

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

An incident handler concluded that a recent breach could have been prevented with a software patch. In their report they recommended the organization perform regular vulnerability scans, document the findings and update software assets.

Six months later the incident handler investigates a new breach and concludes the web server was infected due to an outdated version of a Content Management System (CMS).

Based on this information, what part of the incident handling process does the organization need to improve?

- A. Disabling unused software to prevent infection
- B. Identifying and responding to incidents quickly
- C. Following up on post-incident recommendations
- D. Maintaining time-stamped logs of user activity

Correct Answer: C

QUESTION 2

A client wants a system so that they can monitor connection queues on network equipment for too many half-open connections, as well as look for bandwidth consumption from the same types of connections. What kind of attacks will this type of system defend against?

- A. Smurf attacks
- B. Passive scans
- C. CPUHog attacks
- D. SYN Floods

Correct Answer: C

QUESTION 3

Which of the following attacking methods allows the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer by changing the Media Access Control address?

- A. IP address spoofing
- B. VLAN hopping
- C. ARP spoofing
- D. MAC spoofing

Correct Answer: D

QUESTION 4

Which of the following describes a suspicious event in the service data below? root@kali:~/volatility# ./vol.py -f ../mem/Desk005.vmem svcscan

BLUE	Offset: 0x16c2705b6c0 Order: 377 Start: SERVICE_DFMAND_START Process ID: 1208 Service Name: SEMgrSvc Display Name: Payments and NFC/SE Manager Service Type: SERVICE_WIN32_OWN_PROCESS Service State: SERVICE_RUNNING Binary Path: C:\Windows\system32\svchost.exe -k LocalService -p
-------------	---

GREEN	Offset: 0x16c274f6860 Order: 591 Start: SERVICE_DFMAND_START Process ID: 8839 Service Name: PimIndexMaintenanceSvc_4e3d6 Display Name: Contact Host_4e3d6 Service Type: SERVICE_WIN32_SHARE_PROCESS Service State: SERVICE_RUNNING Binary Path: C:\TEMP\Windows\system32\svchost.exe -k UnistackSvcGroup -p
--------------	---

YELLOW	Offset: 0x16c274f6520 Order: 590 Start: SERVICE_AUTO_START Process ID: 3928 Service Name: OneSyncSvc_4e3d6 Display Name: Sync Host_4e3d6 Service Type: SERVICE_WIN32_SHARE_PROCESS Service State: SERVICE_RUNNING Binary Path: C:\Windows\system32\svchost.exe -k UnistackSvcGroup
---------------	--

PURPLE	Offset: 0x16c2704a1c0 Order: 286 Start: SERVICE_DEMAND_START Process ID: Service Name: NetSetupSvc Display Name: - Service Type: SERVICE_WIN32_SHARE_PROCESS Service State: SERVICE_STOPPED Binary Path: -
---------------	--

- A. GREEN: Executables should not be run from temporary folders
- B. BLUE: Service names should be all capital letters
- C. PURPLE: Services should not be in the STOPPED state
- D. YELLOW: Option -k should be followed by -p for svchost

Correct Answer: D

QUESTION 5

Which of the following makes it difficult to block the source of DNS amplification attacks?

- A. TCP packets are easy to spoof
- B. UDP packets are easy to spoof
- C. Clients require external DNS communications
- D. Clients require recursive DNS lookups

Correct Answer: C