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

QUESTION 1

Mark works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network. Mark uses SmartDefense on the HTTP servers of the company to fix the limitation for the maximum response header length. Which of the following attacks can be blocked by defining this limitation?

A. HTR Overflow worms and mutations

B. Ramen worm attack

C. Melissa virus attack

D. Shoulder surfing attack

Correct Answer: A

QUESTION 2

Eve and Alice have the same 8 character password of "password" for their Linux accounts. A simplified entry from /etc/shadow is displayed below. Which of the following explains why their MD5 hashes are different?

Alice 1ZxCnCjhq$H1COX0aY6XZ4dVF.1Njux1

Eve 1IHLSRNty$kwokpFBzomNYph.ZVnHMv.

A. Unique salts were used to create each MD5 hash.

B. Passwords are encrypted using the user\\'s name and PID prior to hashing.

C. The accounts were created at different times.

D. The algorithm inserts random characters into the passphrases after hashing.

Correct Answer: A

Salts are used in Linux password hashing. In this example, the IHLSRNty value is the salt for Eve\\'s account and the ZxCnCjhq value is used to salt Alice\\'s account. When unique, randomly generated salts are added to the password prior to hashing the MD5 sums will be different. The time the accounts were created does not have modify the value of the hashes it only allows for a different random salt to be created. The MD5 generating algorithm also does not use the user name or PID during the hashing and thought the values of the salt are random, they are not inserted into the passphrase after it is hashed.

QUESTION 3

Which of the following viruses/worms uses the buffer overflow attack?

A. Chernobyl (CIH) virus

B. Nimda virus

C. Klez worm

D. Code red worm

Correct Answer: D

QUESTION 4

A server was infected by malware and controlled by an attacker for six months. The server was recovered and returned to production. Which of the following would provide the most effective information to build a post-incident monitoring service for this server?

A. A root cause analysis of the vector and methods of attack

B. The network and host firewall rules in place when the attack began

C. The operating system files installed on the server

D. The Acceptable Use policy and a list of organization-tested applications

Correct Answer: A

The attacker will likely try to return through the same channels he tried initially ?so a good place to start for a monitoring service is to review the root cause of the attack, and create signatures for those IOCs or artifacts. Using the baseline operating system would generate many false positives.

QUESTION 5

What is the third step in the three-way handshake?

A. FIN

B. ACK

C. SYN-ACK

D. SYN

Correct Answer: B