report
C. chmod 555 report
D. chmod 754 report

Answer: D

NEW QUESTION 232
Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

A. It uses TCP port 443 as the default por
B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure sit
C. It is a protocol used to provide security for a database server in an internal networ
D. It uses TCP port 80 as the default por

Answer: AB

NEW QUESTION 235
What does the "x" character in the second field of the user account record of the /etc/passwd file indicate?

A. The user account is using a shadow passwor
B. The user account is shared by more than one use
C. The user account is disable
D. The user account does not exis

Answer: A

NEW QUESTION 240
Which of the following statements best describes where a border router is normally placed?

A. Between your firewall and your internal network
B. Between your firewall and DNS server
C. Between your ISP and DNS server
D. Between your ISP and your external firewall

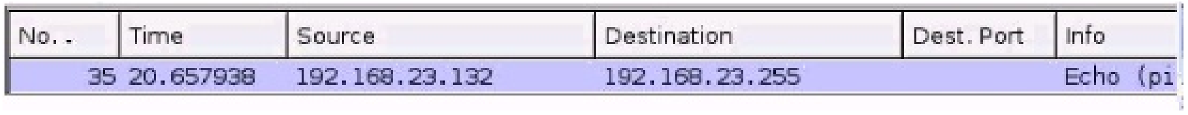
Answer: D

NEW QUESTION 243
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. For testing purposes, you have configured a default IP-table with several filtering rules. You want to reconfigure the table. For this, you decide to remove the rules from all the chains in the table. Which of the following commands will you use?

A. IPTABLES -D
B. IPTABLES -A
C. IPTABLES -h
D. IPTABLES -F

Answer: D

NEW QUESTION 248
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 251
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 252
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 253
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 packers 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 254
Which of the following networking topologies uses a hub to connect computers?

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

Answer: C

NEW QUESTION 255
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

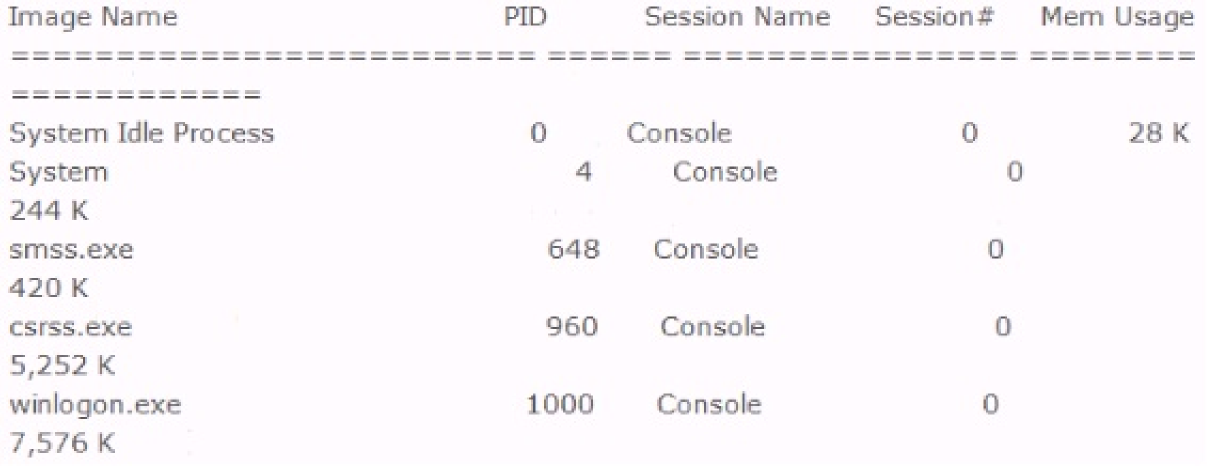
Answer: D

NEW QUESTION 258
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 262
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 264
One of your Linux systems was compromised last night. According to change management history and a recent vulnerability scan, the system's patches were up-to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

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

Answer: A

NEW QUESTION 266
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 268
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 273
......