# 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.pass2lead.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

**QUESTION 1**

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?

A. Spoofing

B. Hacking

C. SYN attack

D. PING attack

Correct Answer: C

**QUESTION 2**

What kind of topics should be addressed by the Lessons Learned report?

A. Official press release, evidence from the intrusion, and future testing plans

B. Process modifications, technology needs, and incident handling improvements

C. Personnel issues, disciplinary actions, and mistakes made by incident handlers

D. Individual accounts of the incident, system log entries, and legal warrants

Correct Answer: B

The Lessons Learned report should address process improvements, technology recommendations, and improvements that can be made to the Incident Handling process.

**QUESTION 3**

What is an effective mitigation for an HTTP flood attack?

A. Inspect connections using a reverse proxy and stall those showing repetitive patterns

B. Drop connections using the most bandwidth

C. Interrupt connections using CAPTCHA

D. Analyze requests and drop those using multiple GETs

Correct Answer: C

HTTP floods are difficult to mitigate through analysis of sessions or by statistical criteria because HTTP flood requests are designed to appear as normal traffic. Floods originate from bots that are running scripts that make normal-looking GET and POST requests in normal traffic volumes and with expected Useragent values. It is the collective bandwidth of all bots rather than high traffic from a single source that creates the DoS. Because they are bots that are running a script, they are unable to react to situations that require human interactions, like CAPTCHAs. Another characteristic of website traffic is its repetitiveness as users traverse pages in the site, which renders this ineffective as a tactic for preventing floods.

**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**

What is one of the simplest AND most common ways for an attacker to camouflage files on a UNIX system?

A. Use S-Tools to embed the files into a graphic image

B. Run "chmod 600" on the files to be hidden

C. Use a dot-space or dot-dot-space as the file or directory name

D. Insert the data into an alternate data stream using the colon (:)

E. Install a kernel-level rootkit

Correct Answer: E

Reference: https://www.sciencedirect.com/topics/computer-science/rootkits

GCIH Study Guide GCIH Exam Questions GCIH Braindumps