Free Questions for SSCP by vceexamstest

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

Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?

Options:

A- Stealth viruses

B- Polymorphic viruses

C- Trojan horses

D- Logic bombs

Answer:

B

Explanation:

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants, making it harder to detect by anti-virus software. The particularity of a stealth virus is that it tries to hide its presence after infecting a system. A Trojan horse is a set of

unauthorized instructions that are added to or replacing a legitimate program. A logic bomb is a set of instructions that is initiated when a specific event occurs.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 786).

Question 2

Question Type: MultipleChoice

Which of the following virus types changes some of its characteristics as it spreads?

Options:

A- Boot Sector

B- Parasitic

C- Stealth

D- Polymorphic

Answer:

D

Explanation:

A Polymorphic virus produces varied but operational copies of itself in hopes of evading anti-virus software.

The following answers are incorrect:

boot sector. Is incorrect because it is not the best answer. A boot sector virus attacks the boot sector of a drive. It describes the type of attack of the virus and not the characteristics of its composition.

parasitic. Is incorrect because it is not the best answer. A parasitic virus attaches itself to other files but does not change its characteristics.

stealth. Is incorrect because it is not the best answer. A stealth virus attempts to hide changes of the affected files but not itself.

Question 3

Question Type: MultipleChoice

In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.

Options:

A- virus

B- worm

C- Trojan horse.

D- trapdoor

Answer:

C

Explanation:

A trojan horse is any code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it. A Trojan often also includes a trapdoor as a means to gain access to a computer system bypassing security controls.

Wikipedia defines it as:

A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

The following answers are incorrect:

virus. Is incorrect because a Virus is a malicious program and is does not appear to be harmless, it's sole purpose is malicious intent often doing damage to a system. A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be 'infected'.

worm. Is incorrect because a Worm is similiar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self-propagate and devour the resources of a system. 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.

trapdoor. Is incorrect because a trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.

References:

http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

and

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

and

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

and

http://en.wikipedia.org/wiki/Backdoor_%28computing%29

Question 4

Question Type: **MultipleChoice**

Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

Options:

A- DNS

B- FTP

C- SSH

D- SMTP

Answer:

A

Explanation:

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point - Internet service providers access internet using net access point.A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-

profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client

may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:

SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp.

SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

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

CISA review

manual 2014 page number 273 and 274

Question 5

Question Type: MultipleChoice

While using IPsec, the ESP and AH protocols both provides integrity services. However when using AH, some special attention needs to be paid if one of the peers uses NAT for address translation service. Which of the items below would affects the use of AH and its Integrity Check Value (ICV) the most?

Options:

A- Key session exchange

B- Packet Header Source or Destination address

C- VPN cryptographic key size

D- Crypotographic algorithm used

Answer:

B

Explanation:

It may seem odd to have two different protocols that provide overlapping functionality.

AH provides authentication and integrity, and ESP can provide those two functions and confidentiality.

Why even bother with AH then?

In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.

The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with

the packet, which means the packet will be discarded automatically.

The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.

Here is a tutorial on IPSEC from the Shon Harris Blog:

The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. It can be more flexible and less expensive than end-to end and link encryption methods.

IPSec has strong encryption and authentication methods, and although it can be used to enable tunneled communication between two computers, it is usually employed to establish virtual private networks (VPNs) among networks across the Internet.

IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to use. Rather, it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology. IPSec uses two basic security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity.

IPSec can work in one of two modes: transport mode, in which the payload of the message is protected, and tunnel mode, in which the payload and the routing and header information are protected. ESP in transport mode encrypts the actual message information so it cannot be sniffed and uncovered by an unauthorized entity. Tunnel mode provides a higher level of protection by also protecting the header and trailer data an attacker may find useful. Figure 8-26 shows the high-level view of the steps of setting up an IPSec connection.

Each device will have at least one security association (SA) for each VPN it uses. The SA, which is critical to the IPSec architecture, is a record of the configurations the device needs to support an IPSec connection. When two devices complete their handshaking process, which means they have agreed upon a long list of parameters they will use to communicate, these data must be recorded and stored somewhere, which is in the SA.

The SA can contain the authentication and encryption keys, the agreed-upon algorithms, the key lifetime, and the source IP address. When a device receives a packet via the IPSec protocol, it is the SA that tells the device what to do with the packet. So if device B receives a packet from device C via IPSec, device B will look to the corresponding SA to tell it how to decrypt the packet, how to properly authenticate the source of the packet, which key to use, and how to reply to the message if necessary.

SAs are directional, so a device will have one SA for outbound traffic and a different SA for inbound traffic for each individual communication channel. If a device is connecting to three devices, it will have at least six SAs, one for each inbound and outbound connection per remote device. So how can a device keep all of these SAs organized and ensure that the right SA is invoked for the right connection? With the mighty secu rity parameter index (SPI), that's how. Each device has an SPI that keeps track of the different SAs and tells the device which one is appropriate to invoke for the different packets it receives. The SPI value is in the header of an IPSec packet, and the device reads this value to tell it which SA to consult.

IPSec can authenticate the sending devices of the packet by using MAC (covered in the earlier section, "The One-Way Hash"). The ESP protocol can provide authentication, integrity, and confidentiality if the devices are configured for this type of functionality.

So if a company just needs to make sure it knows the source of the sender and must be assured of the integrity of the packets, it would choose to use AH. If the company would like to use these services and also have confidentiality, it would use the ESP protocol because it provides encryption functionality. In most cases, the reason ESP is employed is because the company must set up a secure VPN connection.

It may seem odd to have two different protocols that provide overlapping functionality. AH provides authentication and integrity, and ESP can provide those two functions and confidentiality. Why even bother with AH then? In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.

The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically.

The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.

Because IPSec is a framework, it does not dictate which hashing and encryption algorithms are to be used or how keys are to be exchanged between devices. Key management can be handled manually or automated by a key management protocol. The de facto standard for IPSec is to use Internet Key Exchange (IKE), which is a combination of the ISAKMP and OAKLEY protocols. The Internet Security Association and Key Management Protocol (ISAKMP) is a key exchange architecture that is independent of the type of keying mechanisms used. Basically, ISAKMP provides the framework of what can be negotiated to set up an IPSec connection (algorithms, protocols, modes, keys). The OAKLEY protocol is the one that carries out the negotiation process. You can think of ISAKMP as providing the playing field (the infrastructure) and OAKLEY as the guy running up and down the playing field (carrying out the steps of the negotiation).

IPSec is very complex with all of its components and possible configurations. This complexity is what provides for a great degree of flexibility, because a company has many different configuration choices to achieve just the right level of protection. If this is all new to you and still confusing, please review one or more of the following references to help fill in the gray areas.

The following answers are incorrect:

The other options are distractors.

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

Shon Harris

, CISSP All-in-One Exam Guide- fiveth edition, page 759

and

https://neodean.wordpress.com/tag/security-protocol/

Question 6

Question Type: **MultipleChoice**

At which layer of ISO/OSI does the fiber optics work?

Options:

A- Network layer

B- Transport layer

C- Data link layer

D- Physical layer

Answer:

D

Explanation:

The Answer: Physical layer The Physical layer is responsible for the transmission of the data

All of the other answers are incorrect.

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

Shon Harris

all in one - Chapter 7 (Cabling)

Question 7

Question Type: MultipleChoice

Which of the following media is MOST resistant to EMI interference?

Options:

A- microwave

B- fiber optic

C- twisted pair

D- coaxial cable

Answer:

B

Explanation:

A fiber optic cable is a physical medium that is capable of conducting modulated light trasmission. Fiber optic cable carries signals as light waves, thus creating higher trasmission speeds and greater distances due to less attenuation. This type of cabling is more difficult to tap than other cabling and is most resistant to interference, especially EMI.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 103).

Question 8

Question Type: MultipleChoice

What is a packet sniffer?

Options:

A- It tracks network connections to off-site locations.

B- It monitors network traffic for illegal packets.

C- It scans network segments for cabling faults.

D- It captures network traffic for later analysis.

Answer:

D

Explanation:

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

Question 9

Question Type: MultipleChoice

Which one of the following is used to provide authentication and confidentiality for e-mail messages?

Options:

A- Digital signature

B- PGP

C- IPSEC AH

D- MD4

Answer:

B

Explanation:

Instead of using a Certificate Authority, PGP uses a 'Web of Trust', where users can certify each other in a mesh model, which is best applied to smaller groups.

In cryptography, a web of trust is a concept used in PGP, GnuPG, and other OpenPGP compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0.

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.

As per Shon Harris's book:

Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program. PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions. PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP initially used its own type of digital certificates rather than what is used in PKI, but they both have similar purposes. Today PGP support X.509 V3 digital certificates.

Reference(s) used for this question:

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 169).

Shon Harris, CISSP All in One book

https://en.wikipedia.org/wiki/Pretty_Good_Privacy

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

Question 10

Question Type: MultipleChoice

Why is traffic across a packet switched network difficult to monitor?

Options:

A- Packets are link encrypted by the carrier

B- Government regulations forbids monitoring

C- Packets can take multiple paths when transmitted

D- The network factor is too high

Answer:

C

Explanation:

With a packet switched network, packets are difficult to monitor because they can be transmitted using different paths.

A packet-switched network is a digital communications network that groups all transmitted data, irrespective of content, type, or structure into suitably sized blocks, called packets. The network over which packets are transmitted is a shared network which routes each packet independently from all others and allocates transmission resources as needed.

The principal goals of packet switching are to optimize utilization of available link capacity, minimize response times and increase the robustness of communication. When traversing network adapters, switches and other network nodes, packets are buffered and queued, resulting in variable delay and throughput, depending on the traffic load in the network.

Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.

All of the other answer are wrong

Reference(s) used for this question:

TIPTON,

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

and

https://en.wikipedia.org/wiki/Packet-switched_network

and

http://www.webopedia.com/TERM/P/packet_switching.html

Question 11

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.