



PASS-GUARANTEED.COM

100% Money Back Guarantee!!!

Your #1 Certification Training Resource

Product Details from Pass-Guaranteed.com:

Certified Information Security Systems Professional **CISSP**

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 ->



CISSP Demo – 100% Money Back Guarantee!!!

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 sign up 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.

CISSP Demo – 100% Money Back Guarantee!!!

QUESTION: 1

Why must senior management endorse a security policy?

- A. So that they will accept ownership for security within the organization.
- B. So that employees will follow the policy directives.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they can be held legally accountable.

Answer: A

Explanation:

This really does not a reference as it should be known. Upper management is legally accountable (up to 290 million fine). External organizations answer is not really to pertinent (however it stated that other organizations will respect a BCP and disaster recover plan). Employees need to be bound to the policy regardless of who signs it but it gives validity. Ownership is the correct answer in this statement. However, here is a reference. "Fundamentally important to any security program's success us the senior management's high-level statement of commitment to the information security policy process and a senior management's understanding of how important security controls and protections are to the enterprise's continuity. Senior management must be aware of the importance of security implementation to preserve the organization's viability (and for their own 'due care' protection) and must publicly support that process throughout the enterprise."

QUESTION: 2

What tool do you use to determine whether a host is vulnerable to known attacks?

- A. Padded Cells
- B. Vulnerability analysis
- C. Honey Pots
- D. IDS

Answer: B

Explanation:

Vulnerability analysis (also known as vulnerability assessment) tools test to determine whether a network or host is vulnerable to known attacks. Vulnerability assessment represents a special case of the intrusion detection process. The information sources used are system state attributes and outcomes of attempted attacks. The information sources are collected by a part of the assessment engine. The timing of analysis is interval-based or batch-mode, and the type of analysis is misuse detection. This means that vulnerability assessment systems are essentially batch mode misuse detectors that operate on system state information and results of specified test routines.

QUESTION: 3

A "critical application" is one that MUST

- A. Remain operational for the organization to survive.
- B. Be subject to continual program maintenance.

- C. Undergo continual risk assessments.
- D. Be constantly monitored by operations management.

Answer: A

Explanation:

I am assuming that I don't need to put a reference for this answer. Yeah ok here it is but I cheated and used a earlier reference "A BIA is performed at the beginning of disaster recovery and continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of disaster or disruption."

QUESTION: 4

To ensure least privilege requires that _____ is identified.

- A. what the users privilege owns
- B. what the users job is
- C. what the users cost is
- D. what the users group is

Answer: B

Explanation:

Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges couldn't be used to circumvent the organizational security policy.

Although the concept of least privilege currently exists within the context of the TCSEC, requirements restrict those privileges of the system administrator. Through the use of RBAC, enforced minimum privileges for general system users can be easily achieved.

QUESTION: 5

An example of an individual point of verification in a computerized application is:

- A. An inference check.
- B. A boundary protection.
- C. A sensitive transaction.
- D. A check digit.

Answer: D

Checkdigit: A one-digit checksum.

Checksum: A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.

The checksum may be 8 bits (modulo 256 sum), 16, 32, or some other size. It is computed by summing the bytes or words of the data block ignoring overflow. The checksum may be negated so that the total of the data words plus the checksum is zero.

QUESTION: 6

Which of the following is an operating system security architecture that provides flexible support for security policies?

- A. OSKit
- B. LOMAC
- C. SE Linux
- D. Flask

Answer: D

Explanation:

Flask is an operating system security architecture that provides flexible support for security policies. The architecture was prototyped in the Fluke research operating system. Several of the Flask interfaces and components were then ported from the Fluke prototype to the OSKit. The Flask architecture is now being implemented in the Linux operating system (Security-Enhanced Linux) to transfer the technology to a larger developer and user community.

QUESTION: 7

Which of the following yellow-book defined types of system recovery happens after a system fails in an uncontrolled manner in response to a TCB or media failure and the system cannot be brought to a consistent state?

- A.) Recovery restart
- B.) System reboot
- C.) Emergency system restart
- D.) System Cold start

Answer: C

Explanation:

"Emergency system restart is done after a system fails in an uncontrolled manner in response to a TCB or media failure. In such cases, TCB and user objects on nonvolatile storage belonging to processes active at the time of TCB or media failure may be left in an inconsistent state. The system enters maintenance mode, recovery is performed automatically, and the system restarts with no user processes in progress after bringing up the system in a consistent state."

QUESTION: 8

What is the PRIMARY component of a Trusted Computer Base?

- A. The computer hardware
- B. The security subsystem
- C. The operating system software

D. The reference monitor

Answer: D

Explanation:

"The security kernel is made up of hardware, software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems. There are three main requirements of the security kernel:

It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.

It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way. It must be small enough to be able to be tested and verified in a complete and comprehensive manner.

These are the requirements of the reference monitor; therefore, they are the requirements of the components that provide and enforce the reference monitor concept-the security kernel."

QUESTION: 9

Which TCSEC (Orange Book) level requires the system to clearly identify functions of security administrator to perform security-related functions?

- A.) C2
- B.) B1
- C.) B2
- D.) B3

Answer: D

Explanation:

B1: Labeled Security

Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject and object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement and the design specifications are reviewed and verified. It is intended for environments that require systems to handle classified data.

B2: Structured Protection

The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers.

Subjects and devices require labels, and the system must not allow covert channels. A trusted

path for logon and authentication processes must be in place, which means there are no trapdoors. A trusted path means that the subject is communicating directly with the application or operating system. There is no way to circumvent or compromise this communication channel.

There is a separation of operator and administration functions within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system.

The environment that would require B2 systems could process sensitive data that require a higher degree of security. This environment would require systems that are relatively resistant to penetration and compromise.

(A trusted path means that the user can be sure that he is talking to a genuine copy of the operating system.)

B3: Security Domains

In this class, more granularity is provided in each protection mechanism, and the programming code that is not necessary to support the security policy is excluded. The design and implementation should not provide too much complexity because as the complexity of a system increases, the ability of the individual who need to test, maintain, and configure it reduces; thus, the overall security can be threatened. The reference monitor components must be small enough to test properly and be tamperproof. The security administrator role is clearly defined, and the system must be able to recover from failures without its security level being compromised. When the system starts up and loads its operating system and components, it must be done in an initial secure state to ensure that any weakness of the system cannot be taken advantage of in this slice of time.

QUESTION: 10

Which of the following is a feature of the Rule based access control?

- A. The use of profile.
- B. The use of information flow label.
- C. The use of data flow diagram.
- D. The use of token.

Answer: A

Explanation:

Rule based access control is based on a specific profile for each user. Information can be easily changed for only one user but this scheme may become a burden in a very large environment. A rule-based access control unit will intercept every request to the server and compare the source specific access conditions with the rights of the user in order to make an access decision. A good example could be a firewall. Here a set of rules defined by the network administrator is recorded in a file. Every time a connection is attempted (incoming or outgoing), the firewall software checks the rules file to see if the connection is allowed. If it is not, the firewall closes the connection.

QUESTION: 11

CISSP Demo – 100% Money Back Guarantee!!!

Which of the following security modes of operation involved the highest risk?

- A.) Compartmented Security Mode
- B.) Multilevel Security Mode
- C.) System-High Security Mode
- D.) Dedicated Security Mode

Answer: B

Explanation:

Security Modes

In a secure environment, information systems are configured to process information in one of four security modes. These modes are set out by the Department of Defense as follows:

Systems running compartmental security mode may process two or more types of compartmented information. All system users must have an appropriate clearance to access all information processed by the system but do not necessarily have a need to know all of the information in the system. Compartments are subcategories or compartments within the different classification levels and extreme care is taken to preserve the information within the different compartments. The system may be classified at the Secret level but contain five different compartments, all classified Secret. If a user has only the need to know about two of the five different compartments to do their job, that user can access the system but can only access the two compartments. Compartmented systems are usually dedicated systems for each specific compartment to prevent the chance of any errors, because compartmentalization is the most secret of all the secrets.

Systems running in the dedicated security mode are authorized to process only a specific classification level at a time, and all system users must have clearance and a need to know that information.

Systems running in multilevel security mode are authorized to process information at more than one level of security even when all system users do not have appropriate clearances or a need to know for all information processed by the system. Systems running in system-high security mode are authorized to process only information that all system users are cleared to read and to have a valid need to know.

These systems are not trusted to maintain separation between security levels, and all information processed by these systems must be handled as if it were classified at the same level as the most highly classified information processed by the system.

QUESTION: 12

Which of the following are the types of eye scan in use today?

- A. Retinal scans and body scans.
- B. Retinal scans and iris scans.
- C. Retinal scans and reflective scans.
- D. Reflective scans and iris scans.

Answer: B

Explanation:

There are two types of eye scan in use today for authentication purposes: retinal scans and iris scans. Retinal Scan technology maps the capillary pattern of the retina, a thin (1/50th inch) nerve on the back of the eye. To enroll, a minimum of five scans is required, which takes 45 seconds. The subject must keep his head and eye motionless within 1/2" of the device, focusing on a small rotating point of green light. 320 - 400 points of reference are captured and stored in a 35-byte field, ensuring the measure is accurate with a negligible false rejection rate.

This compares to 30-70 points of reference for a finger scan. Unfortunately a retinal scan is considerably more intrusive than an iris scans and many people are hesitant to use the device [Retina-scan]. In addition a significant number of people may be unable to perform a successful enrolment, and there exist degenerative diseases of the retina that alter the scan results over time. Despite these disadvantages, there are several successful implementations of this technology [Retina-scan].

QUESTION: 13

Which of the following is a disadvantage of a memory only card?

- A. High cost to develop.
- B. High cost to operate.
- C. Physically infeasible.
- D. Easy to counterfeit.

Answer: D

Explanation:

Memory Only Card - This type of card is the most common card. It has a magnetic stripe on the back. These cards can offer two-factor authentication, the card itself (something you have) and the PIN (something you know). Everyone is familiar with the use of an ATM (Automated Teller Machine) card. These memory cards are very easy to counterfeit. There was a case in Montreal where a store owner would swipe the card through for the transaction; he should then swipe it through a card reader to get a copy, while a small hidden camera was registering the PIN as the user was punching it on the pad. This scheme was quickly identified as the victims had one point in common; they all visited the same store.

QUESTION: 14

Which of the following attacks could be the most successful when the security technology is properly implemented and configured?

- A. Logical attacks
- B. Physical attacks
- C. Social Engineering attacks
- D. Trojan Horse attacks

Answer: C

Explanation:

Social Engineering attacks - In computer security systems, this type of attack is usually the most

CISSP Demo – 100% Money Back Guarantee!!!

successful, especially when the security technology is properly implemented and configured. Usually, these attacks rely on the faults in human beings.

An example of a social engineering attack has a hacker impersonating a network service technician. The serviceman approaches a low-level employee and requests their password for network servicing purposes. With smartcards, this type of attack is a bit more difficult. Most people would not trust an impersonator wishing to have their smartcard and PIN for service purposes.

QUESTION: 15

Which expert system operating mode allows determining if a given hypothesis is valid?

- A.) Vertical chaining
- B.) Lateral chaining
- C.) Forward chaining
- D.) Backward chaining

Answer: D

Explanation:

"The expert system operates in either a forward-chaining or backward-chaining mode. In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs. In a backward-chaining mode, the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs. Another type of expert system is the blackboard. A blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual "blackboard," wherein information or solutions are placed on the blackboard by the plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.

QUESTION: 16

SQL security issues include which of the following?

- A.) The granularity of authorizations
- B.) The size of databases
- C.) The complexity of key structures
- D.) The number of candidate key elements

Answer: A

Developed by IBM, SQL is a standard data manipulation and relational database definition language. The SQL Data Definition Language creates and deletes views and relations (tables). SQL commands include Select, Update, Delete, Insert, Grant, and Revoke. The latter two commands are used in access control to grant and revoke privileges to resources. Usually, the owner of an object can withhold or transfer GRANT privileges to an object to another subject. If the owner intentionally does not transfer the GRANT privileges, however, which are relative to an object to the individual A, A cannot pass on the GRANT privileges to another subject. In some instances, however, this security control can be circumvented. For example, if A copies the object, A essentially becomes the owner of that object and thus can transfer the GRANT privileges to another user, such as user B. SQL security issues include

the granularity of authorization and the number of different ways you can execute the same query.

QUESTION: 17

Which one of the following properties of a transaction processing system ensures that once a transaction completes successfully (commits), the update service even if there is a system failure?

- A. Atomicity
- B. Consistency
- C. Isolation
- D. Durability

Answer: A

Atomicity is correct. Consistency is not a viable answer.

Atomicity states that database modifications must follow an "all or nothing" rule. Each transaction is said to be "atomic." If one part of the transaction fails, the entire transaction fails. It is critical that the database management system maintain the atomic nature of transactions in spite of any DBMS, operating system or hardware failure.

Consistency states that only valid data will be written to the database. If, for some reason, a transaction is executed that violates the database's consistency rules, the entire transaction will be rolled back and the database will be restored to a state consistent with those rules. On the other hand, if a transaction successfully executes, it will take the database from one state that is consistent with the rules to another state that is also consistent with the rules.

Isolation requires that multiple transactions occurring at the same time not impact each other's execution. For example, if Joe issues a transaction against a database at the same time that Mary issues a different transaction, both transactions should operate on the database in an isolated manner. The database should either perform Joe's entire transaction before executing Mary's or vice-versa. This prevents Joe's transaction from reading intermediate data produced as a side effect of part of Mary's transaction that will not eventually be committed to the database. *Note:* that the isolation property does not ensure which transaction will execute first, merely that they will not interfere with each other.

Durability ensures that any transaction committed to the database will not be lost. Durability is ensured through the use of database backups and transaction logs that facilitate the restoration of committed transactions in spite of any subsequent software or hardware failures.

QUESTION: 18

Removing unnecessary processes, segregating inter-process communications, and reducing executing privileges to increase system security is commonly called

- A. Hardening
- B. Segmenting
- C. Aggregating
- D. Kerneling

Answer: A

Explanation:

What is hardening? Naturally, there is more than one definition, but in general, one tightens control using policies which affect authorization, authentication and permissions. Nothing happens by default. You only give out permission after thinking about it, something like "deny all" to everyone, then "allow" with justification. Shut off everything, then only turn on that which must be turned on. It is not unlike locking every single door, window and access point in your house, then unlocking only those that need to be. It is quite common for users to take all the defaults when their new system gets turned on making for instant vulnerability. A major problem is trying to figure out where all those details are that need to be turned off, without making the system unusable.

QUESTION: 19

In what way could Java applets pose a security threat?

- A.) Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
- B.) Java interpreters do not provide the ability to limit system access that an applet could have on a client system
- C.) Executables from the Internet may attempt an intentional attack when they are downloaded on a client system
- D.) Java does not check the byte code at runtime or provide other safety mechanisms for program isolation from the client system.

Answer: C

Explanation:

Java Security

Java applets use a security scheme that employs a sandbox to limit the applet's access to certain specific areas within the user's system and protects the system from malicious or poorly written applets. The applet is supposed to run only within the sandbox. The sandbox restricts the applet's environment by restricting access to a user's hard drives and system resources. If the applet does not go outside the sandbox, it is considered safe.

However, as with many other things in the computing world, the bad guys have figured out how to escape their confines and restrictions. Programmers have figured out how to write applets that enable the code to access hard drives and resources that are supposed to be protected by the Java security scheme. This code can be malicious in nature and cause destruction and mayhem to the user and her system.

Java employs a sandbox in its security scheme, but if an applet can escape the confines of the sandbox, the system can be easily compromised.

QUESTION: 20

IDS can be described in terms of what fundamental functional components?

- A. Response
- B. Information Sources
- C. Analysis
- D. All of the choices.

Answer: D

Explanation:

Many IDSs can be described in terms of three fundamental functional components: Information Sources - the different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.

Analysis - the part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection.

Response - the set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

QUESTION: 21

What are the primary approaches IDS takes to analyze events to detect attacks?

- A. Misuse detection and anomaly detection.
- B. Log detection and anomaly detection.
- C. Misuse detection and early drop detection.
- D. Scan detection and anomaly detection.

Answer: A

Explanation:

There are two primary approaches to analyzing events to detect attacks: misuse detection and anomaly detection. Misuse detection, in which the analysis targets something known to be "bad", is the technique used by most commercial systems. Anomaly detection, in which the analysis looks for abnormal patterns of activity, has been, and continues to be, the subject of a great deal of research.

Anomaly detection is used in limited form by a number of IDSs. There are strengths and weaknesses associated with each approach, and it appears that the most effective IDSs use mostly misuse detection methods with a smattering of anomaly detection components.

QUESTION: 22

CISSP Demo – 100% Money Back Guarantee!!!

To ensure dependable and secure logging, all computers must have their clock synchronized to:

- A. A central timeserver.
- B. The log time stamp.
- C. The respective local times.
- D. None of the choices.

Answer: A

Explanation:

The following pre-requisite must be met to ensure dependable and secure logging: All computers must have their clock synchronized to a central timeserver to ensure accurate time on events being logged.

If possible all logs should be centralized for easy analysis and also to help detect patterns of abuse across servers. Logging information traveling on the network must be encrypted if possible. Log files are stored and protected on a machine that has a hardened shell. Log files must not be modifiable without a trace or record of such modification.

QUESTION: 23

Which of the following are functions that are compatible in a properly segregated environment?

- A.) Security administration and quality assurance
- B.) Security administration and data entry
- C.) Security administration and application programming
- D.) Application programming and data entry

Answer: A

Explanation:

Security Administration and Quality Assurance are the most similar tasks.

Administrative Management: Administrative management is a very important piece of operational security. One aspect of administrative management is dealing with personnel issues.

This includes separation of duties and job rotation. The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way.

High-risk activities should be broken up into different parts and distributed to different individuals. This way the company does not need to put a dangerously high level of trust on certain individuals and if fraud were to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity.

Separation of duties also helps to prevent many different types of mistakes that can take place if one person is performing a task from the beginning to the end. For instance, a programmer should not be the one to test her own code. A different person with a different job and agenda should perform functionality and integrity testing on the programmer's code because the programmer may have a

focused view of what the program is supposed to accomplish and only test certain functions, input values, and in certain environments.

Another example of separation of duties is the difference between the functions of a computer operator versus the functions of a system administrator. There must be clear cut lines drawn between system administrator duties and computer operator duties. This will vary from environment to environment and will depend on the level of security required within the environment. The system administrators usually have responsibility of performing backups and recovery procedures, setting permissions, adding and removing users, setting user clearance, and developing user profiles. The computer operator on the other hand, may be allowed to install software, set an initial password, alter desktop configurations, and modify certain system parameters. The computer operator should not be able to modify her own security profile, add and remove users globally, or set user security clearance. This would breach the concept of separation of duties.

QUESTION: 24

The concentric circle approach is used to

- A. Evaluate environmental threats.
- B. Assess the physical security facility,
- C. Assess the communications network security.
- D. Develop a personnel security program.

Answer: B

Explanation:

The original answer for this question was C (assess the communications network security) however I think the concentric circle is defining what in the krutz book is know as the security perimeter. To this end this is a reference:

"A circular security perimeter that is under the access control defines the area or zone to be protected. Preventive/physical controls include fences, badges, multiple doors (man-traps that consists of two doors physically separated so that an individual can be 'trapped' in the space between the doors after entering one of the doors), magnetic card entry systems, biometrics (for identification), guards, dogs, environmental control systems (temperature, humidity, and so forth), and building and access area layout."

This is a standard concentric circle model shown in Figure 1 . If you've never seen this, you haven't had a security lecture.

On the outside is our perimeter. We are fortunate to have some defenses on our base. Although some bases don't have people guarding the gates and checking IDs any longer, there's still the perception that it's tougher to commit a crime on a Naval base than it would be at GM.

The point is: How much control do we have over fencing and guards? The answer: Not much. The next circle, the red circle, contains your internal access controls. For our purposes, the heart of the red circle is the computer. That's what I want to zero in on. The internal controls are the

things you can do to keep people out of your PCs and off your network.

QUESTION: 25

What encryption algorithm is best suited for communication with handheld wireless devices?

- A.) ECC
- B.) RSA
- C.) SHA
- D.) RC4

Answer: A

Explanation:

Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An Elliptic Curve Cryptosystem (ECC) provides much of the same functionality that RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. Some devices have limited processing capacity, storage, power supply, and bandwidth like wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality requiring a smaller percentage of resources required by RSA and other algorithms, so it is used in these types of devices. In most cases, the longer the key length, the protection provided, but ECC can provide the same level of protection with a key size that is smaller than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

QUESTION: 26

In what type of attack does an attacker try, from several encrypted messages, to figure out the key using the encryption process?

- A.) Known-plaintext attack
- B.) Ciphertext-only attack
- C.) Chosen-Ciphertext attack
- D.) Known Ciphertext attack

Answer: B

Explanation:

Ciphertext-Only Attack

In this type of attack, the attacker has the ciphertext of several messages. Each of the messages has been encrypted using the same encryption algorithm. The attacker's goal is to discover the key that was used in the encryption process. Once the attacker figures out the key, she can decrypt all other messages encrypted with the same key.

A ciphertext-only attack is the most common because it is very easy to get ciphertext by sniffing someone's traffic, but it is the hardest attack to actually be successful at because the attacker has so little information about the encryption process.

QUESTION: 27

Which of the following layers supervises the control rate of packet transfers in an Open Systems Interconnections (OSI) implementation?

- A. Physical
- B. Session
- C. Transport
- D. Network

Answer: C

Explanation:

The transport layer defines how to address the physical locations and /or devices on the network, how to make connections between nodes, and how to handle the networking of messages. It is responsible for maintaining the end-to-end integrity and control of the session. Services located in the transport layer both segment and reassemble the data from upper-layer applications and unite it onto the same data stream, which provides end-to-end data transport services and establishes a logical connection between the sending host and destination host on a network.

The transport layer is also responsible for providing mechanisms for multiplexing upper-layer applications, session establishment, and the teardown of virtual circuits.

Transport Layer

The agreement on these issues before transferring data helps provide more reliable data transfer, error detection and correction, and flow control and it optimizes network services needed to perform these tasks.

QUESTION: 28

The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers are in which of the following order (1 to 7). (Fill in the blank)

| Select from these | Place here |
|--------------------|--------------------|
| Network layer | Place layer 1 here |
| Physical layer | Place layer 2 here |
| Session layer | Place layer 3 here |
| Transport layer | Place layer 4 here |
| Data link layer | Place layer 5 here |
| Application layer | Place layer 6 here |
| Presentation Layer | Place layer 7 here |

Answer:

Place here

| |
|--------------------|
| Physical layer |
| Data link layer |
| Network layer |
| Transport Layer |
| Session layer |
| Presentation Layer |
| Application layer |

Explanation:

Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer

QUESTION: 29

Which protocol matches an Ethernet address to an Internet Protocol (IP) address?

- A.) Address Resolution Protocol (ARP)
- B.) Reverse Address Resolution Protocol (RARP)
- C.) Internet Control Message Protocol (ICMP)
- D.) User Datagram Protocol (UDP)

Answer: B

Explanation:

"As with ARP, Reverse Address Resolution Protocol (RARP) frames go to all systems on the subnet, but only the RARP server responds. Once the RARP server receives this request, it looks in its table to see which IP address matches the broadcast hardware address. The server then sends a message back to the requesting computer that contains its IP address. The system now has an IP address and can function on the network.

QUESTION: 30

In which way does a Secure Socket Layer (SSL) server prevent a "man-in-the-middle" attack?

- A. It uses signed certificates to authenticate the server's public key.
- B. A 128 bit value is used during the handshake protocol that is unique to the connection.
- C. It uses only 40 bits of secret key within a 128 bit key length.
- D. Every message sent by the SSL includes a sequence number within the message contents.

Answer: A

Explanation:

Secure Sockets Layer (SSL). An encryption technology that is used to provide secure transactions such as the exchange of credit card numbers. SSL is a socket layer security protocol and is a two-layered protocol that contains the SSL Record Protocol and the SSL Handshake Protocol. Similar to SSH, SSL uses symmetric encryption for private connections and asymmetric or public key cryptography (certificates) for peer authentication. It also uses a Message Authentication Code for message integrity checking.

It prevents a man in the middle attack by confirming that you are authenticating with the server desired prior entering your user name and password. If the server was not authenticated, a man-in-the-middle could retrieve the username and password then use it to login.

QUESTION: 31

Which one of the following instigates a SYN flood attack?

- A. Generating excessive broadcast packets.
- B. Creating a high number of half-open connections.
- C. Inserting repetitive Internet Relay Chat (IRC) messages.
- D. A large number of Internet Control Message Protocol (ICMP) traces.

Answer: B

Explanation:

A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target system to time out while waiting for the proper response, which makes the system crash or become unusable.

"In a SYN flood attack, hackers use special software that sends a large number of fake packets with the SYN flag set to the targeted system. The victim then reserves space in memory for the connection and attempts to send the standard SYN/ACK reply but never hears back from the originator. This process repeats hundreds or even thousands of times, and the targeted computer eventually becomes overwhelmed and runs out of available resources for the half-opened connections. At that time, it either crashes or simply ignores all inbound connection requests because it can't possibly handle any more half-open connections.

QUESTION: 32

When companies come together to work in an integrated manner such as extranets, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability and responsibility. These aspects should be defined in the contracts that each party signs. What describes this type of liability?

- A.) Cascade liabilities
- B.) Downstream liabilities
- C.) Down-flow liabilities
- D.) Down-set liabilities

Answer: B

Explanation:

When companies come together to work in an integrated manner, such as extranets and VANs, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability, and responsibility needed, which should be clearly defined in the contracts that each party signs. Auditing and testing should be performed to ensure that each party is indeed holding up its side of the bargain and that its technology integrates properly with all other parties. Interoperability can become a large, frustrating, and expensive issue in these types of arrangements.

If one of the companies does not provide the necessary level of protection and their negligence affects a partner they are working with, the affected company can sue the upstream company.

For example, let's say company A and company B have constructed an extranet. Company A does not put in controls to detect and deal with viruses. Company A gets infected with a destructive virus and it is spread to company B through the extranet. The virus corrupts critical data and causes massive disruption to company B's production. Company B can sue company A for being negligent. Both companies need to make sure that they are doing their part to ensure that their activities, or lack of

them, will not negatively affect another company, which is referred to as downstream liability.

QUESTION: 33

The structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media includes?

- A. The Telecommunications and Network Security domain.
- B. The Telecommunications and Netware Security domain.
- C. The Technical communications and Network Security domain.
- D. The Telnet and Network Security domain.

Answer: A

Explanation:

This is pretty straight forward. The four principal pillars of computer security: integrity, authentication, confidentiality and availability are all part of the network security and telecommunication domain. Why? Because those pillars deal with that. We provide integrity through digital signatures, authentication through passwords, confidentiality through encryption and availability by fault tolerance and disaster recovery. All of those are networking and telecommunication components.

QUESTION: 34

By examining the "state" and "context" of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC). This type of firewall system is used in?

- A. First generation firewall systems.
- B. Second generation firewall systems.
- C. Third generation firewall systems.
- D. Fourth generation firewall systems.

Answer: C

Explanation:

Statefull inspection is a third generation firewall technology designed to be aware of, and inspect, not only the information being received, but the dynamic connection and transmission state of the information being received. Control decisions are made by analyzing and utilizing the following: Communication Information, Communication derived state, Application derived state and information manipulation. Here are some characteristics of Statefull Inspection technology on Firewalls:

1. Scan information from all layers in the packet.
2. Save state information derived from previous communications, such as the outgoing Port command of an FTP session, so that incoming data communication can be verified against it.
3. Provides tracking support for connectionless protocols through the use of session state databases.

4. Allow state information derived from other applications access through the firewall for authorized services only, such as previously authenticated users.
5. Evaluate and manipulate flexible expressions based on communication and application derived state information.

QUESTION: 35

Which of the following is responsible for the most security issues?

- A. Outside espionage
- B. Hackers
- C. Personnel
- D. Equipment failure

Answer: C

Explanation:

As I stated earlier in the comments, the great part of the attacks to companies comes from the personnel. Hackers are out there and attack some targets, but should never forget that your worst enemy can be inside of your company. Is for that that we usually implement IDS and profundity security. It's a very good practice to install Host based IDS to limit the ability of internal attackers through the machines.

Another problem with personal is the ignorance, there are time that they just don't know what they are doing, and certainly are violating the security policy.

QUESTION: 36

Which DES modes can best be used for authentication?

- A. Cipher Block Chaining and Electronic Code Book.
- B. Cipher Block Chaining and Output Feedback.
- C. Cipher Block Chaining and Cipher Feedback.
- D. Output Feedback and Electronic Code Book.

Answer: C

Explanation: Cipher Block Chaining (CBC) uses feedback to feed the result of encryption back into the encryption of the next block. The plain-text is XOR'ed with the previous cipher-text block before it is encrypted. The encryption of each block depends on all the previous blocks. This requires that the decryption side processes all encrypted blocks sequentially. This mode requires a random initialization vector which is XOR'ed with the first data block before it is encrypted. The initialization vector does not have to be kept secret. The initialization vector should be a random number (or a serial number), to ensure that each message is encrypted uniquely. In the Cipher Feedback Mode (CFB) is data encrypted in units smaller than the block size. This mode can be used to encrypt any number of bits e.g. single bits or single characters (bytes) before sending across an insecure data link. Both of those method can be best used to provide user authentication capabilities.