GSNA^{Q&As}

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gsna.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which of the following is a wireless auditing tool that is used to pinpoint the actual physical location of wireless devices in the network?

A. KisMAC

B. Ekahau

C. Kismet

D. AirSnort

Correct Answer: B

Ekahau is an easy-to-use powerful and comprehensive tool for network site surveys and optimization. Itis an auditing tool that can be used to pinpoint the actual physical location of wireless devices in the network. This tool can be used to make a map of the office and then perform the survey of the office. In the process, if one finds an unknown node, ekahau can be used to locate that node. Answer: D is incorrect. AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately5 to 10 million packets to decrypt the WEP keys. Answer: C is incorrect. Kismet is a Linux-based

802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:

1.

To identify networks by passively collecting packets

2.

To detect standard named networks

3.

To detect masked networks

4.

To collect the presence of non-beaconing networks via data traffic Answer: A is incorrect. KisMAC is a wireless network discovery tool for Mac OS X. It has a wide range of features, similar to those of Kismet, its Linux/BSD namesake and

far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared toward network security professionals, and is not as novice-friendly as similar applications. KisMAC will scan for networks passively on supported cards - including Apple\\'s AirPort, and AirPort Extreme, and many third-party cards, and actively on any card supported by Mac OS X itself. Cracking of WEP and WPA keys, both by brute force, and exploiting flaws such as weak scheduling and badly generated keys is supported when a card capable of monitor mode is used, and packet reinjection can be done with a supported card. GPS mapping can be performed when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs such as Wireshark.

QUESTION 2

Which of the following is an enterprise-grade network/application/performance monitoring platform that tightly integrates with other smart building management systems, such as physical access control, HVAC, lighting, and time/attendance control?

A. Airwave Management Platform

B. Andrisoft WANGuard Platform

C. akk@da

D. Aggregate Network Manager

Correct Answer: D

Aggregate Network Manager is an enterprise-grade network/application/performance monitoring platform that tightly integrates with other smart building management systems, such as physical access control, HVAC, lighting, and time/

attendance control.

Answer: A is incorrect. Airwave Management Platform (AMP) is wireless network management software. It offers centralized control for Wi-Fi networks. Some of its common features are access point configuration management, reporting,

user tracking, help desk views, and rogue AP discovery. Answer: C is incorrect. akk@da is a simple network monitoring system. It is designed for small and middle size computer networks. Its function is to quickly detect the system or network

faults and display the information about detected faults to the administrators. The information is collected by it in every single minute (a user can decrease this period to 1 second). Approximately all the services of the monitored hosts are

discovered automatically.

Answer: B is incorrect. Andrisoft WANGuard Platform offers solutions for various network issues such as WAN links monitoring, DDoS detection and mitigation, traffic accounting, and graphing.

QUESTION 3

Which of the following is a method of the HttpSession interface and is used to retrieve the time when the session was created?

A. getCreationTime()

B. getSessionCreationTime()

C. getSessionTime()

D. getTime()

Correct Answer: A

The getCreationTime() method returns the time when the session was created. The time is measured in milliseconds since midnight January 1, 1970. This method throws an IllegalStateException if it is called on an invalidated session.
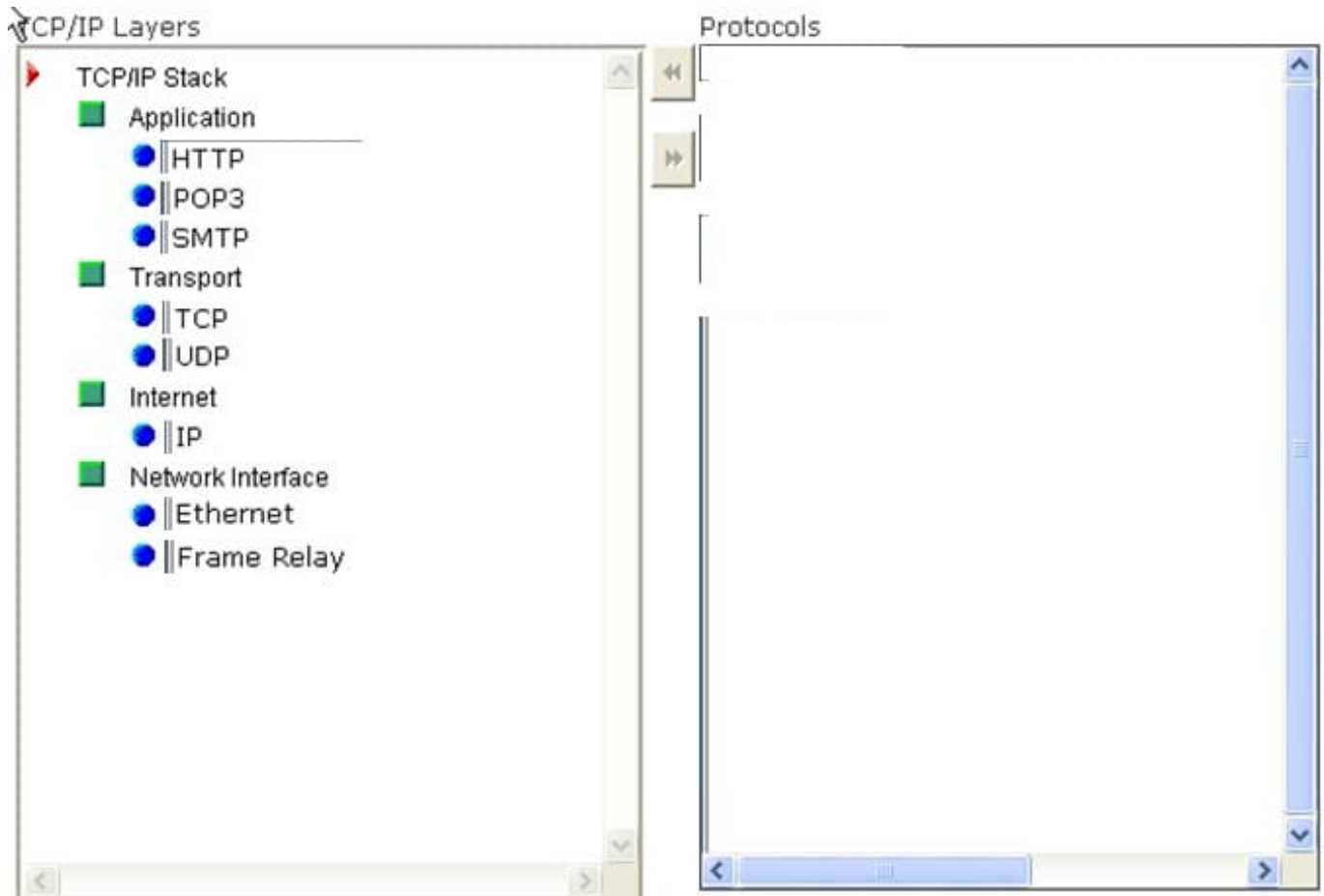
QUESTION 4

DRAG DROP

Place the protocols on the TCP/IP layer to which they are associated.

Select and Place:

Correct Answer:

TCP/IP Layers

Protocols

- TCP/IP Stack
  - Application
    - HTTP
    - POP3
    - SMTP
  - Transport
    - TCP
    - UDP
  - Internet
    - IP
  - Network Interface
    - Ethernet
    - Frame Relay

TCP/IP defines a large set of protocols that allow communication between various devices on a network. TCP/IP classifies the various protocols into different layers. Some of the common protocols are listed in the table below:

TCP/IP Layer	Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Internet	IP
Network Interface	Ethernet, Frame Relay

QUESTION 5

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network. John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

A. Non-operational audit

B. Dependent audit

C. Independent audit

D. Operational audit

Correct Answer: C

An independent audit is an audit that is usually conducted by external or outside resources. It is the process of reviewing detailed audit logs for the following purposes:

1.

To examine the system activities and access logs

2.

To assess the adequacy of system methods

3.

To assess the adequacy of system controls

4.

To examine compliance with established enterprise network system policies

5.

To examine compliance with established enterprise network system procedures

6.

To examine effectiveness of enabling, support, and core processes Answer: B is incorrect. It is not a valid type of security audit. Answer: D is incorrect. It is done to examine the operational and ongoing activities within a network. Answer: B is incorrect. It is not a valid type of security audit. Answer: D is incorrect. It is done to examine the operational and ongoing activities within a network. Answer: A is incorrect. It is not a valid type of security audit.

Latest GSNA Dumps   GSNA PDF Dumps   GSNA Braindumps