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

You have to move the whole directory /foo to /bar. Which of the following commands will you use to accomplish the task?

A. mv /bar /foo

B. mv -R /foo /bar

C. mv /foo /bar

D. mv -r /bar /foo

Correct Answer: C

You will use the mv /foo /bar command to move the whole directory /foo to /bar. The mv command moves files and directories from one directory to another or renames a file or directory. mv must always be given at least two arguments.

The first argument is given as a source file.

The second argument is interpreted as the destination.

If destination is an existing directory, the source file is moved to that directory with the same name as the source. If the destination is any other directory, the source file is moved and/or renamed to that destination name.

Syntax : mv [options] source destination Some important options used with mv command are as follows:

OPTION	DESCRIPTION
-f	It never asks before overwriting.
-i	It asks before overwriting.
-b	It makes a backup of each file that would otherwise be overwritten.
-v	It prints the name of each file before moving it.

Answer: A is incorrect. The mv /bar /foo command will move the whole /bar directory to the /foo directory. Answer: B, D are incorrect. These are not valid Linux commands.

QUESTION 2

Which of the following can be the countermeasures to prevent NetBIOS NULL session enumeration in Windows 2000 operating systems?

A. Denying all unauthorized inbound connections to TCP port 53

B. Disabling SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface

C. Editing the registry key HKLM\SYSTEM\CurrentControlSet\LSA and adding the value RestrictAnonymous

D. Disabling TCP port 139/445

Correct Answer: BCD

NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure. One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator.

2.

A Network Administrator can also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface.

3.

A Network Administrator can also restrict the anonymous user by editing the registry values:

-a.Open regedit32, and go to HKLM\SYSTEM\CurrentControlSet\LSA.

-b.Choose edit > add value. Value name: RestrictAnonymous Data Type: REG_WORD Value: 2

Answer: A is incorrect. TCP port 53 is the default port for DNS zone transfer. Although disabling it can help restrict DNS zone transfer enumeration, it is not useful as a countermeasure against the NetBIOS NULL session enumeration.

QUESTION 3

Which TCP and UDP ports can be used to start a NULL session attack in NT and 2000 operating systems?

A. 149 and 133

B. 203 and 333

C. 139 and 445

D. 198 and 173

Correct Answer: C

A null session is an anonymous connection to a freely accessible network share called IPC$ on Windows- based servers. It allows immediate read and write access with Windows NT/2000 and read-access with Windows XP and 2003. The command to be inserted at the DOS-prompt is as follows: net use \\IP address_or_host name\ipc$ "" "/user:" net use Port numbers 139 TCP and 445 UDP can be used to start a NULL session attack.

QUESTION 4

Which of the following are the methods of the HttpSession interface? (Choose three)

A. setAttribute(String name, Object value)

B. getAttribute(String name)

C. getAttributeNames()

D. getSession(true)

Correct Answer: ABC

The HttpSession interface methods are setAttribute(String name, Object value), getAttribute(String name), and getAttributeNames(). The getAttribute(String name) method of the HttpSession interface returns the value of the named attribute as an object. It returns a null value if no attribute with the given name exists. The setAttribute(String name, Object value) method stores an attribute in the current session. The setAttribute(String name, Object value) method binds an object value to a session using the String name. If an object with the same name is already bound, it will be replaced. The getAttributeNames() method returns an Enumeration containing the names of the attributes available to the current request. It returns an empty Enumeration if the request has no attributes available to it. Answer: D is incorrect. The getSession(true) method is a method of the HttpServletRequest interface. The getSession(true) method gets the current session associated with the client request. If the requested session does not exist, the getSession(true) method creates a new session object explicitly for the request and returns it to the client.

QUESTION 5

Mark is an attacker. He wants to discover wireless LANs by listening to beacons or sending probe requests and thereby provide a launch point for further attacks.

Which of the following tools can he use to accomplish the task?

A. DStumbler

B. Wellenreiter

C. KisMAC

D. Airmon-ng

Correct Answer: ACD

War driving is an attack in which the attacker discovers wireless LANs by listening to beacons or sending probe requests, thereby providing a launch point for further attacks. Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler,

Wellenreiter, and WiFiFoFum are the tools that can be used to perform a war driving attack.

Answer: B is incorrect. Wellenreiter is a tool that is used to perform MAC spoofing attacks.