Free Questions for SSCP

Shared by Lara on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 2

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 3

Question Type: MultipleChoice

What is the greatest danger from DHCP?

Options:

A- An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
B- Having multiple clients on the same LAN having the same IP address.
C- Having the wrong router used as the default gateway.
D- Having the organization's mail server unreachable.

Answer:

A

Explanation:

The greatest danger from BootP or DHCP (Dynamic Host Control Protocol) is from an intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients. Other choices are possible consequences of DHCP impersonation.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

Question 4

Question Type: MultipleChoice

Which of the following protects Kerberos against replay attacks?

Options:

A- Tokens
B- Passwords
C- Cryptography
D- Time stamps

Answer:

D

Explanation:

A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 581).

Question 5

Question Type: MultipleChoice

Another name for a VPN is a:

Options:

A- tunnel
B- one-time password
C- pipeline
D- bypass

Answer:

A

Explanation:

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

Question 6

Question Type: MultipleChoice

Which of the following offers security to wireless communications?

Options:

A- S-WAP
B- WTLS
C- WSP
D- WDP

Answer:

B

Explanation:

Wireless Transport Layer Security (WTLS) is a communication protocol that allows wireless devices to send and receive encrypted information over the Internet. S-WAP is not defined. WSP (Wireless Session Protocol) and WDP (Wireless Datagram Protocol) are part of Wireless Access Protocol (WAP).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

Question 7

Question Type: MultipleChoice

Which of the following statements pertaining to firewalls is incorrect?

Options:

A- Firewalls create bottlenecks between the internal and external network.
B- Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
C- Firewalls protect a network at all layers of the OSI models.
D- Firewalls are used to create security checkpoints at the boundaries of private networks.

Answer:

C

Explanation:

Firewalls can protect a network at multiple layers of the OSI models, however most of the firewalls do not have the ability to monitor the payload of the packets and see if an application level attack is taking place.

Today there are a new breed of firewall called Unified Threat Managers or UTM. They are a collection of products on a single computer and not necessarily a typical firewall. A UTM can address all of the layers but typically a firewall cannot.

Firewalls are security checkpoints at the boundaries of internal networks through which every packet must pass and be inspected, hence they create bottlenecks between the internal and external networks. But since external connections are relatively slow compared to modern computers, the latency caused by this bottleneck can almost be transparent.

By implementing the concept of border security, they centralize security services in machines optimized and dedicated to the task, thus relieving the other hosts on the network from that function.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

Question 8

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 9

Question Type: MultipleChoice

Which of the following is an extension to Network Address Translation that permits multiple devices providing services on a local area network (LAN) to be mapped to a single public IP address?

Options:

A- IP Spoofing
B- IP subnetting
C- Port address translation
D- IP Distribution

Answer:

C

Explanation:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses or to publish multiple hosts with service to the internet while having only one single IP assigned on the external side of your gateway.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

Port Address Translation is also called porting, port overloading, port-level multiplexed NAT and single address NAT.

Shon Harris has the following example in her book:

The company owns and uses only one public IP address for all systems that need to communicate outside the internal network. How in the world could all computers use the exact same IP address? Good question. Here's an example: The NAT device has an IP address of 127.50.41.3. When computer A needs to communicate with a system on the Internet, the NAT device documents this computer's private address and source port number (10.10.44.3; port 43,887). The NAT device changes the IP address in the computer's packet header to 127.50.41.3, with the source port 40,000. When computer B also needs to communicate with a system on the Internet, the NAT device documents the private address and source port number (10.10.44.15; port 23,398) and changes the header information to 127.50.41.3 with source port 40,001. So when a system responds to computer A, the packet first goes to the NAT device, which looks up the port number 40,000 and sees that it maps to computer A's real information. So the NAT device changes the header information to address 10.10.44.3 and port 43,887 and sends it to computer A for processing. A company can save a lot more money by using PAT, because the company needs to buy only a few public IP addresses, which are used by all systems in the network.

As mentioned on Wikipedia:

NAT is also known as Port Address Translation: is a feature of a network device that translate TCP or UDP communications made between host on a private network and host on a public network. I allows a single public IP address to be used by many host on private network which is usually a local area network LAN

NAT effectively hides all TCP/IP-level information about internal hosts from the Internet.

The following were all incorrect answer:

IP Spoofing - In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

Subnetting - Subnetting is a network design strategy that segregates a larger network into smaller components. While connected through the larger network, each subnetwork or subnet functions with a unique IP address. All systems that are assigned to a particular subnet will share values that are common for both the subnet and for the network as a whole.

A different approach to network construction can be thought of as subnetting in reverse. Known as CIDR, or Classless Inter-Domain Routing, this approach also creates a series of subnetworks. Rather than dividing an existing network into small components, CIDR takes smaller components and connects them into a larger network. This can often be the case when a business is acquired by a larger corporation. Instead of doing away with the network developed and used by the newly acquired business, the corporation chooses to continue operating that network as a subsidiary or an added component of the corporation's network. In effect, the system of the purchased entity becomes a subnet of the parent company's network.

IP Distribution - This is a generic term which could mean distribution of content over an IP network or distribution of IP addresses within a Company. Sometimes people will refer to this as Internet Protocol address management (IPAM) is a means of planning, tracking, and managing the Internet Protocol address space used in a network. Most commonly, tools such as DNS and DHCP are used in conjunction as integral functions of the IP address management function, and true IPAM glues these point services together so that each is aware of changes in the other (for instance DNS knowing of the IP address taken by a client via DHCP, and updating itself accordingly). Additional functionality, such as controlling reservations in DHCP as well as other data aggregation and reporting capability, is also common. IPAM tools are increasingly important as new IPv6 networks are deployed with larger address pools, different subnetting techniques, and more complex 128-bit hexadecimal numbers which are not as easily human-readable as IPv4 addresses.

Reference(s) used for this question:

STREBE,

Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Telecommunications and Network Security, Page 350.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 12765-12774). Telecommunications and Network Security, Page 604-606

http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT

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

http://www.wisegeek.com/what-is-subnetting.htm

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

Question 10

Question Type: MultipleChoice

What is malware that can spread itself over open network connections?

Options:

A- Worm
B- Rootkit
C- Adware
D- Logic Bomb

Answer:

A

Explanation:

Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

A notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25, 2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network.

A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised.

Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll.

Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.

The following answers are incorrect:

- Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkit isn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of 'root' (the traditional name of the privileged account on Unix operating systems) and the word 'kit' (which refers to the software components that implement the tool). The term 'rootkit' has negative connotations through its association with malware.

- Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.

- Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer.

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

The CCCure

CompTIA Holistic Security+ Tutorial and CBT

and

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

and

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

and

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

Question 11

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.