GSNA Q&As

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

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

QUESTION 1

You work as a Network Administrator for Infosec Inc. Nowadays, you are facing an unauthorized access in your Wi-Fi network. Therefore, you analyze a log that has been recorded by your favorite sniffer, Ethereal. You are able to discover

the cause of the unauthorized access after noticing the following string in the log file:

(Wlan.fc.type_subtype eq 32 and llc.oui eq 0x00601d and llc.pid eq 0x0001) When you find All your 802.11b are belong to us as the payload string, you are convinced about which tool is being used for the unauthorized access.

Which of the following tools have you ascertained?

A. AiroPeek

B. AirSnort

C. Kismet

D. NetStumbler

Correct Answer: D

NetStumbler, a war driving tool, uses an organizationally unique identifier (OID) of 0x00601A, D protocol identifier (PID) of 0x0001. Each version has a typical payload string. For example, NetStumbler 3.2.3 has a payload string: \\'All your

802.11b are belong to us\\'. Therefore, when you see the OID and PID values, you discover that the attacker is using NetStumbler, and when you see the payload string, you are able to ascertain that the attacker is using NetStumbler 3.2.3.

QUESTION 2

Which of the following user authentications are supported by the SSH-1 protocol but not by the SSH-2 protocol?

A. TIS authentication

B. Kerberos authentication

C. Rhosts (rsh-style) authentication

D. Password-based authentication

Correct Answer: ABC

The Rhosts (rsh-style), TIS, and Kerberos user authentication methods are supported by the SSH-1 protocol but not by SSH-2 protocol. Answer: D is incorrect. Password-based authentication is supported by both the SSH-1 and SSH-2 protocols.

QUESTION 3

Which of the following encryption modes are possible in WEP?

A. 128 bit encryption

B. No encryption

C. 256 bit encryption

D. 40 bit encryption

Correct Answer: ABD

WEP supports three encryption modes, i.e., no encryption, 40 bit encryption, and 128 bit encryption. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and

encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the

attacks that attempt to reveal the key stream.

Answer: C is incorrect. WEP does not support 256 bit encryption.

QUESTION 4

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

A. Safeguards

B. Detective controls

C. Corrective controls

D. Preventive controls

Correct Answer: C

Corrective controls are used after a security breach. After security has been breached, corrective controls are intended to limit the extent of any damage caused by the incident, e.g. by recovering the organization to normal working status as

efficiently as possible.

Answer: D is incorrect. Before the event, preventive controls are intended to prevent an incident from occurring, e.g. by locking out unauthorized intruders.

Answer: B is incorrect. During the event, detective controls are intended to identify and characterize an incident in progress, e.g. by sounding the intruder alarm and alerting the security guards or the police. Answer: A is incorrect. Safeguards

are those controls that provide some amount of protection to an asset.

QUESTION 5

You work as a Security Administrator in Tech Perfect Inc. The company has a TCP/IP based network. The network has a vast majority of Cisco Systems routers and Cisco network switches. You want to take a snapshot of the router running configuration and archive running configuration of the router to persistent storage.

Which of the following steps will you take?

A. Secure the boot configuration

B. Restore an archived primary bootset

C. Verify the security of the bootset

D. Enable the image resilience

Correct Answer: A

In order to take a snapshot of the router running configuration and archive running configuration of the router to persistent storage, you should secure the boot configuration of the router using the secure boot- config command.

Answer: D is incorrect. You can enable the image resilience, if you want to secure the Cisco IOS image. Answer: C is incorrect. By verifying the security of bootset, you can examine whether or not the Cisco IOS Resilient Configuration is

enabled and the files in the bootset are secured. Answer: B is incorrect. By restoring an archived primary bootset, you can restore a primary bootset from a secure archive after an NVRAM has been erased or a disk has been formatted.

Latest GSNA Dumps GSNA PDF Dumps GSNA Exam Questions