GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.leads4pass.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following techniques does an attacker use to sniff data frames on a local area network and modify the traffic?

A. MAC spoofing

B. IP address spoofing

C. Email spoofing

D. ARP spoofing

Correct Answer: D

QUESTION 2

FILL BLANK

Fill in the blank with the appropriate name of the attack.

_____ takes best advantage of an existing authenticated connection.

A. session hijacking

Correct Answer: A

QUESTION 3

Which of the following refers to applications or files that are not classified as viruses or Trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization?

A. Hardware

B. Grayware

C. Firmware

D. Melissa

Correct Answer: B

QUESTION 4

A system administrator finds the entry below in an Apache log. What can be done to mitigate against this?

192.168.116.201 - - [22/Apr/2016:13:43:26 -0400] "GET http://www.giac.org%2Farticles.php%3Fid%3D3+and+%28select+1+from+mysql.user+limit+0%2C1%29%3D1 HTTP/1.1" 200 453 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0"

A. Filter user input using Javascript on the client browser

B. Reduce the permissions of the user account running the web application

C. Filter user input before it gets passed to the application

D. Create drop-downs for users to choose their search terms

Correct Answer: B

QUESTION 5

You are a member of your organization\\'s security team. A new ticket just came into your service desk and was escalated to you. One of the system administrators noticed the following entry in a Windows Server 2008 R2 file server Security event log:

Log Name: Security Source: Microsoft-Windows-Security-Auditing Date: 2/1/2012 2:24:07 AM Event ID: 4674 Task Category: Sensitive Privilege Use Level: Information Keywords: Audit Failure User: N/A Computer: somehost.somecompany.com Description: An operation was attempted on a privileged object.

Subject: Security ID: LOCAL SERVICE Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5

Object: Object Server: LSA Object Type: Object Name: Object Handle: 0x0

Process Information: Process ID: 0x1d8 Process Name: C:\Windows\System32\lsass.exe

Requested Operation: Desired Access: 16777216 Privileges: SeSecurityPrivilege

What is your next step?

A. Initiate the "Containment" phase of the Incident Handling process

B. Search Microsoft\\'s TechNet to find out if this is a normal Windows Security event

C. Disable the trusted account status of the Local Service account

D. Request that all audit failure log entries be forwarded to you

Correct Answer: A