Network Security Questions

Latest Network Security MCQ Objective Questions

Question 1:

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)
5. None of the above

Answer (Detailed Solution Below)

Option 2 : Only (ii)

Network Security Question 1 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).*

Question 2:

View this Question Online >

Which of the following statements is true about modems?

1. Modems use the telephone lines
2. Modem stands for modulator and demodulator
3. Modem are no longer used in secure network
4. Both 1 and 2
5. None of the above/More than one of the above

Answer (Detailed Solution Below)

Option 4 : Both 1 and 2

Network Security Question 2 Detailed Solution

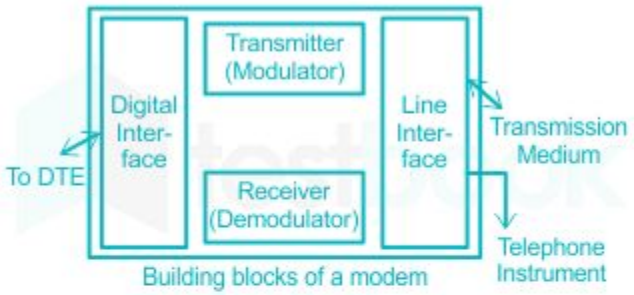
The correct answer is **Both 1 and 2.**

Key Points

- The modem is an abbreviation for **Modulator-Demodulator.**
- Modems are used for data transfer from one computer network to another computer network through telephone lines.
- The computer network works in digital mode, while analog technology is used for carrying messages across phone lines.
- The device which performs modulation is called a modulator and the device which recovers the information signal from the modulated carrier is called a demodulator.

- In data transmission, we usually come across devices that perform both modulations as well as demodulation functions, and these devices are called modems.
- When data is to be transmitted over long distances, modems are needed.

- In a modem, the input signal modulates a carrier which is transmitted to the distant end.
- At the distant end, another modem demodulators the received carrier to obtain the digital signal.



Building blocks of a modem

Question 3:

View this Question Online >

Which of the following is true about Phishing?

1. It is a type of cybersecurity attack that attempts to obtain data that are sensitive like Usernames, Passwords, and more.
2. It is typically carried out by email spoofing, instant messaging, and text messaging.

1. 1
2. 2
3. 1 and 2
4. Neither 1 nor 2
5. None of the above/More than one of the above

Answer (Detailed Solution Below)

Option 3 : 1 and 2

Network Security Question 3 Detailed Solution

The correct answer is **1 and 2**.

Key Points

- Phishing may be a **type of cybersecurity attack that attempts to obtain data that are sensitive like Username, Password, and more.**
- **It attacks the user through mail, text, or direct messages.**
- **It is typically carried out by email spoofing, instant messaging, and text messaging.**
- Phishing often directs users to enter personal information at a fake website that matches the look and feel of the legitimate site.
- **Phishing is an example of social engineering techniques used to deceive users.**
- This word is created as a homophone and a sensational spelling of fishing, influenced by phreaking.
- **Signs of phishing include:**
  - Incorrect URLs
  - No signature or contact information
  - Too good to be true offer
  - Style inconsistencies
  - **Spelling, punctuation, or grammar errors**
  - Attention-grabbing titles

Additional Information

- **Spam:**
  - Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk.
  - Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.
- **Hacking:**
  - The act of compromising digital devices and networks through unauthorized access to an account or computing system.
  - Hacking isn't always a malicious act, but it's most commonly associated with illegal activity and data theft by cybercriminals.
- **Cracking:**
  - Cracking is when someone performs a security hack for criminal or malicious reasons, and therefore the person is called a "cracker."
  - A bit like a bank robber cracks a safe by skillfully manipulating its lock, a cracker breaks into a computing system, program, or account with the help of their technical wizardry.

Question 4:

View this Question Online >

_____ hides the true network addresses and is used to intercept all messages entering and leaving the network.

1. Logic bomb
2. Firewall
3. Patches
4. Proxy server
5. None of the above/More than one of the above

Answer (Detailed Solution Below)

Option 4 : Proxy server

Network Security Question 4 Detailed Solution

The correct answer is **Proxy server.**

Key Points

- **A proxy server could also be a system or router that provides a gateway between users and the internet.**
- Therefore, it helps prevent cyber attackers from entering a private network.
- It's a server, mentioned as an "intermediary" because it goes between end-users and therefore the web pages they visit online.

Additional Information

- **Logic bomb:**
  - It is a malicious piece of code that's secretly inserted into a computer network, OS, or software application.
  - It lies dormant until a specific condition occurs.
  - When this condition is met, the logic bomb is triggered — devastating a system by corrupting data, deleting files, or clearing hard drives.

- **Firewall:**
  - A firewall could also be a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
  - Its purpose is to work out a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Patches:

- A patch could also be a software update comprised of code inserted (or patched) into the code of an executable program.
- Typically, a patch is installed into an existing software program.

Question 5:

View this Question Online >

Which virus spreads in application software?

1. Macro virus
2. Boot virus
3. File virus
4. Antivirus
5. None of the above/More than one of the above

Answer (Detailed Solution Below)

Option 1 : Macro virus

Network Security Question 5 Detailed Solution

The correct answer is **Macro virus.**

Key Points

- A macro virus could also be a computer virus written in the same macro language used to create software programs such as Microsoft Excel or Word.
- It centers on software applications and doesn't depend upon the operating system (OS).
- As a result, it can infect any computer running any kind of OS, including Windows, macOS, and Linux.

Important Points

- **Application Software:**
  - Application software may be a type of computer program that performs a specific personal, educational, and business function.
  - Each program is meant to assist the user with a particular process, which can be related to productivity, creativity, and/or communication.

Additional Information

- **Boot Virus:**
  - The Boot Virus is the name of a ransomware infection, whose main goal is to convince victims to pay ransom to get their files to work once again.
- **File virus:**
  - A file-infecting virus is one of the most common types of virus.
  - Typically, it infects files with .exe or .com extensions.
  - When the infected file is accessed or executed, it may be partially or completely overwritten by the virus.
- **Antivirus:**
  - Antivirus software is designed to detect, prevent, and remove malicious software, aka malware.
  - The classification of malware includes viruses, worms, trojans, and scareware, as well as (depending on the scanner) some forms of potentially unwanted programs (such as adware and spyware).

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 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 8 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 9 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 9 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 10 View this Question Online >

_____ uses pretty good privacy algorithm.

1. Electronic mails
2. File encryption
3. Both Electronic mails and File encryption
4. None of the options

Answer (Detailed Solution Below)

Option 3 : Both Electronic mails and File encryption

Network Security Question 10 Detailed Solution

Electronic mails and File encryption both uses pretty good privacy algorithm.

Key Points

Pretty Good Privacy(PGP)

- PGP is an encryption program that provides cryptographic privacy and authentication for data communication.
- PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Question 11 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 11 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 12 View this Question Online >

A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) **CANNOT**

1. block entire HTTP traffic during 9:00 PM and 5:00 AM
2. block all ICMP traffic
3. stop incoming traffic from a specific IP address but allow outgoing traffic to the same IP address
4. block TCP traffic from a specific user on a multi-user system during 9:00 PM and 5:00 AM

Answer (Detailed Solution Below)

Option 4 : block TCP traffic from a specific user on a multi-user system during 9:00 PM and 5:00 AM

Network Security Question 12 Detailed Solution

The correct answer is **option 4:**

Key Points

Since it is Layer-4 Firewall so it includes the layers → Physical Layer, Data Link Layer, Network Layer as well as Transport Layer

Allow → Transport Layer or those layers who comes below transport Layer

Not Allow → Application Layer

Option 1: Transport Layer specific

It is possible to block entire traffic by blocking all the traffic on port number 80. so, here don't need to check anything that it is application layer specific or not. we only need to block port number 80 for the required time interval.

Option 2: Network Layer specific

ICMP is a network layer protocol that comes below the transport layer

Option 3: Network Layer specific

IP addresses are used in the network layer, which below the transport layer.

Option 4: Application Layer specific

In this option given that it is a multi-user system, so many users use the same port for communication because of this we can't block any specific port number. if we block a specific port number, all the users also blocked who is using that port number for communication. while we want to block a specific user, so how to do this. We need **application layer-specific** information of the user like user_id type of things that can't be checked as it is a 4-layer firewall. so it is not possible to allow other users and block some specific at the same time using a 4-layer firewall.

Question 13 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 13 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 14

View this Question Online >

A digital signature is required:

1. for non-repudiation of communication by a sender
2. for all e-mail sending
3. for all DHCP server
4. for FTP transactions

Answer (Detailed Solution Below)

Option 1 : for non-repudiation of communication by a sender

Network Security Question 14 Detailed Solution

Digital Signature:

- A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
- A digital signature provides message integrity, message authentication but not confidentiality.
- **Non-repudiation** deals with digital signatures which gives the assurance that someone cannot deny the validity of something
- Therefore a digital signature is required for non-repudiation of communication by a sender. Hence option 1 is correct

Important Point:

Message authentication:

It ensures that message has been sent by a genuine identity and not by an imposter. In this, the receiver needs to be sure of the sender's identity. It is a service beyond message integrity.

Message integrity:

It means that data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously.

Message confidentiality:

It means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.

Question 15 View this Question Online >

A sender S sends a message m to receiver R, which is digitally signed by S with its private key. In this scenario. One or more of the following security violations can take place.

1) S can launch a birthday attack to replace m with a fraudulent message.

2) A third-party attacker can launch a birthday attack to replace m with a fraudulent message.

3) R can launch a birthday attack to replace m with a fraudulent message.

Which of the following are possible security violations?

1. 1 and 2 only
2. 1 only
3. 2 only
4. 2 and 3 only

Answer (Detailed Solution Below)

Option 2 : 1 only

Network Security Question 15 Detailed Solution

Concept:

Birthday attack means sending a fraudulent message with the same has value and digitally signed as that of original message.

Two ways are there for using digital signature:

One is, in which whole message will be encrypted first using sender's private key and then receiver's public key.

Second is, when only message digest is encrypted using sender's private key.

Explanation:

Consider all the violations one by one:

1) S can launch a birthday attack to replace m with a fraudulent message. **TRUE**

In this, S can use some fraudulent message and then encrypt it with its private key and then receiver's public key.

2) A third-party attacker can launch a birthday attack to replace m with a fraudulent message. **FALSE**

Third party attacker can't launch birthday attack, as it doesn't have sender's private key and then can't encrypt the message.

3) R can launch a birthday attack to replace m with a fraudulent message. **FALSE**

R can't launch the birthday attack, because it doesn't have the sender's (S) private key and thereby can't encrypt the message.