TEQIP III Mid–Term Assessment

Sample Questions—CYBERSECURITY

Topic: Fundamentals of Computer Networks

Q1: Which among the following is the first stop in a DNS query that acts as a middleman between a client and a DNS nameserver. It is also designed to receive queries from client machines through applications such as web browsers to satisfy clients' DNS query requests?

i. TLD Nameserver
ii. Root Name Server
iii. DNS recursor
iv. DNS Resolver

Correct Answer: iii

Q2: Which of the following is an example of Network Vulnerability?

i. A database request that doesn't require any password to retrieve data
ii. All ports opened in the firewall
iii. Granting access to an application without proper authentication
iv. Access to a physical building (Data Centre) without any badge or identification

Correct Answer: ii

Q3: In an OSI Model (Open Systems Interconnection Model), which of the following is the correct flow of data from receivers and senders' network (Note: Here, the receiver is abbreviated as "R" and the sender as "S")?

i. R: Physical >> Data Link >> Network >> Transport >> Session >> Presentation >> Application
S: Application >> Presentation >> Session >> Transport >> Data Link >> Network >> Physical

ii. R: Physical >> Data Link >> Network >> Transport >> Session >> Application >> Presentation
S: Application >> Presentation >> Session >> Transport >> Physical >> Data Link >> Network

iii. R: Physical >> Data Link >> Network >> Transport >> Session >> Presentation >> Application
S: Application >> Presentation >> Session >> Transport >> Network >> Data Link >> Physical

iv. R: Physical >> Network >> Transport >> Session >> Presentation >> Application >> Data Link
S: Application >> Presentation >> Transport >> Network >> Data Link >> Physical >> Session

Correct Answer: iii

Topic: Network Layers

Q4: Consider the following algorithms mentioned below, which of the following can be used as a routing algorithm for designing a network layer?

i. Link State Routing
ii. Shortest Path algorithm
iii. Distance Vector Routing
iv. All of the above

Correct Answer: iv

Q5: Which of the following are design issues in the network layer?

i. Store and Forward Packet Switching
ii. Implementation of Connectionless service
iii. Both I and II
iv. None of the above

Correct Answer: iii

Q6: You are working as a Network Engineer. You have been asked to implement routing information between two neighboring gateway hosts, each with its router in a network of autonomous systems. Which of the following protocols given below will you choose to implement?

i. Border Gateway Protocol
ii. Inter-Domain Routing Protocol
iii. Exterior Gateway Protocol
iv. Enhanced Interior Gateway Routing Protocol

Correct Answer: iii

Topic: Protocols and Cyber Security Vulnerabilities

Q7: Given an IP address (IPV4) of 172.16.13.5 with a 255.255.255.128 subnet mask, figure out which of the following demonstrates the broadcast address, subnet address, and a class of address it belongs to respectively?

i. Broadcast Address: 172.16.13.127, Subnet: 172.16.13.0, Class A
ii. Broadcast Address: 172.16.13.127, Subnet: 172.16.13.0, Class B
iii. Broadcast Address: 172.16.13.255, Subnet: 172.16.13.0, Class B
iv. Broadcast Address: 172.16.255.255, Subnet: 172.16.0.0, Class B

Correct Answer: ii

Q8: Consider the following IPV6 Address 2001:0db8:85a3:0000:0000:8a2e:0370:7334/64.

a) Which of the following will be its correct network range?

i. 2001:0db8:85a3:0000:0000:0000:0000:0000-2001:0db8:85a3:0000:ffff:ffff:ffff:ffff
ii. 2001:0db8:85a3:b880:0000:0000:0000:0000-2001:0db8:85a3:b880:ffff:ffff:ffff:ffff
iii. 2001:0db8:0000:0000:0000:0000:0000:0000-2001:0db8:ffff:ffff:ffff:ffff:ffff:ffff
iv. None of the above

Correct Answer: i

b) What is the type of the IP address?

i. Global Unicast
ii. Solicited Node
iii. Link Local
iv. Site Local

Correct Answer: i

c) If the prefix length is changed to 61, how many networks will be there?

i. 2
ii. 16
iii. 8
iv. 32

Correct Answer: iii

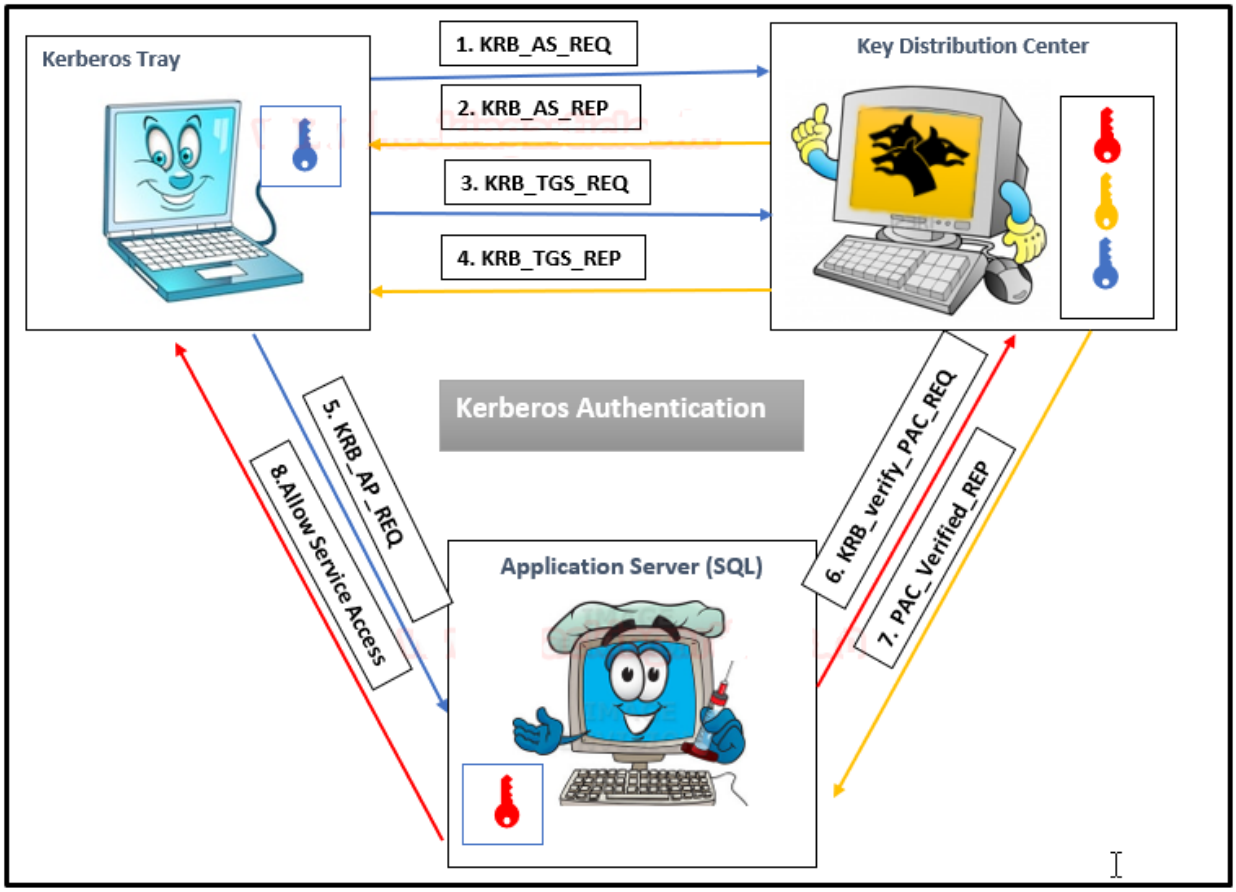
Topic: Essentials for understanding Cybersecurity

Q9: An attacker attacked your organization's security protocol using replays of data transmission from a different sender into the intended receiving system. The attack fooled the employees into believing they have completed the data transmission. Which of the following methods will suit you best to prevent replay attacks?

i. Use Auth0 to use password-less authentication, which relies on single-use codes and email links instead of a traditional password.
ii. Use MFA (Multi-Factor Authentication), which uses a one-time pass as a 2FA, which can be sent via push notifications and text.
iii. Use JSON web Tokens with JTI Claim
iv. All of the Above

Correct Answer: iii

Q10: Consider the following Kerberos workflow using messages; the image given below depicts the role played by Kerberos Distribution Center (KDC) in establishing a secure connection between the server and the client and the entire process uses some special components as shown below:



a) Which of the Key Distribution Center (KDC) keys will generate a Ticket-Granting-Ticket (TGT) for a client that is encrypted using krbtgt hash and some encrypted message using user hash?

i. KRB_AP_REQ
ii. KRB_verify_PAC_REQ
iii. KRB_AS_REP
iv. KRB_AS_REQ

Correct Answer: iii

b) Which of the following keys contains the user sent copy of Ticket Granting Service to the application server?

i. KRB_AP_REQ
ii. PAC_Verified_REP
iii. KRB_AS_REQ
iv. Allow Service Access

Correct Answer: i

c) Which of the following is the correct flow of kerberoasting?

i. SPN Discovery > Brute Force Hash > Convert Kirbi to Hash > Dump KRB_TGS > Request KRB_TGS
ii. Compromised host > Request KRB_TGS > Dump KRB_TGS > brute force hash > Convert Kirbi to hash
iii. SPN discovery > Request KRB_TGS > Dump KRB_TGS > Convert Kirbi to hash > Brute Force Hash
iv. Compromised Host > SPN Discovery > Request KRB_TGS > DUMP KRB_TGS > Convert Kirbi to Hash > Brute Force Hash

Correct Answer: iv