Vendor: ISC2

Exam Code: SSCP

Exam Name: Systems Security Certified Practitioner

Version: DEMO

QUESTION 1
Which of the following would assist the most in Host Based intrusion detection?

A. audit trails.
B. access control lists.
C. security clearances.
D. host-based authentication.

Answer: A
Explanation:
To assist in Intrusion Detection you would review audit logs for access violations.

The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.

host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

QUESTION 2
Controls to keep password sniffing attacks from compromising computer systems include which of the following?

A. static and recurring passwords.
B. encryption and recurring passwords.
C. one-time passwords and encryption.
D. static and one-time passwords.

Answer: C
Explanation:
To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.

The following answers are correct:

static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.

encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.

static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

QUESTION 3
Kerberos can prevent which one of the following attacks?

A. tunneling attack.
B. playback (replay) attack.
C. destructive attack.
D. process attack.

Answer: B
Explanation:
Each ticket in Kerberos has a timestamp and are subject to time expiration to help prevent these types of attacks.

The following answers are incorrect:

tunneling attack. This is incorrect because a tunneling attack is an attempt to bypass security and access low-level systems. Kerberos cannot totally prevent these types of attacks.

destructive attack. This is incorrect because depending on the type of destructive attack, Kerberos cannot prevent someone from physically destroying a server.

process attack. This is incorrect because with Kerberos cannot prevent an authorzied individuals from running processes.

QUESTION 4
In discretionary access environments, which of the following entities is authorized to grant information access to other people?

A. Manager
B. Group Leader
C. Security Manager
D. Data Owner

Answer: D
Explanation:
In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.

The following answers are incorrect:

manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

IMPORTANT NOTE:
The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the

specific set of data.

The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

QUESTION 5
What is the main concern with single sign-on?

A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator's workload would increase.
C. The users' password would be too hard to remember.
D. User access rights would be increased.

Answer: A
Explanation:
A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.

The following answers are incorrect:
The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.

The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.

User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

QUESTION 6
Who developed one of the first mathematical models of a multilevel-security computer system?

A. Diffie and Hellman.
B. Clark and Wilson.
C. Bell and LaPadula.
D. Gasser and Lipner.

Answer: C
Explanation:
In 1973 Bell and LaPadula created the first mathematical model of a multi-level security system.

The following answers are incorrect:

Diffie and Hellman. This is incorrect because Diffie and Hellman was involved with cryptography.
Clark and Wilson. This is incorrect because Bell and LaPadula was the first model. The Clark-Wilson model came later, 1987.
Gasser and Lipner. This is incorrect, it is a distractor. Bell and LaPadula was the first model.

QUESTION 7
A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments.
A database security mechanism that enforces this policy would typically be said to provide which

of the following?

A. Content-dependent access control
B. Context-dependent access control
C. Least privileges access control
D. Ownership-based access control

Answer: A
Explanation:
When access control is based on the content of an object, it is considered to be content dependent access control.

Content-dependent access control is based on the content itself.

The following answers are incorrect:

context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains. least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.

QUESTION 8
Which of the following attacks could capture network user passwords?

A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing

Answer: B
Explanation:
A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.
Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap--a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that

segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:

Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

QUESTION 9
Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

A. holiday
B. Christmas12
C. Jenny
D. GyN19Za!

Answer: D
Explanation:
GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.

All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words:

Christmas23
Christmas123
etc...

QUESTION 10
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

A. clipping level
B. acceptance level
C. forgiveness level
D. logging level

Answer: A
Explanation:
The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the

activity, lock a user account, temporarily close a port, etc.

Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attemts, that is the "clipping level".

The other answers are not correct because:

Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.

QUESTION 11
Examples of types of physical access controls include all EXCEPT which of the following?

A. badges
B. locks
C. guards
D. passwords

Answer: D
Explanation:
Passwords are considered a Preventive/Technical (logical) control.

The following answers are incorrect:

badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.

locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association.

QUESTION 12
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

A. clipping level
B. acceptance level
C. forgiveness level
D. logging level

Answer: A
Explanation:
The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc.

Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attemts, that is the "clipping level".

The other answers are not correct because:

Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.

QUESTION 13
Examples of types of physical access controls include all EXCEPT which of the following?

A. badges
B. locks
C. guards
D. passwords

Answer: D
Explanation:
Passwords are considered a Preventive/Technical (logical) control.

The following answers are incorrect:

badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.

locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association.

QUESTION 14
Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access

Answer: A
Explanation:
The Answer: The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.

The following answers are incorrect:

The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force. The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc. The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.

QUESTION 15

What physical characteristic does a retinal scan biometric device measure?

A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The pattern of light receptors at the back of the eye
D. The pattern of blood vessels at the back of the eye

Answer: D
Explanation:
The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers.

The following answers are incorrect:

The amount of light reaching the retina The amount of light reaching the retina is not used in the biometric scan of the retina.
The amount of light reflected by the retina The amount of light reflected by the retina is not used in the biometric scan of the retina.

The pattern of light receptors at the back of the eye This is a distractor

QUESTION 16
Which is the last line of defense in a physical security sense?

A. people
B. interior barriers
C. exterior barriers
D. perimeter barriers

Answer: A

QUESTION 17
The Computer Security Policy Model the Orange Book is based on is which of the following?

A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest

Answer: A
Explanation:
The Computer Security Policy Model Orange Book is based is the Bell-LaPadula Model. Orange Book Glossary.
The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.
TEMPEST is related to limiting the electromagnetic emanations from electronic equipment.

QUESTION 18
The end result of implementing the principle of least privilege means which of the following?

A. Users would get access to only the info for which they have a need to know
B. Users can access all systems.
C. Users get new privileges added when they change positions.
D. Authorization creep.

Answer: A
Explanation:
The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.

The following answers are incorrect:
Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system.

Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.

Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: ASTR14