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 the Enum tool?

A. It uses NULL and User sessions to retrieve user lists, machine lists, LSA policy information, etc.

B. It is capable of performing brute force and dictionary attacks on individual accounts of Windows NT/2000.

C. One of the countermeasures against the Enum tool is to disable TCP port 139/445.

D. It is a console-based Win32 information enumeration utility.

Correct Answer: ABCD

Enum is a console-based Win32 information enumeration utility. It uses null sessions to retrieve user lists, machine lists, share lists, namelists, group and member lists, passwords, and LSA policy information. It is also capable of performing brute force and dictionary attacks on individual accounts. Since the Enum tool works on the NetBIOS NULL sessions, disabling the NetBIOS port can be a good countermeasure against the Enum tool.

QUESTION 2

You have an online video library. You want to upload a directory of movies. Since this process will take several hours, you want to ensure that the process continues even after the terminal is shut down or session is closed.

What will you do to accomplish the task?

A. Use the bg command to run the process at the background.

B. Add the nohup command in front of the process.

C. Add the nohup command at the end of the process.

D. Run the process inside a GNU Screen-style screen multiplexer.

Correct Answer: BD

Whenever the nohup command is added in front of any command or process, it makes the command or process run even after the terminal is shut down or session is closed. All processes, except the \\'at\\' and batch requests, are killed when a

user logs out. If a user wants a background process to continue running even after he logs out, he must use the nohup command to submit that background command. To nohup running processes, press ctrl+z, enter "bg" and enter "disown".

The other way to accomplish the task is to run the command/process inside a GNU Screen-style screen multiplexer, and then detach the screen. GNU Screen maintains the illusion that the user is always logged in, and allows the user to

reattach at any time. This has the advantage of being able to continue to interact with the program once reattached (which is impossible with nohup alone).

Answer: C is incorrect. The nohup command works when it is added in front of a command.

Answer: A is incorrect. The bg command cannot run the command or process after the terminal is shut down or session is closed.

QUESTION 3

Which of the following encryption encoding techniques is used in the basic authentication method?

A. HMAC_MD5

B. Md5

C. DES (ECB mode)

D. Base64

Correct Answer: D

Base64 encryption encoding, which can easily be decoded, is used in the basic authentication method.

Answer: B is incorrect. The Md5 hashing technique is used in the digest authentication method.

Answer: A is incorrect. The HMAC_MD5 hashing technique is used in the NTLMv2 authentication method.

Answer: C is incorrect. DES (ECB mode) is used in the NTLMv1 authentication method.

QUESTION 4

You work as a Network Auditor for XYZ CORP. The company has a Windows-based network. While auditing the company\\'s network, you are facing problems in searching the faults and other entities that belong to it.

Which of the following risks may occur due to the existence of these problems?

A. Residual risk

B. Inherent risk

C. Secondary risk

D. Detection risk

Correct Answer: D

Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk:

Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample.

Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults). Answer: A is incorrect. Residual risk

is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder".

Answer: B is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the

professional judgment of the auditor, and it is done after assessing the business environment of the entity being audited.

Answer: C is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as

primary risks, but can turn out to be so if not estimated and planned properly.

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. Buesnarfing

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. Blue snarfing 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.

GNSA VCE Dumps GNSA Exam Questions GNSA Braindumps