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.geekcert.com/gsna.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following is used to execute a SQL statement from the SQL buffer?

A. Entering an asterisk (*)

B. Pressing [RETURN] once

C. Pressing [RETURN] twice

D. Entering a slash (/)

E. Pressing [ESC] twice.

Correct Answer: D

A SQL statement or a PL/SQL block can be executed by entering a semicolon (;) or a slash (/), or by using the RUN command at SQL prompt. When a semicolon (;) is entered at the end of a command, the command is completed and

executed. When a slash (/) is entered, the command in the buffer is executed. It can also be used to execute a PL/SQL block. The RUN command is used to execute a command in the buffer. Note: The SQL buffer stores the most recently

used SQL commands and PL/SQL blocks. It does not store SQL* Plus commands. It can be edited or saved to a file. Note: A SQL command can be saved in the buffer by entering a blank line.

Reference: Oracle8i Online Documentation, Contents: "SQL*PLUS Users Guide and Reference", "Learning SQL*PLUS Basics,3 of 4", "Understanding SQL COMMAND Syntax"

QUESTION 2

Which of the following tools monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools?

A. Snort

B. IDS

C. Firewall

D. WIPS

Correct Answer: D

Wireless intrusion prevention system (WIPS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices. Rogue devices can spoof MAC address of an authorized network device as their own. WIPS uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices. Answer B is incorrect. An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins and access

to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components:

1.

Sensors

2.

Console

3.

Engine

Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations,

these three components are combined into a single device.

Basically, following two types of IDS are used:

1.

Network-based IDS

2.

Host-based IDS

Answer: A is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed

for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as

follows:

Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console.

Packet logger mode: It logs the packets to the disk.

Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer: C is incorrect. A firewall is a tool to provide security to a

network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the

Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports.

QUESTION 3

An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person.

What type of attack is this?

A. Session Hijacking

B. Bluesnarfing

C. Privilege Escalation

D. PDA Hijacking

Correct Answer: B

Bluesnarfing is a rare attack in which an attacker takes control of a bluetooth enabled device. One way to do this is to get your PDA to accept the attacker\\'s device as a trusted device.

QUESTION 4

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set some terminal characteristics and environment variables.

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

A. /etc/sysconfig/routed

B. /proc/net

C. /etc/sysconfig/network-scripts/ifcfg-interface

D. /etc/sysconfig/init

Correct Answer: D

In Unix, the /etc/sysconfig/init file is used to set terminal characteristics and environment variables. Answer: B is incorrect. In Unix, the /proc/net file contains status information about the network protocols. Answer: C is incorrect. In Unix, the /

etc/sysconfig/network-scripts/ifcfg-interface file is the configuration file used to define a network interface.

Answer: A is incorrect. In Unix, the /etc/sysconfig/routed file is used to set up the dynamic routing policies.

QUESTION 5

You work as a Web Deployer for UcTech Inc. You write the element for an application in which you write the sub-element as follows: * Who will have access to the application?

A. Only the administrator

B. No user

C. All users

D. It depends on the application.

Correct Answer: C

The element is a sub-element of the element. It defines the roles that are allowed to access the Web resources specified by the sub-elements. The element

is written in the deployment descriptor as follows:

---------- Administrator Writing Administrator within the

element will allow only the administrator to have access to the resource defined within the element.