Free Questions for SSCP by certsinside

Shared by Huber on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following protocols' primary function is to send messages between network devices regarding the health of the network?

Options:

A- Reverse Address Resolution Protocol (RARP).

B- Address Resolution Protocol (ARP).

C- Internet Protocol (IP).

D- Internet Control Message protocol (ICMP).

Answer:

D

Explanation:

Its primary function is to send messages between network devices regarding the health of the network. ARP matches an IP address to an Ethernet address. RARP matches and Ethernet address to an IP address. ICMP runs on top of IP.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Question 2

Question Type: **MultipleChoice**

When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?

Options:

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:

The RARP protocol sends out a packet, which includes its MAC address and a request to be informed of the IP address that should be assigned to that MAC address.

ARP does the opposite by broadcasting a request to find the Ethernet address that matches a known IP address.

ICMP supports packets containing error, control, and informational messages (e.g. PING).

UDP runs over IP and is used primarily for broadcasting messages over a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Question 3

Question Type: MultipleChoice

Address Resolution Protocol (ARP) interrogates the network by sending out a?

Options:

A- broadcast.

B- multicast.

C- unicast.

D- semicast.

Answer:

A

Explanation:

ARP interrogates the network by sending out a broadcast seeking a network node that has a specific IP address, and asks it to reply with its hardware address. A broadcast message is sent to everyone whether or not the message was requested. A traditional unicast is a 'one-to-one' or 'narrowcast' message. A multicast is a 'one-to-many' message that is traditionally only sent to those machine that requested the information. Semicast is an imposter answer.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Question 4

Question Type: **MultipleChoice**

Which of the following is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address?

Options:

A- Address Resolution Protocol (ARP).

B- Reverse Address Resolution Protocol (RARP).

C- Internet Control Message protocol (ICMP).

D- User Datagram Protocol (UDP).

Answer:

A

Explanation:

ARP is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address.

The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's link layer or hardware address when only its Internet Layer (IP) or Network Layer address is known

Reverse Address Resolution Protocol (RARP) is used to find the IP address that matches an Ethernet address.

ICMP is a management protocol and messaging service provider for IP (e.g. PING).

UDP runs over IP. It is a best effort protocol that offers no reliability. UDS is used for application such as streaming media, voice over IP, the DNS protocol, as well as the Simple Network Management Protocol (SNMP).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

also see:

http://en.wikipedia.org/wiki/Address_resolution_protocol

Question 5

Question Type: MultipleChoice

How long are IPv4 addresses?

Options:

A- 32 bits long.

B- 64 bits long.

C- 128 bits long.

D- 16 bits long.

Answer:

A

Explanation:

IPv4 addresses are currently 32 bits long. IPv6 addresses are 128 bits long.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Question 6

Question Type: MultipleChoice

Each data packet is assigned the IP address of the sender and the IP address of the:

Options:

A- recipient.

B- host.

C- node.

D- network.

Answer:

A

Explanation:

Each data packet is assigned the IP address of the sender and the IP address of the recipient. The term network refers to the part of the IP address that identifies each network. The terms host and node refer to the parts of the IP address that identify a specific machine on a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Question 7

Question Type: MultipleChoice

All hosts on an IP network have a logical ID called a(n):

Options:

A- IP address.

B- MAC address.

C- TCP address.

D- Datagram address.

Answer:

A

Explanation:

All hosts on a network have a logical ID that is called an IP address. An IP address is a numeric identifier that is assigned to each machine on an IP network. It designates the location of a device on a network. A MAC address is typically called a hardware address because it is 'burned' into the NIC card. TCP address and Datagram address are imposter answers.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Question 8

Question Type: MultipleChoice

Which of the following statements pertaining to packet switching is incorrect?

Options:

A- Most data sent today uses digital signals over network employing packet switching.

B- Messages are divided into packets.

C- All packets from a message travel through the same route.

D- Each network node or point examines each packet for routing.

Answer:

C

Explanation:

When using packet switching, messages are broken down into packets. Source and destination address are added to each packet so that when passing through a network node, they can be examined and eventually rerouted through different paths as conditions change. All message packets may travel different paths and not arrive in the same order as sent. Packets need to be collected and reassembled into the original message at destination.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Question 9

Question Type: MultipleChoice

What is the main characteristic of a bastion host?

Options:

A- It is located on the internal network.

B- It is a hardened computer implementation

C- It is a firewall.

D- It does packet filtering.

Answer:

B

Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attack. The computer hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of the firewall or in the DMZ and usually involves access from untrusted networks or computers.

References:

http://en.wikipedia.org/wiki/Bastion_host

Question 10

Question Type: **MultipleChoice**

What is the main characteristic of a multi-homed host?

Options:

A- It is placed between two routers or firewalls.

B- It allows IP routing.

C- It has multiple network interfaces, each connected to separate networks.

D- It operates at multiple layers.

Answer:

C

Explanation:

The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.

Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

Question 11

Question Type: MultipleChoice

What works as an E-mail message transfer agent?

Options:

A- SMTP

B- SNMP

C- S-RPC

D- S/MIME

Answer:

A

Explanation:

SMTP (Simple Mail Transfer Protocol) works as a message transfer agent.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 821.

Question 12

Question Type: **MultipleChoice**

In this type of attack, the intruder re-routes data traffic from a network device to a personal machine. This diversion allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization. Pick the best choice below.

Options:

A- Network Address Translation

B- Network Address Hijacking

C- Network Address Supernetting

D- Network Address Sniffing

Answer:

B

Explanation:

Network address hijacking allows an attacker to reroute data traffic from a network device to a personal computer.

Also referred to as session hijacking, network address hijacking enables an attacker to capture and analyze the data addressed to a target system. This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization.

Session hijacking involves assuming control of an existing connection after the user has successfully created an authenticated session. Session hijacking is the act of unauthorized insertion of packets into a data stream. It is normally based on sequence number attacks, where sequence numbers are either guessed or intercepted.

The following are incorrect answers:

Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. See RFC 1918 for more details.

Network Address Supernetting There is no such thing as Network Address Supernetting. However, a supernetwork, or supernet, is an Internet Protocol (IP) network that is formed from the combination of two or more networks (or subnets) with a common Classless Inter-Domain Routing (CIDR) prefix. The new routing prefix for the combined network aggregates the prefixes of the constituent networks.

Network Address Sniffing This is another bogus choice that sound good but does not even exist. However, sniffing is a common attack to capture cleartext password and information unencrypted over the network. Sniffier is accomplished using a sniffer also called a Protocol Analyzer. A network sniffers monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called 'network probes' or 'snoops,' sniffers examine network traffic, making a copy of the data but without redirecting or altering it.

The following reference(s) were used for this question:

Hernandez CISSP

, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 8641-8642). Auerbach Publications. Kindle Edition.

http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm

http://wiki.answers.com/Q/What_is_network_address_hijacking

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 239.