Network Security Questions

Latest Network Security MCQ Objective Questions

Question 1:

View this Question Online >

Symmetric Key Cryptography uses stream cipher to encrypt the information. One of example of stream cipher:

1. SHA
2. RC4
3. MD5
4. Blowfish
5. None of the above

Answer (Detailed Solution Below)

Option 2 : RC4

Network Security Question 1 Detailed Solution

The correct answer is **option 2.**

Concept:

Symmetric Key Cryptography uses a stream cipher to encrypt the information. One example of stream cipher is RC4.

Stream cipher:

A stream cipher is an encryption technique that encrypts and decrypts a set quantity of data using a symmetric key. In contrast to an asymmetric cipher key, a symmetric cipher key is an encryption tool that may be used for both encryption and decryption.

Rivest Cipher 4:

- Rivest Cipher 4, often known as RC4, is a **stream cipher** that was developed in 1987. A stream cipher is a sort of encryption algorithm that encrypts data one byte at a time.
- RC4 is a stream cipher that has been used in the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols, the IEEE 802.11 wireless LAN standard, and the Wi-Fi Security Protocol WEP (Wireless Equivalent Protocol).

Hence the correct answer is RC4.

Additional Information

- **Secure hashing algorithm** (SHA) is an acronym for secure hashing algorithm. SHA is a hashing algorithm that is based on MD5. It is used to hash data and certificates. Using bitwise operations, modular additions, and compression functions, a hashing algorithm compresses the input data into a smaller form that cannot be comprehended.
- **Blowfish** is the first symmetric encryption algorithm created by Bruce Schneier in 1993. Symmetric encryption uses a single encryption key to both encrypt and decrypt data.

Question 2:

View this Question Online >

Keyloggers are a form of _____.

1. Social Engineering
2. Trojan
3. Shoulder Surfing
4. Spyware
5. None of the above

Answer (Detailed Solution Below)

Option 4 : Spyware

Network Security Question 2 Detailed Solution

The correct answer is **option 4.**
Concept:

Keyloggers, also known as keystroke loggers, are software applications or hardware devices that record the activity (keys tapped) on a keyboard. Keyloggers are a type of **spyware** in which users are unaware that their actions are being recorded.

Spyware:

Spyware is a type of malicious software or malware that is installed on a computing device without the end user's knowledge.

Characteristics:

- Keyloggers may be used for a number of objectives, including fraudulently gaining access to your private information and monitoring staff actions. Some keyloggers may also record your screen at random intervals; these are known as screen recorders.
- Keylogger software normally saves your keystrokes in a tiny file that may be viewed later or automatically sent to the person watching your activity.
- A keylogger is a malicious computer application that records everything you write on the keyboard and learns the keystroke pattern, including words, characters, and symbols, and then sends all of the recorded information to hostile hackers.

Hence the correct answer is Spyware.

Question 3:

View this Question Online >

Digital signature cannot provide _____ for the message-

1. Authentication
2. Nonrepudiation
3. Confidentiality
4. Integrity
5. None of the above

Answer (Detailed Solution Below)

Option 3 : Confidentiality

Network Security Question 3 Detailed Solution

The correct answer is **Confidentiality**

Key Points

Confidentiality:

- A **digital signature** does not inherently provide confidentiality. This means that if someone intercepts the message, they can read its content.
- Confidentiality must be ensured by other means, such as encryption. Encryption scrambles the content of a message so that it can be understood only by someone who has the corresponding decryption key.
- This keep the contents hidden from anyone who might intercept the message during transmission.
- In other words, digital signature alone cannot prevent unwanted third parties from reading the message if it is intercepted; it only ensures that the receiver will know if the message was tampered with during transmission.

Additional Information

A digital signature provides three functions:

- **Authentication**: It verifies the sender's identity. The receiver can be sure that the message was indeed sent by the claimed sender, as it's based on the sender's private key, which is not publicly accessible.
- **Non-Repudiation**: It ensures that the sender cannot deny having sent the message. Once signed with a digital signature, a message can always be proven to have been signed by that unique private key.
- **Integrity**: It verifies that the message content has not been altered in transit. Any modification to the message would alter the signature and, therefore, be detected at the receiving end.

Question 4:

View this Question Online >

Digital signature cannot provide _____ for the message-

1. Authentication
2. Nonrepudiation
3. Confidentiality

4. More than one of the above

5. None of the above

Answer (Detailed Solution Below)

Option 3 : Confidentiality

Network Security Question 4 Detailed Solution

The correct answer is **Confidentiality**

Key Points

Confidentiality:

- A **digital signature** does not inherently provide confidentiality. This means that if someone intercepts the message, they can read its content.
- Confidentiality must be ensured by other means, such as encryption. Encryption scrambles the content of a message so that it can be understood only by someone who has the corresponding decryption key.
- This keep the contents hidden from anyone who might intercept the message during transmission.
- In other words, digital signature alone cannot prevent unwanted third parties from reading the message if it is intercepted; it only ensures that the receiver will know if the message was tampered with during transmission.

Additional Information

A digital signature provides three functions:

- **Authentication**: It verifies the sender's identity. The receiver can be sure that the message was indeed sent by the claimed sender, as it's based on the sender's private key, which is not publicly accessible.
- **Non-Repudiation**: It ensures that the sender cannot deny having sent the message. Once signed with a digital signature, a message can always be proven to have been signed by that unique private key.
- **Integrity**: It verifies that the message content has not been altered in transit. Any modification to the message would alter the signature and, therefore, be detected at the receiving end.

Question 5:

View this Question Online >

Which of the following is/are the virus attacks?

1. Citrix breach.
2. WannaCry.
3. NotPetya.
4. More than one of the above
5. None of the above

Answer (Detailed Solution Below)

Option 4 : More than one of the above

Network Security Question 5 Detailed Solution

The correct option is 4 i.e., **More than one of the above**

- **Citrix** was hit by hackers that potentially exposed large amounts of customer data.
- The WannaCry ransomware attack was made in May 2017 worldwide.
- **The WannaCry** ransomware affected over 200,000 victims and more than 300,000 computers infected.
- **Petya** is a family of encrypting malware that was first discovered in 2016.
- **Bad Rabbit** similar pattern to WannaCry and Petya.
- Bad Rabbit affected Russia most.

Top Network Security MCQ Objective Questions

Question 6 View this Question Online >

In computing, _____ is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

1. Spyware
2. Cookie
3. Spam
4. Firewall

Answer (Detailed Solution Below)

Option 4 : Firewall

Network Security Question 6 Detailed Solution

The correct answer is **option 4) i.e. Firewall.**

- A firewall is a type of **computer-security system**.
- A firewall controls the flow of data from one computer or network to another and they are mainly intended to protect an individual computer system or a network from being accessed by an intruder, especially via the Internet.

Note:

- **Cookies** are small files that are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website and can be accessed either by the web server or the client computer.
- **Spam** is an **undesired or illegal email** message.
- **Spyware** is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.

Question 7

View this Question Online >

A computer virus is a

1. Hardware
2. Software
3. Bacteria
4. Freeware

Answer (Detailed Solution Below)

Option 2 : Software

Network Security Question 7 Detailed Solution

The correct answer is Software.

- A computer virus is a malicious software that, when executed replicates itself by modifying other computer programs.
- The full form of VIRUS is Vital Information Resources Under Seize because they replicate and multiply and use up computer memory processing power with fake repetitive commands. It causes the system to become slow and keeps hanging.

Question 8

View this Question Online >

Which type of virus attaches with EXE files and the resulting infected EXE file attacks other EXE files and infects them ?

1. Parasitic virus
2. Boot Sector Virus
3. Stealth Virus
4. Memory Resident Virus

Answer (Detailed Solution Below)

Option 1 : Parasitic virus

Network Security Question 8 Detailed Solution

The type of virus that attaches to EXE files and infects other EXE files is a type of **Parasitic virus**, also known as an executable virus or file infecting virus.

Boot sector viruses infect the boot sector of storage devices such as hard drives and floppy disks.

Stealth viruses use various techniques to hide themselves from detection by antivirus software and other system tools.

Memory resident viruses, as the name suggests, reside in a computer's memory and can infect other files that are loaded into memory. However, they do not typically infect EXE files specifically.

Hence, the correct answer is **option 1**.

Question 9

View this Question Online >

What is the term for a cyber-security attack that targets multiple interconnected devices simultaneously to create a large- scale attack network?

1. DDoS attack
2. Botnet attack
3. Zero-day attack
4. Spear phishing attack

Answer (Detailed Solution Below)

Option 2 : Botnet attack

Network Security Question 9 Detailed Solution

The correct answer is **Botnet attack.**

Key Points

- **Botnet** is a network of computers that have been infected with malware and are controlled by a single attacker. The attacker can use the botnet to launch a variety of attacks, including DDoS attacks.
- **DDoS attack** is a cyber-security attack that targets a website or server with a flood of traffic. This traffic can overwhelm the website or server, making it unavailable to legitimate users.
- **Zero-day attack** is an attack that exploits a vulnerability in software that the software vendor is not aware of. This means that there is no patch available to fix the vulnerability, making it very difficult to defend against.
- A spear phishing attack is a targeted attack that is designed to trick the victim into clicking on a malicious link or opening an infected attachment.

- Therefore, the term for a cyber-security attack that targets multiple interconnected devices simultaneously to create a large-scale attack network is botnet attack.

Additional Information

Here are some ways to protect yourself from botnet attacks:

- Keep your software up to date. Software vendors often release patches to fix security vulnerabilities.
- Use a firewall. A firewall can help to block malicious traffic from reaching your computer.
- Use antivirus software. Antivirus software can help to detect and remove malware from your computer.
- Be careful about what websites you visit and what links you click on.
- Do not open attachments from unknown senders.

Question 10 View this Question Online >

Which of the following is an attack in which the user receives the unwanted amount of e-mails?

1. Email bomb
2. Ping storm
3. Spoofing
4. Smurfing

Answer (Detailed Solution Below)

Option 1 : Email bomb

Network Security Question 10 Detailed Solution

Important Points

Email bomb

It is an **attack on your inbox that involves sending massive amounts of emails** to your address. Sometimes these messages are complete gibberish, but more often they'll be confirmation emails for newsletters and subscriptions.

Additional Information

Spoofing

It is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Smurf Attack

It is a form of a DDoS attack that causes packet flood on the victim by exploiting/abusing ICMP protocol. When deployed, large packets are created using a technique called "spoofing". The phony source address that is now attached to these packets becomes the victim, as their IP is flooded with traffic. The small ICMP packet generated by the tool causes big trouble for a victim, hence the name Smurf.

Ping storm

It is a condition in which the Internet ping program is used to send a flood of packets to a server to test its ability to handle a high amount of traffic or, maliciously, to make the server inoperable

Hence Option 1 is correct

Question 11 View this Question Online >

Which of the following is a malicious software that, on execution, runs its own code and modifies other computer programs?

1. Virus
2. Spam

3. Spyware

4. Adware

5. None of the above

Answer (Detailed Solution Below)

Option 1 : Virus

Network Security Question 11 Detailed Solution

Virus

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code

Important Point:

- Spam is any kind of unwanted, unsolicited digital communication, often an email, that gets sent out in bulk. Spam is a huge waste of time and resources.
- Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is classified as a type of malware.
- Adware, or advertising supported software, is software that displays unwanted advertisements on user computer

Question 12 View this Question Online >

Knowing the password of a user for hacking is called?

1. Sneaking

2. Spoofing

3. Cyber stalking

4. Spamming

Answer (Detailed Solution Below)

Option 2 : Spoofing

Network Security Question 12 Detailed Solution

The correct answer is **Spoofing.**

Key Points

- **Spoofing** occurs in cybersecurity when fraudsters pretend to be someone or something else in order to gain someone's trust. Typically, the goal is to gain access to systems, steal data, steal money, or spread malware.

Additional Information

- **Cyber Stalking-**
  - The repeated use of electronic communications to harass or frighten someone is known as cyber stalking. For example by sending threatening emails.
- **Sneaking-**
  - Sneak means done without warning in an unknown, secret or quiet manner.
- **Spamming-**
  - Spamming is the practic of sending unsolicited bulk messages via electronic messaging systems such as e-mail and other digital delivery systems and broadcast media.

Question 13 View this Question Online >

Unsolicited electronic messages sent for marketing purposes are called_____.

1. virus
2. unzip
3. spam
4. URL

Answer (Detailed Solution Below)

Option 3 : spam

Network Security Question 13 Detailed Solution

The correct answer is **spam.**

Key Points

- Any **unwanted, uninvited digital communication** transmitted in bulk is referred to as **spam.**
- Spam is **frequently transmitted** by **email.**
- But it can also be sent through **social media, text messages, and phone calls.**
- **Cybercriminals** send **phishing emails** to a large number of recipients in an effort to "**hook**" a select few recipients.
- **Phishing emails** con people into **disclosing private data** like credit card numbers or website logins.

Additional Information

- **Virus:**
  - A **computer virus** is a form of **malware** that accompanies another program and has the **ability to multiply** and **propagate** once it has been run on a machine.
- **Unzip:**
  - **Extraction** of the files from a **single-file zip archive** or other comparable file archive is known as **unzipping.**
- **URL**:
  - URL stands for **Uniform Resource Locator.**
  - A URL is nothing more than the **Web address of a specific, particular resource.**

Question 14 View this Question Online >

Dynamic packet filters firewall are fourth generation firewalls that work at

1. Application layer
2. TCP
3. UDP
4. TCP, UDP
5. Session Layer

Answer (Detailed Solution Below)

Option 4 : TCP, UDP

Network Security Question 14 Detailed Solution

Fourth Generation Firewalls are also known as stateful firewalls. The most important upgrade from First Generation Firewalls is the ability to keep track of the TCP connection state. Greatly prevents hackers access, also these firewalls are able to determine if packets are a part of a new connection or existing connection, relying on a three-way handshake with TCP.

Additional Information

TCP (Transmission Control Protocol):

- TCP (Transmission control protocol) **is a connection-oriented reliable transport protocol.** It provides a process to process communications using port numbers.

UDP (User datagram protocol):

- UDP (User datagram protocol) is called a **connectionless, unreliable transport protocol.**
- UDP protocol encapsulates and decapsulates messages in an IP datagram.

Application Layer Protocol:-

- In the Internet protocol stack, when data is sent from device A to device B, the 5th layer to receive data at B is the Application layer.
- It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services.

Session Layer Protocol:-

- The Session Layer is the 5th layer of the OSI model.
- The session layer controls the dialogues (connections) between computers. It establishes, manages, and terminates the connections between the local and remote applications.

Question 15 View this Question Online >

Which of the following statement is/are FALSE?

(i) A firewall acts as a packet filter inspecting all the packets entering the local network.

(ii) Digital signatures do not provide nonrepudiation.

(iii) Asymmetric cryptography uses both public and private keys.

1. Only (ii) and (iii)
2. Only (ii)
3. Only (i) and (iii)
4. Only (iii)

Answer (Detailed Solution Below)

Option 2 : Only (ii)

Network Security Question 15 Detailed Solution

The correct answer is **option 2.**

Concept:

Option 1: A firewall acts as a packet filter inspecting all the packets entering the local network.

True, A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up. If the packet passes the test, it's allowed to pass to the local network. If the packet doesn't pass, it's rejected. Packet filters are the least expensive type of firewall.

Option 2: Digital signatures do not provide nonrepudiation.

False, Digital signatures (combined with other measures) can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or send the message in the first place.

Option 3: Asymmetric cryptography uses both public and private keys.

True, Asymmetric Encryption uses two distinct, yet related keys. One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption. As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message.

Hence the correct answer is *Only (ii).*