SSCP$^{Q\&As}$

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

Which of the following is the primary reason why a user would choose a dial-up modem connection to the Internet when they have a faster, secure Internet connection through the organization\\'s network?

A. To access web sites that blocked by the organization\\'s proxy server.

B. To set up public services using the organization\\'s resources.

C. To check their personal e-mail.

D. To circumvent the organization\\'s security policy.

Correct Answer: D

All the choices above represent examples of circumventing the organization\\'s security policy, which is the primary reason why a user would be using a dial-up Internet connection when a secure connection is available through the organization\\'s network. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

QUESTION 2

A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

A. concern that the laser beam may cause eye damage

B. the iris pattern changes as a person grows older.

C. there is a relatively high rate of false accepts.

D. the optical unit must be positioned so that the sun does not shine into the aperture.

Correct Answer: D

Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader. An Iris recognition is a form of biometrics that is based on the uniqueness of a subject\\'s iris. A camera like device records the patterns of the iris creating what is known as Iriscode. It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject\\'s identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.

Reference(s) used for this question:

AIO, 3rd edition, Access Control, p 134.

AIO, 4th edition, Access Control, p 182.

Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition The following answers are incorrect:

concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue. the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the

QUESTION 3

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

A. badges

B. locks

C. guards

D. passwords

Correct Answer: D

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.

The following reference(s) were/was used to create this question:

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of

Computer Security, John Wiley and Sons, 2001, Chapter 2: Access control systems (page 35).

QUESTION 4

Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.

B. The initial authentication steps are done using public key algorithm.

C. The KDC is aware of all systems in the network and is trusted by all of them

D. It performs mutual authentication

Correct Answer: B

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/ server applications by using secret-key cryptography. It has the following characteristics:

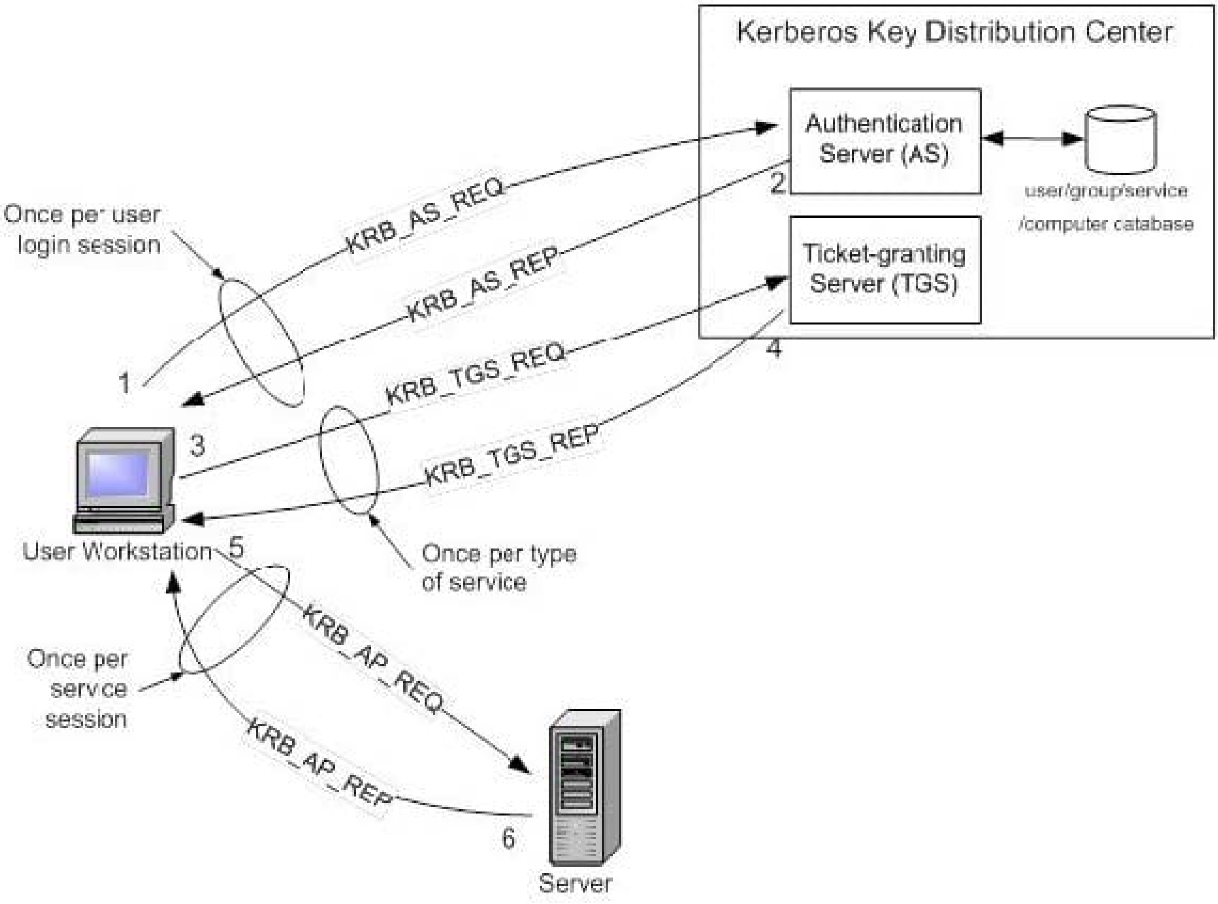
It is secure: it never sends a password unless it is encrypted.

Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.

The concept depends on a trusted third party a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.

It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client. Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS a ticket is a time-limited cryptographic message giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.

Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 "The Kerberos Network Authorization Service (V5)".


Kerberos Key Distribution Center
Authentication Server (AS)
user/group/service /computer database
Ticket-granting Server (TGS)
Once per user login session
KRB_AS_REQ
KRB_AS_REP
1
2
KRB_TGS_REQ
KRB_TGS_REP
3
4
User Workstation
5
Once per type of service
KRB_AP_REQ
KRB_AP_REP
Once per service session
6
Server

Kerberos Authentication Step by Step

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT). Step 2: The Authorization Server verifies the user\\'s access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user\\'s password and sends a message back to the user workstation.

The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key one encrypted with the client password, and one encrypted by the service password.

Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.

Step 6: If mutual authentication is required, then the server will reply with a server authentication message.

The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above. To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client\\'s clock and server\\'s clock. If the difference between a client\\'s clock and the server\\'s clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.

Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.

For more information about Kerberos, see http://web.mit.edu/kerberos/www/.

References:

Introduction to Kerberos Authentication from Intel

and

http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3

and

http://www.ietf.org/rfc/rfc4120.txt

QUESTION 5

Which of the following is best at defeating frequency analysis?

A. Substitution cipher

B. Polyalphabetic cipher

C. Transposition cipher

D. Ceasar Cipher

Correct Answer: B

Simple substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis. In every language, there are words and patterns that are used more than others.

Some patterns common to a language can actually help attackers figure out the transformation between plaintext and ciphertext, which enables them to figure out the key that was used to perform the transformation. Polyalphabetic ciphers use different alphabets to defeat frequency analysis.

The ceasar cipher is a very simple substitution cipher that can be easily defeated and it does show repeating letters.

Out of list presented, it is the Polyalphabetic cipher that would provide the best protection against simple frequency analysis attacks.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, Chapter

8: Cryptography (page 507).

And : DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.