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

John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.

Which of the following worms has attacked the computer?

A. Code red

B. Ramen

C. LoveLetter

D. Nimda

Correct Answer: B

QUESTION 2

You are the leader of an incident handling team for a mid-size manufacturer in the United States. Several of your company\\'s products are patented and several processes used in the manufacturing process are considered trade secrets. A member of your company\\'s firewall team sent you a tcpdump of a firewall log thought looked suspicious. The packets in question had the same external source IP address, the same internal destination IP addresses, and the same source and destination ports were used in each packet. The only difference between the packets was that the TTL\\'s had been incremented. How can you best determine if this is a sign of something malicious or not?

A. Set up a host intrusion detection system on the host with the internal IP address

B. Gather more data from your firewall logs and from other system logs inside your network

C. Check the Internet Storm Center\\'s Top 10 Source IPs Report to see if the external IP address is listed

D. Run a protocol analyzer on your computer with a filter that will only show the internal or external IP address

Correct Answer: A

QUESTION 3

An attacker is launching an attack against an input field in a form that is used to retrieve restricted information that is filtered dependent upon the privileges of the logged in user. This attacker inserts "\\' or 1=1;--" into this field. What is most likely the attacker\\'s desired result from this insertion?

A. This forces a bypass on the back-end authentication mechanism, allowing total access to the entire database

B. This forces a TRUE condition and may cause the SQL server to return all of the information in the selected field(s)

C. This forces a UNION condition and may cause the SQL server to return a list of all columns in the database

D. This forces an INSERT condition and will dump all rows in the table to the users screen

Correct Answer: D

QUESTION 4

How would an attacker hide an executable from being viewed by Windows Explorer?

A. Rename it to `.. `

B. Change the extension from .exe to .dll

C. Encrypt it with RC4

D. Place it into an ADS of a .txt file

Correct Answer: B

Reference: https://www.bleepingcomputer.com/news/microsoft/hiding-windows-file-extensions-is-a-security-risk-enable-now/

QUESTION 5

Which of the following is one of the fields that Covert TCP uses to transmit data?

A. IP Options

B. Urgent Pointer

C. IP Identification

D. Code Bits

Correct Answer: A