DUMPSHQ

Free Questions for SSCP by dumpshq

Shared by Wood on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?

Options:

A- The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network.

B- They don't protect against IP or DNS address spoofing.

C- They do not support strong user authentication.

D- They are appropriate for medium-risk environment.

Answer:

D

Explanation:

Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port.

They offer minimum security but at a very low cost, and can be an appropriate choice for a low-risk environment.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 60).

Question 2

Question Type: MultipleChoice

Which of the following statements pertaining to IPSec is incorrect?

Options:

A- IPSec can help in protecting networks from some of the IP network attacks.

B- IPSec provides confidentiality and integrity to information transferred over IP networks through transport layer encryption and authentication.

C- IPSec protects against man-in-the-middle attacks.

D- IPSec protects against spoofing.

Answer:

B

Explanation:

IPSec provides confidentiality and integrity to information transferred over IP networks through network (not transport) layer encryption and authentication. All other statements are correct.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 6, Extranet Access Control Issues (page 110).

Question 3

Question Type: **MultipleChoice**

Which SSL version offers client-side authentication?

Options:

A- SSL v1

B- SSL v2

C- SSL v3

D- SSL v4

Answer:

C

Explanation:

Secure Sockets Layer (SSL) is the technology used in most Web-based applications. SSL version 2.0 supports strong authentication of the web server, but the authentication of the client side only comes with version 3.0. SSL v4 is not a defined standard.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 54).

Question 4

Question Type: **MultipleChoice**

Which of the following is the core of fiber optic cables made of?

Options:

A- PVC

B- Glass fibers

C- Kevlar

D- Teflon

Answer:

B

Explanation:

Fiber optic cables have an outer insulating jacket made of Teflon or PVC, Kevlar fiber, which helps to strengthen the cable and prevent breakage, plastic coatings, used to cushion the fiber center. The center (core) of the cable is made of glass or plastic fibers.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 31).

Question 5

Question Type: **MultipleChoice**

Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

Options:

A- Application Layer.

B- Transport Layer.

C- Session Layer.

D- Network Layer.

Answer:

A

Explanation:

The Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at the Application Layer of the Open Systems Interconnect (OSI) model.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

Question 6

Question Type: MultipleChoice

Which of the following protocols is designed to send individual messages securely?

Options:

A- Kerberos

B- Secure Electronic Transaction (SET).

C- Secure Sockets Layer (SSL).

D- Secure HTTP (S-HTTP).

Answer:

D

Explanation:

An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers. SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

Question 7

Question Type: MultipleChoice

What enables a workstation to boot without requiring a hard or floppy disk drive?

Options:

A- Bootstrap Protocol (BootP).

B- Reverse Address Resolution Protocol (RARP).

C- Address Resolution Protocol (ARP).

D- Classless Inter-Domain Routing (CIDR).

Answer:

A

Explanation:

Bootstrap Protocol (BootP) is an Internet Layer protocol that enables a workstation to boot without requiring a hard or floppy disk drive. Reverse Address Resolution Protocol (RARP) is a TCP/IP protocol that permits a physical address, such as an Ethernet address, to be translated into an IP address. Address Resolution Protocol (ARP) is a TCP/IP protocol that permits an IP address to be translated into a physical address. Classless Inter-Domain Routing (CIDR) is a new IP addressing scheme.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

Question 8

Question Type: MultipleChoice

Which protocol is used to send email?

Options:

A- File Transfer Protocol (FTP).

B- Post Office Protocol (POP).

C- Network File System (NFS).

D- Simple Mail Transfer Protocol (SMTP).

Answer:

D

Explanation:

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

Question 9

Question Type: MultipleChoice

Why is Network File System (NFS) used?

Options:

A- It enables two different types of file systems to interoperate.

B- It enables two different types of file systems to share Sun applications.

C- It enables two different types of file systems to use IP/IPX.

D- It enables two different types of file systems to emulate each other.

Answer:

A

Explanation:

Network File System (NFS) is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

Question 10

Question Type: MultipleChoice

What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

Options:

A- It is too complex to manage user access restrictions under TFTP

B- Due to the inherent security risks

C- It does not offer high level encryption like FTP

D- It cannot support the Lightwight Directory Access Protocol (LDAP)

Answer:

B

Explanation:

Some sites choose not to implement Trivial File Transfer Protocol (TFTP) due to the inherent security risks. TFTP is a UDP-based file transfer program that provides no security. There is no user authentication.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.