
PASS-GUARANTEED.COM
100% Money Back Guarantee!!!
Your #1 Certification Training Resource
Product Details from Pass-Guaranteed.com:
Security+
SY0-101
Demo Version
Download Full Version
Visit
http://www.Pass-Guaranteed.com
Complete Certification Training Solutions
Practice Exam Test Questions
Click Here To Learn More
Go ->
Online Course Tutorials
with TESTING ENGINE
Go ->
Study Guides
Click Here to Learn More About Our Prep Labs
Go ->
Lab Scenarios
Click Here to Learn More About Our Prep Labs
Go ->
Preparation Labs
Click Here to Learn More About Our Prep Labs
Go ->
Online Testing Engine
Click Here To Learn More
Go ->

Study Tips

This product will provide you with questions and answers carefully compiled and written by our Expert Senior Certified Staff. Our practice questions are designed to help you learn the concepts behind the questions rather than be a strict memorization tool.

Important Note:

Please Read Carefully

Repeated readings of our Pass-Guaranteed.com Practice Exam will increase your comprehension. We constantly add to and update our Practice Exams with new questions, answers and explanations, so check that you have the latest version of this Practice Exam before you take your exam.

For security purposes, each PDF file is encrypted with a unique serial number associated With your Pass-Guaranteed.com account information. In accordance with International Copyright Law, Pass-Guaranteed.com reserves the right to take legal action against you should we find copies of this PDF file distributed to other parties.

Update Notifications (Latest Version)

We are constantly reviewing our products. New material is added and old material is revised. Free Updates are available for 180 days after purchase. If you purchased a bundle, you will have Free Updates for 1 YEAR!

You can signup to our newsletter for instant notification whenever an update is released by becoming a Pass-Guaranteed.com member at: http://www.pass-guaranteed.com/log.htm

By becoming a Pass-Guaranteed.com member, you also get a chance to win a FREE Practice Exam of your choosing. We give away 3 Pass-Guaranteed.com Practice Exams every week to 3 lucky winners.

Pass-Guaranteed.com Product Specials

Pass-Guaranteed.com Custom Bundle Requests, cover all Pass-Guaranteed.com Products!!! You can visit our Special Bundle Discounts from Pass-Guaranteed.com or make your own Custom Bundle Request with Pass-Guaranteed.com here: http://www.pass-guaranteed.com/bundles.htm

***Pass-Guaranteed.com Custom Bundle Request Form let's you create your own Bundle Of Products!!!** You can select and group any of our products for your Custom Bundle and we will give you up to a **50% Discount** on your Custom Bundle Package. This includes our Practice Test Questions, Online Course Tutorials, Study Guides, Lab Scenarios and our Certified Online Instructor service.*

Please visit: http://www.pass-guaranteed.com/custom-request.htm If you would like to purchase a Custom Bundle from Pass-Guaranteed.com.

QUESTION 1
You work as the security administrator at Pass.com. Pass has a RBAC (Role Based Access Control) compliant system for which you are planning the security implementation. There are three types of resources including files, printers, and mailboxes and four distinct departments with distinct functions including Sales, Marketing, Management, and Production in the system. Each department needs access to different resources. Each user has a workstation.

Which roles should you create to support the RBAC (Role Based Access Control) model?

A. File, printer, and mailbox roles
B. Sales, marketing, management, and production roles
C. User and workstation roles
D. Allow access and deny access roles

Answer: B

Explanation:
Each distinct department (sales, marketing, management, and production) has their own role in the company, which probably includes using the: filer server, print server, and mail server. So it would be wise to create roles for each department.

QUESTION 2
Which of the following password generators is based on challenge-response mechanisms?

A. asynchronous
B. synchronous
C. cryptographic keys
D. smart cards

Answer: A

Explanation:
An synchronous password generator, has an authentication server that generates a challenge (a large number or string) which is encrypted with the private key of the token device and has that token device's public key so it can verify authenticity of the request (which is independent from the time factor). That challenge can also include a hash of transmitted data, so not only can the authentication be assured; but also the data integrity.

QUESTION 3
Which of the following provides the strongest form of authentication?

A. token
B. username and password
C. biometrics
D. one time password

Answer: C

Explanation:

Biometrics is the use of authenticating a user by scanning on of their unique physiological body parts. Just like in the movies, a user places their hand on a finger print scanner or they put their eyes against a retinal scanner. If the image matches what's on the database, it authenticates the user. Since a persons fingerprint, blood vessel print, or retinal image is unique the only way the system can authenticate is if the proper user is there. The only way an unauthorized user to get access is to physically kidnap the authorized user and force them through the system. For this reason, biometrics are the strongest (and the costliest) for of authentication.

QUESTION 4
Determine the authentication mechanisms that use key fob based identification systems? (Select TWO)

A. Kerberos uses key fob based identification systems.
B. Token uses key fob based identification systems.
C. Biometrics uses key fob based identification systems.
D. Username/password uses key fob based identification systems.
E. Certificates uses key fob based identification systems.

Answer: B, D

QUESTION 5
Why are non-essential services appealing to attackers? (Select TWO)

A. Non-essential services are often appealing to attackers since less bandwidth is used.

B. Non-essential services are often appealing to attackers since the surface area for the attack is reduced.

C. Non-essential services are often appealing to attackers since root level access is offered.

D. Non-essential services are often appealing to attackers since attacks are maintained that go unnoticed.

E. Non-essential services are often appealing to attackers since it's not typically configured correctly or secured.

F. Non-essential services are often appealing to attackers since it's not visible to IDS.

Answer: D, E

QUESTION 6
Which of the following attacks uses ICMP (Internet Control Message Protocol) and improperly formatted MTUs (Maximum Transmission Unit) to crash a target computer?

A. Man in the middle attack
B. Smurf attack
C. Ping of death attack
D. TCP SYN (Transmission Control Protocol / Synchronized) attack

Answer: C

Explanation:
The Ping of Death attack involved sending IP packets of a size greater than 65,535 bytes to the target computer. IP packets of this size are illegal, but applications can be built that are capable of creating them. Carefully programmed operating systems could detect and safely handle illegal IP packets, but some failed to do this.

Note: MTU packets that are bigger than the maximum size the underlying layer can handle are fragmented into smaller packets, which are then reassembled by the receiver. For ethernet style devices, the MTU is typically 1500.

Incorrect Answers
A: A man in the middle attack allows a third party to intercept and replace components of the data stream.

B: The "smurf" attack, named after its exploit program, is one of the most recent in the category of network-level attacks against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim.

D: In a TCP SYN attack a sender transmits a volume of connections that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate TCP users.

QUESTION 7
Which of the following best describes TCP/IP (Transmission Control Protocol/Internet Protocol) session hijacking?

A. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state is altered in a way that intercepts legitimate packets and allows a third party host to insert acceptable packets.

B. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state is altered allowing third party hosts to create new IP (Internet Protocol) addresses.

C. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state remains unaltered allowing third party hosts to insert packets acting as the server.

D. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state remains unaltered allowing third party hosts to insert packets acting as the client.

Answer: A

Explanation:
A detailed site on how to hijack a TCP/IP a session can be found at:
http://staff.washington.edu/dittrich/talks/qsm-sec/script.html

QUESTION 8
What is the process of forging an IP (Internet Protocol) address to impersonate another machine called?

A. TCP/IP (Transmission Control Protocol/Internet Protocol) hijacking
B. IP (Internet Protocol) spoofing
C. man in the middle
D. replay

Answer: B

Explanation:
The word spoofing was popularized in the air-force. When a fighter jet notices an enemy missile (air-to-air or surface-to-air) coming, the pilot will fire off a flair or a chaff (depending on whether or not the missile is heat seeking or radar guided) to spoof (trick) the missile into going after the wrong target. IP spoofing works the same way, and is commonly used by computer hackers because it's easy to implement, it takes advantage of someone else's trust relationship, it makes it harder to identify the source of the true attack, and it focuses attention away to an innocent 3rd party.

QUESTION 9
Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Differential cryptanalysis
B. Differential linear cryptanalysis
C. Birthday attack
D. Statistical attack

Answer: C
A good hashing algorithm should not produce the same hash value for two different messages. If the algorithm does produce the same value for two distinctly different messages, it is referred to as a collision. If an attacker finds an instance of a collision, he has more information to use when trying to break the cryptographic methods used. A complex way of attacking a one-way hash function is called the birthday attack. If an attacker has one hash value and wants to find a message that hashes to the same hash value, this process could take him years. However, if he just wants to find any two messages with the same hashing value, it could take him only a couple hours.

QUESTION 10
What should a network administrator's first course of action be on receiving an e-mail alerting him to the presence of a virus on the system if a specific executable file exists?

A. Investigate the e-mail as a possible hoax with a reputable anti-virus vendor.
B. Immediately search for and delete the file if discovered.
C. Broadcast a message to the entire organization to alert users to the presence of a virus.
D. Locate and download a patch to repair the file.

Answer: A

Explanation:
If a virus threat is for real, the major anti-virus players like Symantec, McAfee, or Sophos will know about it before you, and they will have details on their sites.

Incorrect answers:
Searching for and deleting a file is not only a waste of time with today's OS's complex directory systems, but its also ineffective. One can miss a file, the file could be hidden, the wrong file can be deleted, and worst of all: when you delete a file it doesn't really get completely deleted, instead it gets sent to a 'recycle bin.' Broadcasting an alert and creating panic isn't the right thing to do, because it will waste bandwidth, and perhaps terrorizing the users is the original intent of the attack. The act of locating and downloading a patch

isn't just time consuming, but there's a chance that the patch itself could be the virus, or the process of resetting the computer could activate the virus.

QUESTION 11
Which of the following are characteristics of a computer virus?

A. Find mechanism, initiation mechanism and propagate.
B. Learning mechanism, contamination mechanism and exploit.
C. Search mechanism, connection mechanism and integrate.
D. Replication mechanism, activation mechanism and objective.

Answer: D

Explanation:
Replication mechanism: To replicate a virus needs to attach itself to the right code, where it can replicate and spread past security systems into other systems. Activation mechanism: Most viruses require the user to actually do something. During the 80's and early 90's most viruses were activated when you booted from a floppy disk, or inserted a new floppy disk into an infected drive. Nowadays most computer virus's come as email forwards, and they require the user to execute. Objective: many viruses have no objective at all, but some have the objective to delete data, hog up memory, or crash the system.

QUESTION 12
Why does social engineering attacks often succeed?

A. strong passwords are not required
B. lack of security awareness
C. multiple logins are allowed
D. audit logs are not monitored frequently

Answer: B

Explanation:
Social engineering attacks work because of the availability heuristic, law of reciprocity, and law of consistency. In the past people have had experiences where a co-worker with a legitimate problem asked for help and been grateful for it. So by consistency, they feel the urge to help others again the way they've helped out somebody in the past. By availability, when someone asks for help, they associate that ask for help for every legitimate cry for help, and times when they needed help themselves and were helped; so essentially they're being a good Samaritan. If an awareness program were to be implemented where employees could be aware of social engineering tactics, they would be more likely to think about them, and be more suspect of an attack when someone does ask for a favor. With this knowledge in intuition, an employee will make a smarter decision.

QUESTION 13
In addition to opening the appropriate L2TP (Layer Two Tunneling Protocol) and IKE (Internet Key Exchange) transport layer ports on the perimeter router and firewall, what steps must be performed on the perimeter router and firewall to allow AH (Authentication Header) and ESP (Encapsulating Security Payload) tunnel-encapsulated IPSec (Internet Protocol Security) traffic to flow between a client and the firewall?

A. The perimeter router and firewall must allow inbound protocol number 51 for ESP (Encapsulating Security Payload) encapsulated IPSec (Internet Protocol Security) traffic

B. The perimeter router and firewall must allow inbound protocol number 49 for ESP (Encapsulating Security Payload) encapsulated IPSec (Internet Protocol Security) traffic

C. The perimeter router and firewall must allow inbound protocol numbers 50 and 51 for ESP (Encapsulating Security Payload) and All (Authentication Header) encapsulated IPSec (Internet Protocol Security) traffic

D. The perimeter router and firewall must allow inbound protocol numbers 52 and 53 for AH (Authentication Header) and ESP (Encapsulating Security Payload) encapsulated IPSec (Internet Protocol Security) traffic

Answer: C

Explanation:
The most secure firewall configuration is one in which the firewall permits only IKE and IPSec traffic to flow between the specific IP addresses of the peers. However, if these addresses are not static, or if there are many addresses, a less secure configuration might be required to permit IPSec and IKE traffic to flow between subnets. When a firewall or filtering router exists between IPSec peers, it must be configured to forward IPSec traffic on UDP source and destination port 500, IP protocol 50 (ESP), or IP protocol 51 (AH).

Reference:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=

QUESTION 14
What is the main purpose of an e-mail relay server?

A. It is used to block all spam, which allows the e-mail system to function more efficiently without the additional load of spam.

B. It is used to prevent viruses from entering the network.

C. It is used to defend the primary e-mail server and limit the effects of any attack.

D. It is used to eliminate e-mail vulnerabilities since all e-mail is passed through the relay first.

Answer: C

Explanation:
An email relay will essentially make your mail server invisible to the internet, so you can protect yourself from port scans, viruses, and arbitrary access.

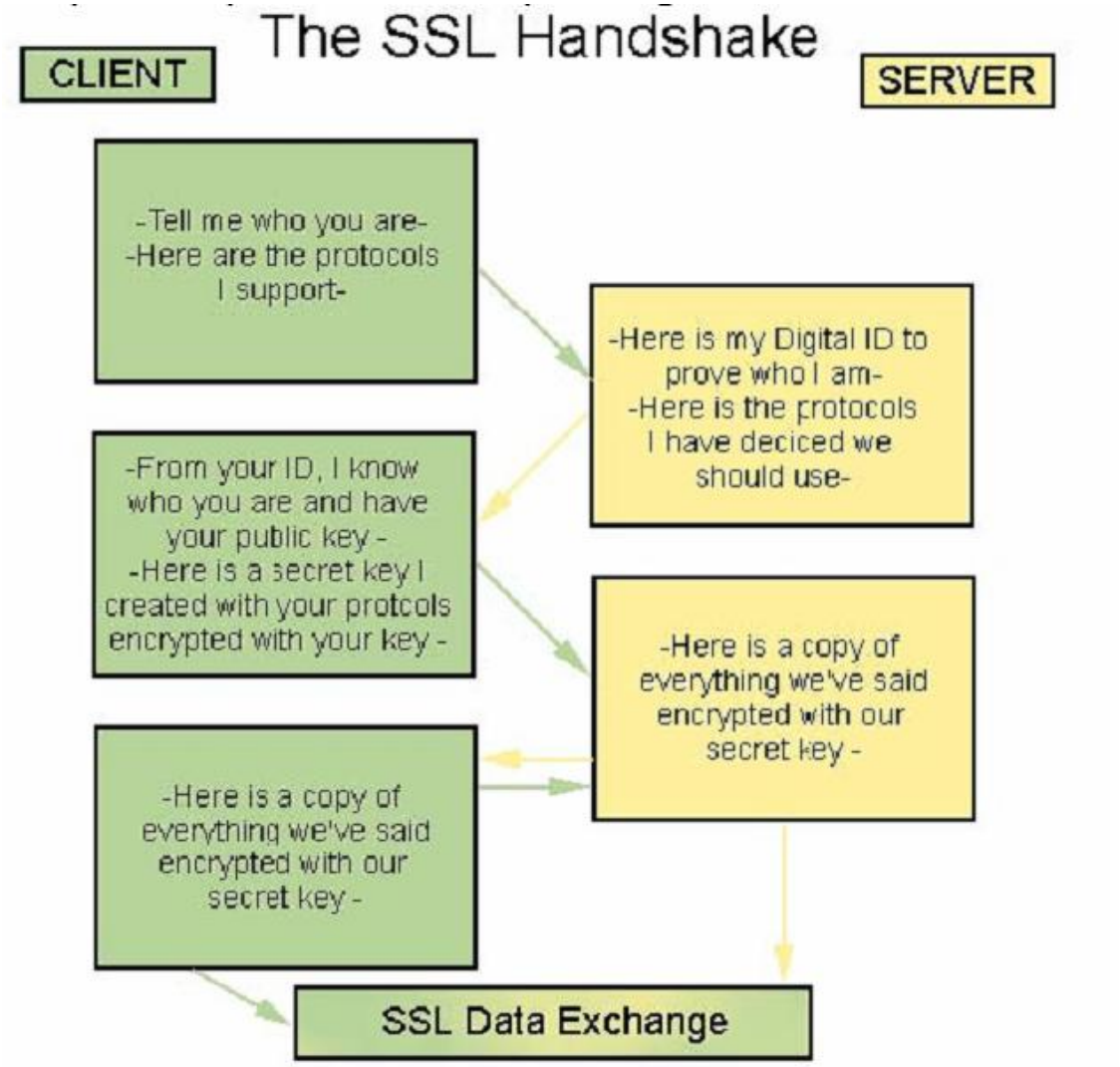
QUESTION 15
How many steps are used during the SSL (Secure Sockets Layer) handshake process?

A. Five
B. Six
C. Seven

D. Eight

Answer: B

Explanation:
Graphical explanation of 6 steps to Digital Handshake for SSL



Note: The handshake begins when a browser connects to an SSL-enabled server, and asks the server to send back its identification, a digital certificate that usually contains the server name, the trusted certifying authority, and the server public encryption key. The browser can contact the server of the trusted certifying authority and confirm that the certificate is authentic before proceeding. The browser then presents a list of encryption algorithms and hashing functions (used to generate a number from another); the server picks the strongest encryption that it also supports and notifies the client of the decision. In order to generate the session keys used for the secure connection, the browser uses the server public key from the certificate to encrypt a random number and send it to the server. The client can encrypt this data, but only the server can decrypt it: this is the one fact that makes the keys hidden from third parties, since only the server and the client have access to this data. The server replies with more random data (which doesn't have to be

encrypted), and then both parities use the selected hash functions on the random data to generate the session keys. This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the session keys. The SSL handshake allows the establishment of a secured connection over an insecure channel. Even if a third party were to listen to the conversation, it would not be able to obtain the session keys. The process of creating good random numbers and applying hash functions can be quite slow, but usually the session keys are cached, so the handshake occurs only on the first connection between the parties. This process works on top of HTTP, so its portable to any platform that supports it, and is in principle applicable to other protocols as well (Welling 2001, p.334). The process described is part of SSL version 2.0, but version 3.0 is supposed to replace it soon. Another standard, Transport Layer Security (TSL) is still in draft and is supposed to replace SSL in the future.

QUESTION 16
Which of the following represents the main advantage of using SSL (Secure Sockets Layer) has over HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)?

A. SSL (Secure Sockets Layer) offers full application security for HTTP (Hypertext Transfer Protocol) while HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) does not.

B. SSL (Secure Sockets Layer) supports additional application layer protocols such as FTP (File Transfer Protocol) and NNTP (Network News Transport Protocol) while HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) does not.

C. SSL (Secure Sockets Layer) and HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) are transparent to the application.

D. SSL (Secure Sockets Layer) supports user authentication and HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) does not.

Answer: B

Explanation:
SSL on its own works at the session layer (layer 5) so it has more versatility in protocols that it supports.

QUESTION 17
Pass.com issues Certificates as a Local Registration Authority.

Identify the actions that should be taken to ensure that e-mails sent to clients outside the company can be authenticated by the recipients?

A. Your best option would be to ensure that digital signatures are turned off on all outgoing e-mails.
B. Your best option would be to request that the recipients turn on their digital signatures.
C. Your best option would be to request that the recipients to add them to their spam filter as 'Allow'.
D. Your best option would be to make use of a free online Internet e-mail account.

Answer: A

QUESTION 18
What is the purpose of a FTP (File Transfer Protocol) bounce attack?

A. Exploiting a buffer overflow vulnerability on the FTP (File Transfer Protocol) server
B. Rebooting the FTP (File Transfer Protocol) server
C. Storing and distributing malicious code
D. Establishing a connection between the FTP (File Transfer Protocol) server and another computer

Answer: D

Explanation:
In some implementations of FTP daemons, the PORT command can be misused to open a connection to a port of the attacker's choosing on a machine that the attacker could not have accessed directly. There have been ongoing discussions about this problem (called "FTP bounce") for several years, and some vendors have developed solutions for this problem.

For more detailed information on this FTP Bounce attack refer to the hyperlink.

Reference:
http://www.cert.org/advisories/CA-1997-27.html

QUESTION 19
Which of the following can be used to prevent intruders from using access points on a wireless network?

A. ESP (Encapsulating Security Payload)
B. WEP (Wired Equivalent Privacy)
C. TLS (Transport Layer Security)
D. SSL (Secure Sockets Layer)

Answer: B

Explanation:
The 802.11 standard describes the communication that occurs in wireless local area networks (LANs). The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP. WEP relies on a secret key that is shared between a mobile station (eg. a laptop with a wireless Ethernet card) and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system we are aware of has mechanisms to support such techniques.

Reference:
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

QUESTION 20
With regard to network based lDSs (Intrusion Detection Systems), which of the following statements is true?

A. Network based lDSs (Intrusion Detection System) are never passive devices that listen on a network wire- without interfering with the normal operation of a network.

B. Network based IDSs (Intrusion Detection System) are usually passive devices that listen on a network wire while interfering with the normal operation of a network.

C. Network based lDSs (Intrusion Detection System) are usually intrusive devices that listen on a network wire while interfering with the normal operation of a network.

D. Network based lDSs (Intrusion Detection System) are usually passive devices that listen on a network wire without interfering with the normal operation of a network.

Answer: D

Explanation:
In a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

QUESTION 21
Which of the following best describes tunneling?

A. The act of encapsulating encrypted/secure IP packets inside of ordinary/non-secure IP packets.
B. The act of encapsulating ordinary/non-secure IP packets inside of encrypted/secure IP packets.
C. The act of encapsulating encrypted/secure IP packets inside of encrypted/non-secure IP packets.
D. The act of encapsulating ordinary/secure IP packets inside of ordinary/non-secure IP packets.

Answer: B

Explanation:
IPSec Tunneling
When used alone for interoperability scenarios, IPSec performs Layer 3 tunneling, meaning the tunneled payload is a Network Layer packet. The entire IP packet is encapsulated and encrypted for transfer by one of the IPSec security protocols:

ESP Tunnel Mode
The inner IP header (the original packet header) usually carries the ultimate source and destination addresses, while the outer IP header contains the address of a security gateway. The Signed area indicates where the packet has been protected with integrity. The Encrypted area indicates what information is encrypted for confidentiality. The original header is placed after the ESP header. The entire packet is appended with an ESP trailer prior to encryption. Everything following the ESP header, except for the ESP authentication trailer, is encrypted, including the original header because it is now considered to be part of the data portion. The entire packet is then encapsulated. The information in the new IP header is used to route the packet from origin to the next destination; usually a security gateway.

QUESTION 22
What are the three categories of active responses relating to intrusion detection?

A. Collect additional information, maintain the environment, and take action against the intruder.
B. Collect additional information, change the environment, and alert the manager.
C. Collect additional information, change the environment, and take action against the intruder.
D. Discard any additional information, change the environment, and take action against the intruder.

Answer: C

Explanation:
An active intrusion detection response is to begin taking action against the intruder as soon as the breach is detected. Te principles are: detection (collect additional information), deflection (change the environment), and countermeasures (take action against the intruder). So changing the environment to spoof the attacker and hide your valuable resources; and collecting details about the source of the intrusion and the type of intrusion to gather evidence for prosecution and future system hardening are all components of active intrusion detection.

QUESTION 23
What is the main purpose of TCP (Transmission Control Protocol) wrappers?

A. Preventing IP (Internet Protocol) spoofing.
B. Controlling access to selected services.
C. Encrypting TCP (Transmission Control Protocol) traffic.
D. Sniffing TCP ('transmission Control Protocol) traffic to troubleshoot.

Answer: B

Explanation:
TCP wrappers are an additional method of providing security against unwelcome visitors. In a Solaris environment there's a TCP daemon called inted which responds to TCP/IP connections and initiates the right program to furnish the needs of that request. A TCP wrapper, wraps itself around this daemon with a tcpd program which logs the incoming request first, putting up an optional layer of access control that can allow or deny a request depending on where its from.

QUESTION 24
When disabling services to harden a machine against external attacks, what process should be followed?

A. Disable services such as DHCP (Dynamic Host Configuration Protocol) client and print servers from servers that do not use/serve those functions.

B. Disable one unnecessary service after another, while reviewing the effects of the previous action.

C. Research the services and their dependencies before disabling any default services.

D. Disable services not directly related to financial operations.

Answer: C

Explanation:
Platform hardening procedures can be categorized into three basic areas:

* The first area to address is removing unused software and processes from the workstations. The services and processes may create opportunities for exploitation.

* The second are involves ensuring that all services and applications are up-to-date and configured in the most secure manner allowed. This may include assigning passwords, limiting access, and restricting capabilities.

* The third area to address involves the minimization of information dissemination about the operating system, services, and capabilities of the system.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 120

QUESTION 25
Which of the following kinds of attacks is a hashed password vulnerable to?

A. Man in the middle.
B. Dictionary or brute force.
C. Reverse engineering.
D. DoS (Denial of Service)

Answer: B

Explanation:
A hashed password cannot be guessed, or reversed engineered. Hashing is a number used for data integrity also known as checksum, not encryption of password. As you can see the hash value is just a single number. The hash value cannot be used to derive the meaning of the original message.

Note: If a hash was stolen off the wire using a man in the middle attack, it would do him no good. The reason is that the hash can represent several different words. The hash cannot be used to crack a password or message; it is used to verify or to store on a server as opposed to plain text. But a password can still be guessed using a dictionary or brute force. Here is how a hash is arrived at.

Password: this
ASCll Values t = 116, h = 104, i = 105, s = 115 (These values are multiplied by 2 to get the calculated number, which would be 232, 208, 210, 230. These numbers are added together then divided by 10. (232+208+210+230)/10 This gives you a hash of 80, but there are other number/ letter combinations that would give you this one way hash. So it cannot be used to crack the password.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 313.

Hashed Password or Password-Verifier
Passwords stored in a database should be stored in a one-way hashed form, to prevent casual retrieval of the information. Since passwords are often vulnerable to dictionary attack, preventing unauthorized access to this data thus remains a high priority. In general, the requirement for secure host storage is characteristic of all mutual authentication cryptographic systems. Alternative public-key methods are especially sensitive to the theft of a stored private key.