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.passapply.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 administrator needs to protect his organization\\'s IIS webservers from Cross-Site Scripting attacks. Which action should he take?

A. Use the Anti-XSS library from Microsoft

B. Configure two-factor authentication for clients

C. Use a random element when setting session cookies

D. Configure application whitelisting on the IIS server

Correct Answer: C

Reference: https://www.sciencedirect.com/topics/computer-science/hidden-form-field

QUESTION 2

US Garments wants all encrypted data communication between corporate office and remote location.

They want to achieve following results: l Authentication of users l Anti-replay l Anti-spoofing l IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Anti-replay

B. IP packet encryption

C. Authentication of users

D. Anti-spoofing

Correct Answer: AD

QUESTION 3

What would be the classification of a worm with the following characteristics?

```
Initial vulnerability:
    Existing IIS vulnerability that had been addressed in a service pack
Infection vector:
    Email, open shares, compromised websites, IIS directory traversal, Code Red backdoors
Payload:
    Guest account added to Administrator user group
    Opens all local drives for sharing
    Modifies web documents
    Network scans
    Email propagation
```

A. Zero day

B. Multiplatform

C. Multi-Exploit

D. Metamorphic

E. Polymorphic

Correct Answer: A

QUESTION 4

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in

following the test. Visitors were allowed to click on a company\\'s icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows

strict Internet access.

How was security compromised and how did the firewall respond?

A. The attack was social engineering and the firewall did not detect it.

B. Security was not compromised as the webpage was hosted internally.

C. The attack was Cross Site Scripting and the firewall blocked it.

D. Security was compromised as keylogger is invisible for firewall.

Correct Answer: A

QUESTION 5

As an incident handler for the xyz widget company, you have responded to the breach of your mail server. The server is not in a DMZ but on your internal network and was being used as a launching point to attack other systems on the same network. The compromise was discovered quickly and the network cable was disconnected from the mail server. Which

of the following tools will allow you to complete the next sub phase, following short-term containment activities, on the server in its current state?

A. Wireshark

B. Enum

C. dd

D. Cain

Correct Answer: C

The second sub phase is backup. Of the listed tools only dd can be used to create a backup of the compromised hard drive. Cain and Enum are tools used to attack systems and Wireshark is a network sniffer.