Exam Questions GSEC

GIAC Security Essentials Certification

https://www.2passeasy.com/dumps/GSEC/

NEW QUESTION 1
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 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
Where could you go in Windows XP/2003 to configure Automatic Updates?

A. Right click on the Start Menu and choose select Properties in the pop-up Men
B. Open the MMC and choose the Automatic Updates snap-i
C. Right click on your desktop and choose the automatic update
D. Go to the System applet in Control Panel and click on the Automatic Updates ico

Answer: D

NEW QUESTION 6
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 7
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 8

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 9
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 10
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 10
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 13
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 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 19
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 21
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 22
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 23
What is the discipline of establishing a known baseline and managing that condition known as?

A. Condition deployment
B. Observation discipline
C. Security establishment
D. Configuration management

Answer: C

NEW QUESTION 28
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 31
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 35
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 37
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 41
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 43
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 48
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 51
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 52
Which type of risk assessment results are typically categorized as low, medium, or high-risk events?

A. Technical
B. Qualitative
C. Management
D. Quantitative

Answer: B

NEW QUESTION 53
Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 56
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 59
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 60
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 63
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 67
Which of the following are the types of intrusion detection systems?
Each correct answer represents a complete solution. Choose all that apply.

A. Host-based intrusion detection system (HIDS)
B. Client-based intrusion detection system (CIDS)
C. Server-based intrusion detection system (SIDS)
D. Network intrusion detection system (NIDS)

Answer: AD

NEW QUESTION 70
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 75
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 78
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 81
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 83
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 85
Which of the following Unix syslog message priorities is the MOST severe?

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

Answer: B

NEW QUESTION 90
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 91
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Privacy policy
B. Backup policy
C. User password policy
D. Network security policy

Answer: A

NEW QUESTION 94
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 95
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 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:

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 type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

A. Trojans
B. Boot infectors
C. Viruses
D. Worms

Answer: D

NEW QUESTION 102
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 107
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You want to mount an SMBFS share from a Linux workstation. Which of the following commands can you use to accomplish the task?
Each correct answer represents a complete solution. Choose two.

A. smbmount
B. mount smb
C. smbfsmount
D. mount -t smbfs

Answer: AD

NEW QUESTION 110
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 112
You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadserver.com so that it can connect to it. There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware connect to it instead. How do you get the malware to connect to that computer on the test network?

A. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
B. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadserveriamabadserver.com
C. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
D. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.115 iamabadserver iamabadserver.com

Answer: B

NEW QUESTION 116
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 121

Which of the following files contains the shadowed password entries in Linux?

A. /etc/passwd
B. /etc/shadow
C. /etc/profile
D. /etc/shdpwd

Answer: B

NEW QUESTION 126
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 130
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 133
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 135
What is the key difference between Electronic Codebook mode and other block cipher modes like Cipher Block Chaining, Cipher-Feedback and Output-Feedback?

A. Plaintext patterns are concealed by XO Ring with previous cipher text block but input to the block cipher is not randomize
B. Plaintext patterns are concealed and input to the block cipher is randomized by XO Ring with previous cipher text bloc
C. Plaintext patterns encrypted with the same key will always generate the same Cipher text pattern
D. Plaintext patterns are not concealed but input to the block cipher is randomized by XO Ring with previous cipher text bloc

Answer: C

NEW QUESTION 140
How often is session information sent to the web server from the browser once the session information has been established?

A. With any change in session data
B. With every subsequent request
C. With any hidden form element data
D. With the initial request to register the session

Answer: A

NEW QUESTION 145
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 148

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 149
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 151
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 154
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 158
You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

A. Take a full backup daily with the previous night's tape taken offsit
B. Take a full backup daily and use six-tape rotatio
C. Take a full backup on Monday and an incremental backup on each of the following weekday
D. Keep Monday's backup offsit
E. Take a full backup on alternate days and keep rotating the tape
F. Take a full backup on Monday and a differential backup on each of the following weekday
G. Keep Monday's backup offsit
H. Take a full backup daily with one tape taken offsite weekl

Answer: A

NEW QUESTION 161
There is not universal agreement on the names of the layers in the TCP/IP networking model. Which of the following is one of the functions of the bottom layer which is sometimes called the Network Access or Link Layer?

A. Provides end-to-end data delivery service for user applications
B. Handles the routing of the data packets over the network
C. Manages IP addressing and encryption for data packets
D. Defines the procedures for interfacing with Ethernet devices

Answer: D

NEW QUESTION 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 167
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 170
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 172
Analyze the screenshot below. What is the purpose of this message?

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

Answer: D

NEW QUESTION 173
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 178
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 183
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 187
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 192
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 193
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 195
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 196
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 197
Which of the following services resolves host name to IP Address?

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

Answer: C

NEW QUESTION 200
Many IIS servers connect to Microsoft SQL databases. Which of the following statements about SQL server security is TRUE?

A. SQL Server patches are part of the operating system patche
B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web applicatio
C. It is good practice to never use integrated Windows authentication for SQL Serve
D. It is good practice to not allow users to send raw SQL commands to the SQL Serve

Answer: D

NEW QUESTION 205

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 210
Which of the following heights of fence deters only casual trespassers?

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

Answer: D

NEW QUESTION 211
Which of the following processes is known as sanitization?

A. Assessing the risk involved in discarding particular informatio
B. Verifying the identity of a person, network host, or system proces
C. Physically destroying the media and the information stored on i
D. Removing the content from the media so that it is difficult to restor

Answer: D

NEW QUESTION 216
A new data center is being built where customer credit information will be processed and stored. Which of the following actions will help maintain the confidentiality of the data?

A. Environmental sensors in the server room
B. Access control system for physical building
C. Automated fire detection and control systems
D. Frequent off-site backup of critical databases

Answer: B

NEW QUESTION 221
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 226
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 228
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 232
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 235
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 239
When a packet leaving the network undergoes Network Address Translation (NAT), which of the following is changed?

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

Answer: B

NEW QUESTION 242
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 247
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 252
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 253
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 257

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

A. A denial-of-service attack is preventing a response from the porta
B. Another access point is deauthenticating legitimate client
C. The encrypted data is being intercepted and decrypte
D. Another access point is attempting to intercept the dat

Answer: D

NEW QUESTION 261
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 265
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 266
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 271
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 276
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 278
You are the security director for an off-shore banking site. From a business perspective, what is a major factor to consider before running your new vulnerability scanner against the company's business systems?

A. It may harm otherwise healthy system
B. It may produce false negative result
C. It may generate false positive result
D. It may not return enough benefit for the cos

Answer: C

NEW QUESTION 280
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 281
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 284
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 288
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 291
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?

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 295
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 299
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 300
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 305
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 306
While using Wire shark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below. Based on what you see below, which of the following would you recommend to prevent future damage to your database?

A. Use ssh to prevent a denial of service attack
B. Sanitize user inputs to prevent injection attacks
C. Authenticate users to prevent hackers from using your database
D. Use https to prevent hackers from inserting malware

Answer: D

NEW QUESTION 308
Which of the following terms refers to the process in which headers and trailers are added around user data?

A. Encapsulation
B. Authentication
C. Authorization
D. Encryption

Answer: A

NEW QUESTION 310
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 315
Which of the following SIP INVITE lines indicates to the remote registrar the VoIP phone that initiated the call?

A. Via
B. To
C. From-Agent
D. User-Agent

Answer: D

NEW QUESTION 320
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 324
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 328
......