GNSA Q&As

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

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

https://www.pass2lead.com/gnsa.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 statements are true about SSIDs?

A. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.

B. SSIDs are case insensitive text strings and have a maximum length of 64 characters.

C. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

D. SSID is used to identify a wireless network.

Correct Answer: ACD

SSID stands for Service SetIdentifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters. All wireless devices on a wireless network must have the same SSID in order to communicate with each other. The SSID on computers and the devices in WLAN can be set manually and automatically. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict. A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to disable the automatic SSID broadcast feature in order to improve network security.

QUESTION 2

You are the Network Administrator for a software development company. Your company creates various utilities and tools. You have noticed that some of the files your company creates are getting deleted from systems. When one is deleted,

it seems to be deleted from all the computers on your network.

Where would you first look to try and diagnose this problem?

A. Antivirus log

B. IDS log

C. System log

D. Firewall log

Correct Answer: A

Check the antivirus log and see if it is detecting your file as a virus and deleting it. All antivirus programs have a certain rate of false positives. Since the file is being deleted from all computers, it seems likely that your antivirus has mistakenly

identified that file as a virus.

Answer: D is incorrect. The firewall log can help you identify traffic entering or leaving your network, but won\\'t help with files being deleted. Answer: B is incorrect. An IDS log would help you identify possible attacks, but this scenario is unlikely

to be from an external attack.

Answer: C is incorrect. Your system log can only tell you what is happening on that individual computer.

QUESTION 3

Which of the following statements is true about residual risks?

A. It is the probabilistic risk after implementing all security measures.

B. It can be considered as an indicator of threats coupled with vulnerability.

C. It is a weakness or lack of safeguard that can be exploited by a threat.

D. It is the probabilistic risk before implementing all security measures.

Correct Answer: A

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer: B is incorrect. In information security, security risks are considered as an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. Answer: C is incorrect. Vulnerability is a weakness or lack of safeguard that can be exploited by a threat, thus causing harm to the information systems or networks. It can exist in hardware, operating systems, firmware, applications, and configuration files. Vulnerability has been variously defined in the current context as follows:

1.A security weakness in a Target of Evaluation due to failures in analysis, design, implementation, or operation and such.

2.Weakness in an information system or components (e.g. system security procedures, hardware design, or internal controls that could be exploited to produce an information-related misfortune.)

3. The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

QUESTION 4

What is the extension of a Cascading Style Sheet?

A. .hts

B. .cs

C. .js

D. .css

Correct Answer: D

A Cascading Style Sheet (CSS) is a separate text file that keeps track of design and formatting information, such as colors, fonts, font sizes, and margins, used in Web pages. CSS is used to provide Web site authors greater control on

the appearance and presentation of their Web pages. It has codes that are interpreted and applied by the browser on to the Web pages and their elements. CSS files have .css extension. There are three types of Cascading Style Sheets: External Style Sheet Embedded Style Sheet Inline Style Sheet

QUESTION 5

In which of the following social engineering attacks does an attacker first damage any part of the target\\'s equipment and then advertise himself as an authorized person who can help fix the problem.

A. Reverse social engineering attack

B. Impersonation attack

C. Important user posing attack

D. In person attack

Correct Answer: A

A reverse social engineering attack is a person-to-person attack in which an attacker convinces the target that he or she has a problem or might have a certain problem in the future and that he, the attacker, is ready to help solve the problem.

Reverse social engineering is performed through the following steps: An attacker first damages the target\\'s equipment. He next advertises himself as a person of authority, ably skilled in solving that problem. In this step, he gains the trust of

the target and obtains access to sensitive information.

If this reverse social engineering is performed well enough to convince the target, he often calls the attacker and asks for help. Answer: B, C, D are incorrect. Person-to-Person social engineering works on the personal level. It can be

classified as follows:

Impersonation: In the impersonation social engineering attack, an attacker pretends to be someone else, for example, the employee\\'s friend, a repairman, or a delivery person. In Person Attack: In this attack, the attacker just visits the

organization and collects information. To accomplish such an attack, the attacker can call a victim on the phone, or might simply walk into an office and pretend to be a client or a new worker.

Important User Posing: In this attack, the attacker pretends to be an important member of the organization. This attack works because there is a common belief that it is not good to question authority. Third-Party Authorization: In this attack,

the attacker tries to make the victim believe that he has the approval of a third party. This works because people believe that most people are good and they are being truthful about what they are saying.