final
Answer Section

TRUE/FALSE

1. ANS: T PTS: 1 REF: 5
2. ANS: F PTS: 1 REF: 13
3. ANS: T PTS: 1 REF: 89
4. ANS: F PTS: 1 REF: 225
5. ANS: F PTS: 1 REF: 393

MULTIPLE CHOICE

6. ANS: A PTS: 1 REF: 45
7. ANS: C PTS: 1 REF: 59
8. ANS: D PTS: 1 REF: 341
9. ANS: A PTS: 1 REF: 360
10. ANS: A PTS: 1 REF: 378

COMPLETION

11. ANS:
    Voice over wireless LAN (VoWLAN)
    Voice over wireless LAN
    VoWLAN

    PTS: 1 REF: 3
12. ANS: information security

    PTS: 1 REF: 11
13. ANS: Wireless gateways

    PTS: 1 REF: 121
14. ANS:
    certification authority (CA)
    certification authority
    CA

    PTS: 1 REF: 263
15. ANS: inform request

PTS: 1 REF: 337

MATCHING

16. ANS: C PTS: 1 REF: 85

17. ANS: F PTS: 1 REF: 159

18. ANS: D PTS: 1 REF: 267

19. ANS: C PTS: 1 REF: 301

20. ANS: D PTS: 1 REF: 362

SHORT ANSWER

21. ANS:
. What is the difference between active and passive monitoring?

One creates traffic on nw, one does not….

Passive Monitoring

The passive approach uses devices to watch the traffic as it passes by. These devices can be special purpose devices such as a Sniffer or they can be built into other devices such as routers, switches or end node hosts.

Examples of such built in techniques include Remote Monitoring (RMON), Simple Network Monitoring Protocol (SNMP) and netflow capable devices.

The passive monitoring devices are polled periodically and information is collected

(in the case of SNMP devices the data is extracted from Management Information Bases (MIB)) to assess network performance and status.

The passive approach does not increase the traffic on the network for the measurements.

And It also measures real traffic. However, the polling required to collect the data, traps and alarms generate network traffic, which can be substantial.

Further the amount of data gathered can be substantial especially if one is doing flow analysis or trying to capture information on all packets.

The passive approach is extremely valuable in network trouble-shooting, however they are limited in their ability emulate error scenarios or isolating the exact fault location.

Since the passive approach may require viewing all packets on the network, there can be privacy or security issues about how to access or protect the data gathered.

Active Monitoring

The active approach relies on the capability injecting test packets into the network or sending packets to servers and applications, following them and measuring service obtained from the network.

As such it does create extra traffic, and the traffic or its parameters are artificial. The volume and other parameters of the introduced traffic is fully adjustable and small traffic volumes are enough to obtain meaningful measurements. See a Comparison of some Internet Active End-to-end Performance Measurement projects for some active measurement projects.

On the other hand, the active approach provides explicit control on the generation of packets for measurement scenarios. This includes control on the nature of traffic generation, the sampling techniques, the timing, frequency, scheduling, packet sizes and types (to emulate various applications), statistical quality, the path and function chosen to be monitored. Being active implies testing what you want, when you need it. Emulation of scenarios is easy and checking if Quality of Service (QoS) or Service Level Agreements (SLAs) are met is relatively straightforward.

PTS: 1 REF: 101

22. ANS:
WPA replaces WEP with an encryption technology called Temporal Key Integrity Protocol (TKIP). WEP uses a 40-bit encryption key and does not change.TKIP has several advantages over WEP. First, it uses a longer 128-bit key. Also, TKIP keys are known as per-packet keys. This means that TKIP dynamically generates a new key for each packet that is created. Per-packet keys prevent collisions, which was one of the primary weaknesses of WEP.When coupled with IEEE 802.1x,TKIP provides an even greater level of security. After accepting a device's credentials, the authentication server can use 802.1x to produce a unique master key for that user session. TKIP distributes the key to the wireless device and AP, setting up an automated key hierarchy and management system. TKIP then dynamically generates unique keys to encrypt every data packet that is wirelessly communicated during a session.

PTS: 1 REF: 151

23. Could you estimate the amount of time it would take to crack a DES encryption by testing all possibilities? If you have a 1GHZ processor, could you estimate the amount of time it would take to crack a DES encryption by testing all 2^56 possibilities?
(2^56) * 100/60/60/24/365/1000000000 = 228.49yrs

24. Alic and Bob question
Responses vary, reasonable response is accepted