ICS MCQs

1. Which of the following field in IPv4 datagram is not related to fragmentation?
a) Flags
b) Offset
c) TOS
d) Identifier

Answer: c

Explanation: TOS-type of service identifies the type of packets. It is not related to fragmentation but is used to request specific treatment such as high throughput, high reliability or low latency for the IP packet depending upon the type of service it belongs to.

2. The TTL field has value 10. How many routers (max) can process this datagram?
a) 11
b) 5
c) 10
d) 1

Answer: c
Explanation: TTL stands for Time to Live. This field specifies the life of the IP packet based on the number of hops it makes (Number of routers it goes through). TTL field is decremented by one each time the datagram is processed by a router. When the value is 0, the packet is automatically destroyed.

4. Which field helps to check rearrangement of the fragments?
a) offset
b) flag
c) ttl
d) identifier
View Answer

Answer: a
Explanation: The Fragment Offset field specifies where the fragment fits in the original datagram. The offset of the first fragment will always be 0. The size of the field (13 bits) is 3-bits shorter than the size of the total length field (16 bits).

5. The size of an IP address in IPv6 is _____
a) 4bytes
b) 128bits
c) 8bytes
d) 100bits
View Answer

Answer: b
Explanation: An IPv6 address is 128 bits long. Therefore, 2128 i.e. 340 undecillion unique addresses are available in IPv6. IPv4 has only 4 billion possible addresses and IPv6 would be a brilliant alternative in case IPv4 runs out of possible new addresses.

6. The header length of an IPv6 datagram is _____
a) 10bytes
b) 25bytes
c) 30bytes
d) 40bytes
View Answer

Answer: d

Explanation: IPv6 datagram has fixed header length of 40bytes, which results in faster processing of the datagram. There is one fixed header and optional headers which may or may not exist. The fixed header contains the mandatory essential information about the packet while the optional headers contain the optional “not that necessary” information.

7. In an IPv6 header, the traffic class field is similar to which field in the IPv4 header?
a) Fragmentation field
b) Fast switching
c) TOS field
d) Option field
View Answer

Answer: c
Explanation: The traffic class field is used to specify the priority of the IP packet which is a similar functionality to the Type of Service field in the IPv4 header. It’s an 8-bit field and its values are not defined in the RFC 2460.

8. IPv6 does not use _____ type of address.
a) Broadcast
b) Multicast
c) Any cast
d) Unicast
View Answer

Answer: a
Explanation: There is no concept of broadcast address in IPv6. Instead, there is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

9. Which are the features present in IPv4 but not in IPv6?
a) Fragmentation
b) Header checksum
c) Options
d) Anycast address
View Answer

Answer: d

Explanation: There is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

10. _____ provides authentication at the IP level.
a) AH
b) ESP
c) PGP
d) SSL
View Answer

Answer: a
Explanation: The Authentication Header (AH) authenticates the origin of data, and guarantees the integrity of the information that's being sent using IPSec. It also provides anti-reply security.

11. ESP does not provide _____
a) source authentication
b) data integrity
c) privacy
d) error control
View Answer

Answer: d
Explanation: The ESP provides data confidentiality, integrity and authentication. It provides confidentiality through encryption. ESP can operate in two modes, transport mode and tunnel mode.

12. _____ ensures the integrity and security of data that are passing over a network.
a) Firewall
b) Antivirus
c) Pentesting Tools
d) Network-security protocols
View Answer

Answer: d
Explanation: The methods and processes in securing network data from unauthorized content extraction are controlled by network-security protocols.

13. Which of the following is not a strong security protocol?
a) HTTPS
b) SSL
c) SMTP
d) SFTP
View Answer

Answer: c
Explanation: SMTP (is abbreviated as Simple Mail Transfer Protocol) is a standard protocol to transmit electronic mail and is a widely used mail transmitting protocol.

14. Which of the following is not a secured mail transferring methodology?
a) POP3
b) SSMTP
c) Mail using PGP
d) S/MIME
View Answer

Answer: a
Explanation: POP (Post Office Protocol) is a simple protocol which fetches the updated mail stored for you by the server. S/MIME (Secure/Multipurpose Internet Mail Extensions), SSMTP (Secure-Simple Mail Transfer Protocol), and PGP (Pretty Good Privacy) are examples of protocols and methods for secure mailing.

15. _____ is a set of conventions & rules set for communicating two or more devices residing in the same network?
a) Security policies
b) Protocols
c) Wireless network
d) Network algorithms
View Answer

Answer: b
Explanation: Network protocols are designed with mechanisms for identifying devices and make connections between them. In addition, some proper rules are defined as to how data packets will be sent and received.

16. TSL (Transport Layer Security) is a cryptographic protocol used for securing HTTP/HTTPS based connection.
a) True
b) False
View Answer

Answer: a
Explanation: TLS which has now become SSL (Secure Socket Layer) is one of the popular cryptographic protocols developed to provide security to computer network while communication.

17. HTTPS is abbreviated as _____
a) Hypertexts Transfer Protocol Secured
b) Secured Hyper Text Transfer Protocol
c) Hyperlinked Text Transfer Protocol Secured
d) Hyper Text Transfer Protocol Secure
View Answer

Answer: d
Explanation: Hyper Text Transfer Protocol Secure (HTTPS) is a security protocol which maintains security when data is sent from browser to server and vice versa. It denotes that all communication setup between the browser and the server is encrypted.

18. SSL primarily focuses on _____

a) integrity and authenticity
b) integrity and non-repudiation
c) authenticity and privacy
d) confidentiality and integrity
View Answer

Answer: a
Explanation: SSL primarily focuses on maintaining the integrity of the data. Also, it maintains authenticity which helps the customers feel secure to communicate over the internet.

19. In SSL, what is used for authenticating a message?
a) MAC (Message Access Code)
b) MAC (Message Authentication Code)
c) MAC (Machine Authentication Code)
d) MAC (Machine Access Code)
View Answer

Answer: b
Explanation: For authenticating in SSL, a short message known as MAC (Message Authentication Code) is used for authenticating a message; where both the sender & the receiver need to implement the same key in order to start communicating.

20. _____ is used for encrypting data at network level.
a) IPSec
b) HTTPS
c) SMTP
d) S/MIME
View Answer

Answer: a
Explanation: IPSec (Secure Internet Protocol) is used for securing data at the network level by using 3 different protocols. These are Encapsulating Secure Payload (ESP), Authentication Header, and Internet Key Exchange (IKE).

21. S/MIME is abbreviated as _____
a) Secure/Multimedia Internet Mailing Extensions
b) Secure/Multipurpose Internet Mailing Extensions
c) Secure/Multimedia Internet Mail Extensions
d) Secure/Multipurpose Internet Mail Extensions
View Answer

Answer: d
Explanation: Secure/Multipurpose Internet Mail Extensions is the most popular protocol used to send encrypted messages that are digitally signed. In this protocol, the encryption is done with a digital sign in them.

22. Users are able to see a pad-lock icon in the address bar of the browser when there is _____ connection.
a) HTTP

b) HTTPS
c) SMTP
d) SFTP
View Answer

Answer: b
Explanation: It is when HTTPS (Hyper Text Transfer Protocol Secure) connection is built an extended validation certificate is installed in the website for security reasons.

23. Why did SSL certificate require in HTTP?
a) For making security weak
b) For making information move faster
c) For encrypted data sent over HTTP protocol
d) For sending and receiving emails unencrypted
View Answer

Answer: c
Explanation: In the case of HTTP connection, data are sent as plain-text, which is easily readable by hackers, especially when it is credit card details and personal information. But with the incorporation of SSL certificate, communication becomes secure and data sent and received are encrypted.

24. Number of phases in the handshaking protocol?
a) 2
b) 3
c) 4
d) 5
View Answer

Answer: c
Explanation: There are 4 phases in the handshaking protocol. These are –
Phase 1 : Establishing security capabilities
Phase 2 : Server Authentication and Key Exchange
Phase 3 : Client Authentication and Key Exchange
Phase 4 : Finish/ End.

25. In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange?
a) server_done
b) server_key_exchange
c) certificate_request
d) crtificate_verify
View Answer

Answer: a
Explanation: The last step of the Phase 2 is the server_done step.

26. In the handshake protocol which is the message type first sent between client and server ?

a) server_hello
b) client_hello
c) hello_request
d) certificate_request
View Answer

Answer: b

Explanation: Interaction between the client and server starts via the client_hello message.

27. Pretty good privacy (PGP) security system uses
a) Public key cryptosystem
b) Private key cryptosystem
c) Public & Private key cryptosystem
d) None of the mentioned
View Answer

Answer: c
Explanation: PGP uses many encryption techniques such as private key cryptosystem and also public key cryptosystem.

28. S/MIME stands for _____.
a. standard multipurpose internet mail extensions.
b. secure multipurpose internet mail extensions.
c. secure multipurpose international mail extensions.
d. standard multipurpose international mail extensions.
Answer: B.

29. _____ uniquely identifies the MIME entities uniquely with reference to multiple contexts.
a. Content description.
b. Content -id.
c. Content type.
d. Content transfer encoding.
Answer: B.

30. In S/MIME,MLA stands for _____.
a. mailing list agent.
b. multipurpose list agent.
c. mail lock agent.
d. message link agent.
Answer: A.

31. The cryptography algorithms used in S/MIME are _____.
a. IDEA.
b. RC4.
c. RSA,DES-3.
d. RC5.

Answer: C.

32. The _____ acts as financial institutions who provides a payment card to a card holder.
a. payment gateway.
b. card holder.
c. acquirer.
d. issuer.
Answer: D.

33. Who will be responsible for processing the payment from the customer's account to the merchant account?
a. Acquirer.
b. Merchant.
c. Issuer.
d. Payment gateway.
Answer: D

34. Which process will ensure that the issues of the credit card is an approved transactions?
a. Payment capture.
b. Payment authorization.
c. Purchase request.
d. Purchase reply.

Answer: B.
30. _____ is used for hiding the payment information from the merchant.
a. SET.
b. SSL.
c. SHTTP.
d. TSP.
Answer: A.

31. What are the different ways to intrude?
a) Buffer overflows
b) Unexpected combinations and unhandled input
c) Race conditions
d) All of the mentioned
View Answer

Answer: d
Explanation: None.

32. What are the major components of the intrusion detection system?
a) Analysis Engine
b) Event provider
c) Alert Database

d) All of the mentioned
View Answer

Answer: d
Explanation: None.

33. What are the different ways to classify an IDS?
a) anomaly detection
b) signature based misuse
c) stack based
d) all of the mentioned
View Answer

Answer: d
Explanation: None.

34. What are the characteristics of anomaly based IDS?
a) It models the normal usage of network as a noise characterization
b) It doesn't detect novel attacks
c) Anything distinct from the noise is not assumed to be intrusion activity
d) It detects based on signature
View Answer

Answer: a
Explanation: None.

35. What is the major drawback of anomaly detection IDS?
a) These are very slow at detection
b) It generates many false alarms
c) It doesn't detect novel attacks
d) None of the mentioned
View Answer

Answer: b
Explanation: None.

36. What are the characteristics of signature based IDS?
a) Most are based on simple pattern matching algorithms
b) It is programmed to interpret a certain series of packets
c) It models the normal usage of network as a noise characterization
d) Anything distinct from the noise is assumed to be intrusion activity
View Answer

Answer: a
Explanation: None.

37. What are the drawbacks of signature based IDS?
a) They are unable to detect novel attacks
b) They suffer from false alarms

c) They have to be programmed again for every new pattern to be detected
d) All of the mentioned
View Answer

Answer: d
Explanation: None.

38. What are the characteristics of Host based IDS?
a) The host operating system logs in the audit information
b) Logs includes logins,file opens and program executions
c) Logs are analysed to detect tails of intrusion
d) All of the mentioned
View Answer

Answer: d
Explanation: None.

39. What are the drawbacks of the host based IDS?
a) Unselective logging of messages may increase the audit burdens
b) Selective logging runs the risk of missed attacks
c) They are very fast to detect
d) They have to be programmed for new patterns
View Answer

Answer: a
Explanation: None.
11. What are the strengths of the host based IDS?
a) Attack verification
b) System specific activity
c) No additional hardware required
d) All of the mentioned
View Answer

Answer: d
Explanation: None.

39. What are characteristics of stack based IDS?
a) They are integrated closely with the TCP/IP stack and watch packets
b) The host operating system logs in the audit information
c) It is programmed to interpret a certain series of packets
d) It models the normal usage of network as a noise characterization
View Answer

Answer: a
Explanation: None.

40. What are characteristics of Network based IDS?
a) They look for attack signatures in network traffic
b) Filter decides which traffic will not be discarded or passed
c) It is programmed to interpret a certain series of packet

d) It models the normal usage of network as a noise characterization
View Answer

Answer: a
Explanation: None.

41. What are strengths of Network based IDS?
a) Cost of ownership reduced
b) Malicious intent detection
c) Real time detection and response
d) All of the mentioned
View Answer

Answer: d
Explanation: None.

42. Network layer firewall works as a _____
a) Frame filter
b) Packet filter
c) Content filter
d) Virus filter
View Answer

Answer: b

Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

43. Network layer firewall has two sub-categories as _____
a) State full firewall and stateless firewall
b) Bit oriented firewall and byte oriented firewall
c) Frame firewall and packet firewall
d) Network layer firewall and session layer firewall
View Answer

Answer: a
Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

44. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____
a) Chock point
b) Meeting point
c) Firewall point
d) Secure point
View Answer

Answer: a

Explanation: A firewall can be a PC, a router, a midrange, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Generally, a firewall is installed at the point where the secure internal network and untrusted external network meet, which is also known as a chokepoint.

45. Which of the following is / are the types of firewall?
a) Packet Filtering Firewall
b) Dual Homed Gateway Firewall
c) Screen Host Firewall
d) Dual Host Firewall
View Answer

Answer: a
Explanation: A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router

46. A proxy firewall filters at _____
a) Physical layer
b) Data link layer
c) Network layer
d) Application layer
View Answer

Answer: d
Explanation: The application firewall is typically built to control all network traffic on any layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is – without additional software – unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

47. A packet filter firewall filters at _____
a) Physical layer
b) Data link layer
c) Network layer
d) Application layer
View Answer

Answer: c
Explanation: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.

48. What tells a firewall how to reassemble a data stream that has been divided into packets?
a) The source routing feature
b) The number in the header's identification field
c) The destination IP address
d) The header checksum field in the packet header
View Answer

Answer: a
Explanation: The source routing feature provides a path address for the packet to help the firewall to reassemble the data stream that was divided into packets. After reassembling, the firewall can then filter the stream.

49. A stateful firewall maintains a _____ which is a list of active connections.
a) Routing table
b) Bridging table
c) State table
d) Connection table
View Answer

Answer: a
Explanation: The routing table basically gives the state of each connection i.e. whether the connection is active or not. A routing table ensures the best performance for the stateful firewall.

50. A firewall needs to be _____ so that it can grow proportionally with the network that it protects.
a) Robust
b) Expansive
c) Fast
d) Scalable
View Answer

Answer: b
Explanation: The firewall has to be expansive because a network is expected to grow with time and if the firewall is unable to grow with it, the firewall won't be able to handle the growing network traffic flow and will hence fail.

51. Firewalls can be of _____ kinds.
a) 1

b) 2
c) 3
d) 4
View Answer

Answer: c
Explanation: Firewalls are of three kinds – one is the hardware firewalls, another is software firewalls and the other is a combination of both hardware and software.

52. _____ is the kind of firewall is connected between the device and the network connecting to internet.
a) Hardware Firewall
b) Software Firewall
c) Stateful Inspection Firewall
d) Microsoft Firewall
View Answer

Answer: a
Explanation: Hardware firewalls are those firewalls that need to be connected as additional hardware between the device through which the internet is coming to the system and the network used for connecting to the internet.

53. _____ is software that is installed using an internet connection or they come by-default with operating systems.
a) Hardware Firewall
b) Software Firewall
c) Stateful Inspection Firewall
d) Microsoft Firewall
View Answer

Answer: b
Explanation: Software firewalls are those kinds of firewalls that are installed in the system using internet connection as we install normal applications and update them. Some operating system vendors provide default firewalls with their operating systems.

54. Which of the following is not a software firewall?
a) Windows Firewall
b) Outpost Firewall Pro
c) Endian Firewall
d) Linksys Firewall
View Answer

Answer: d
Explanation: Windows Firewall, Outpost Firewall Pro and Endian Firewall are software firewalls that are installed in the system. Linksys firewall is not an example of a software firewall.

55. Firewall examines each _____ that are entering or leaving the internal network.
a) emails users

b) updates
c) connections
d) data packets
View Answer

Answer: d
Explanation: Firewalls examines each data packets that are entering or leaving the internal network which ultimately prevents unauthorized access.

56. A firewall protects which of the following attacks?
a) Phishing
b) Dumpster diving
c) Denial of Service (DoS)
d) Shoulder surfing
Answer: c

Explanation: Firewalls are used to protect the computer network and restricts illicit traffic. Denial of Service (DoS) attack is one such automated attack which a firewall with proper settings and the updated version can resist and stop from getting executed.

57. There are _____ types of firewall.
a) 5
b) 4
c) 3
d) 2
View Answer

Answer: b
Explanation: There are four types of firewall based on their working and characteristics. These are Packet Filtering Firewalls, Circuit Level Gateway Firewalls, Application level Gateway Firewalls, and Stateful Multilayer Inspection Firewalls.

58. Packet filtering firewalls are deployed on _____
a) routers
b) switches
c) hubs
d) repeaters
View Answer

Answer: a
Explanation: Packet filtering firewalls are deployed on routers that help in connecting internal network worldwide via the internet.

59. In the _____ layer of OSI model, packet filtering firewalls are implemented.
a) Application layer
b) Session layer
c) Presentation layer
d) Network layer
View Answer

Answer: d
Explanation: In the network layer, which is the third layer of the OSI (Open Systems Interconnection) model, packet filtering firewalls are implemented.

60. The _____ defines the packet filtering firewall rules.
a) Access Control List
b) Protocols
c) Policies
d) Ports
View Answer

Answer: a
Explanation: The Access Control List is a table containing rules that instruct the firewall system to provide the right access. It checks all the packets and scans them against the defined rule set by Network administrator in the packet filtering firewall.

61. ACL stands for _____
a) Access Condition List
b) Anti-Control List
c) Access Control Logs
d) Access Control List
View Answer

Answer: d
Explanation: The Access Control List is a table containing to check all the packets and scans them against the defined rule set by Network administrator in any particular system or firewall.

62. Network administrators can create their own ACL rules based on _____ _____ and _____
a) Address, Protocols and Packet attributes
b) Address, Protocols and security policies
c) Address, policies and Packet attributes
d) Network topology, Protocols and data packets
View Answer

Answer: a
Explanation: Network administrators can create their own ACL rules based on Address, Protocols and Packet attributes. This is generally done where the specific customised type of data packets need to pass through firewall screening.

63. One advantage of Packet Filtering firewall is _____
a) more efficient
b) less complex
c) less costly
d) very fast
View Answer

Answer: c
Explanation: Packet filtering firewalls are more advantageous because they are less costly and they use fewer resources and are used effectively in small networks.

64. Packet filtering firewalls work effectively in _____ networks.
a) very simple
b) smaller
c) large
d) very large complex
View Answer

Answer: b
Explanation: Packet Filtering Firewalls are applied within routers which connect the internal Network system with the outside network using the internet. It works effectively if the internal network is smaller in size.

65. Which of the following is a strong password?
a) 19thAugust88
b) Delhi88
c) P@assw0rd
d) !augustdelhi
View Answer

Answer: c

Explanation: It has a combination of Alphabet both capital and small along with number and special character. Thus always use complex password with a combination of all these.

66. Why is one time password safe?
a) It is easy to generated
b) It cannot be shared
c) It is different for every access
d) It is a complex encrypted password
View Answer

Answer: c
Explanation: One time password is safe since it is generated per access and thus cannot be brute forced or deduced.

67. What is not a best practice for password policy?
a) Deciding maximum age of password
b) Restriction on password reuse and history
c) Password encryption
d) Having change password every 2 years
View Answer

Answer: d

Explanation: Old passwords are more vulnerable to being misplaced or compromised. Passwords should be changed periodically to enhance security.

68. PII stands for
a) Personally identifiable information
b) Personally information Identification
b) Personally information Inquiry
b) Personally Inquiry information

Answer: a

Answer: d

70. Information Technology (IT) Act 2000 came into force on ..... ?
A 17 October 2000
B 9 June 2000
C 1 June 2000
D 1 October 2000

Answer: a