



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.pass4itsure.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**

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security equivalent to wired networks for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key.

Which of the following statements are true about WEP?

- A. WEP uses the RC4 encryption algorithm.
- B. The Initialization Vector (IV) field of WEP is only 24 bits long.
- C. It provides better security than the Wi-Fi Protected Access protocol.
- D. Automated tools such as AirSnort are available for discovering WEP keys.

Correct Answer: ABD

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security equivalent to wired networks for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP uses the RC4 encryption algorithm. The main drawback of WEP is that its Initialization Vector (IV) field is only 24 bits long. Many automated tools such as AirSnort are available for discovering WEP keys. Answer: C is incorrect. WPA stands for Wi-Fi Protected Access. It is a wireless security standard. It provides better security than WEP (Wired Equivalent Protection). Windows Vista supports both WPA-PSK and WPAEAP. Each of these is described as follows:

1.

WPA-PSK: PSK stands for Preshared key. This standard is meant for home environment. WPA-PSK requires a user to enter an 8- character to 63-character passphrase into a wireless client. The WPA converts the passphrase into a 256bit key.

2.

WPA-EAP: EAP stands for Extensible Authentication Protocol. This standard relies on a back-end server that runs Remote Authentication Dial-In User Service for user authentication. Note: Windows Vista supports a user to use a smart card to connect to a WPA-EAP protected network.

QUESTION 2

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory- based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company's security policy states that all users using laptops must use smart cards for authentication.

Which of the following authentication techniques will you use to implement the security policy of the company?

- A. IEEE 802.1X using EAP-TLS
- B. IEEE 802.1X using PEAP-MS-CHAP
- C. Pre-shared key



D. Open system

Correct Answer: A

In order to ensure that the laptop users use smart cards for authentication, you will have to configure IEEE 802.1X authentication using the EAP-TLS protocol on the network.

QUESTION 3

Which of the following does an anti-virus program update regularly from its manufacturer's Web site?

A. Hotfixes

B. Permissions

C. Service packs

D. Definition

Correct Answer: D

An anti-virus program updates the virus definition file regularly from the anti-virus manufacturer's Web site. Antivirus (or anti-virus) software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware. Traditional antivirus software solutions run virus scanners on schedule, on demand and some run scans in real time. If a virus or malware is located, the suspect file is usually placed into a quarantine to terminate its chances of disrupting the system. Traditional antivirus solutions scan and compare against a publicized and regularly updated dictionary of malware otherwise known as a blacklist. Some antivirus solutions have additional options that employ a heuristic engine which further examines the file to see if it is behaving in a similar manner to previous examples of malware. A new technology utilized by a few antivirus solutions is whitelisting; this technology first checks if the file is trusted and only questions those that are not. With the addition of wisdom of crowds, antivirus solutions backup other antivirus techniques by harnessing the intelligence and advice of a community of trusted users to protect each other. Answer: C is incorrect. A service pack is a collection of Fixes and Patches in a single product. A service pack can be used to handle a large number of viruses and bugs or to update an operating system with advanced better capabilities. A service pack usually contains a number of file replacements. Answer: A is incorrect. Hotfix is a collection of files used by Microsoft for software updates that are released between major service pack releases. A hotfix is about a problem, occurring under specific circumstances, which cannot wait to be fixed till the next service pack release. Hotfixes are generally related to security problems. Hence, it is essential to fix these problems as soon as possible. Answer: B is incorrect. An anti-virus program does not update Permissions regularly from its manufacturer's Web site.

QUESTION 4

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set the hard disk geometry parameters, cylinders, heads, and sectors.

Which of the following Unix commands can you use to accomplish the task?

A. mke2fs

B. mkswap

C. mkfs



D. hdparm

Correct Answer: D

In Unix, the hdparm command is used to get or set hard disk geometry parameters, cylinders, heads, and sectors.

Answer: C is incorrect. In Unix, the mkfs command initializes a Unix filesystem. This is a front end that runs a separate program depending on the filesystem's type.

Answer: A is incorrect. In Unix, the mke2fs command creates a Unix second extended filesystem. Answer: B is incorrect. In Unix, the mkswap command sets up a Unix swap area on a device or file.

QUESTION 5

You have detected what appears to be an unauthorized wireless access point on your network. However, this access point has the same MAC address as one of your real access points and is broadcasting with a stronger signal.

What is this called?

- A. Bluesnarfing
- B. The evil twin attack
- C. WAP cloning
- D. DOS

Correct Answer: B

In the evil twin attack, a rogue wireless access point is set up that has the same MAC address as one of your legitimate access points. That rogue WAP will often then initiate a denial of service attack on your legitimate access point making it

unable to respond to users, so they are redirected to the 'evil twin'. Answer: A is incorrect. Bluesnarfing is the process of taking over a PDA. Answer: D is incorrect. A DOS may be used as part of establishing an evil twin, but this attack is not

specifically for denial of service.

Answer C is incorrect. While you must clone a WAP MAC address, the attack is not called WAP cloning.

[GSNA PDF Dumps](#)

[GSNA Practice Test](#)

[GSNA Brindumps](#)