効果的なGCIHテスト模擬問題集試験-試験の準備方法-真実的なGCIH最新受験攻略

P.S. JPNTestがGoogle Driveで共有している無料かつ新しいGCIHダンプ：https://drive.google.com/open?id=1rCwBuNNpUawht1xsI6hhB7OD0QnrU_tB

きみはGIACのGCIH認定テストに合格するためにたくさんのルートを選択肢があります。JPNTestは君のために良い訓練ツールを提供し、君のGIAC認証試に高品質の参考資料を提供しいたします。あなたの全部な需要を満たすためにいつも頑張ります。

GCIH認定は、インシデントハンドリングとレスポンスを担当するプロフェッショナル、セキュリティアナリスト、インシデントレスポンダー、ネットワーク管理者、およびITセキュリティマネージャーを対象としています。この認定は、個人がセキュリティインシデントを検出、対応、回復するために必要な技術的スキルと知識、およびインシデント対応計画を開発および実装する能力を持っていることを示します。

GCIH認定プログラムは、情報セキュリティの分野の主要な組織の1つであるGlobal Information Assurance Certification（GIAC）によって提供されています。 GCIH試験は、インシデント対応と管理、ネットワークセキュリティ、マルウェア分析、デジタルフォレンジックなど、インシデント処理のさまざまな分野で候補者の知識をテストするように設計されています。認定プログラムは、世界中の企業や組織によって認識されており、GCIH認定の専門家は情報セキュリティ業界で高い需要があります。

>> GCIHテスト模擬問題集 <<

GCIH最新受験攻略 & GCIH勉強の資料

研究により、学習への関心を刺激することが最善の解決策であることがわかっています。したがって、GCIH準備ガイドの焦点は、GCIH試験の準備方法を変更することにより、厳格で無駄なメモリモードを改革することです。 GCIH実践教材のソフトバージョンは、知識と最新テクノロジーを組み合わせて学習力を大幅に刺激します。楽しい学習シーンと鮮明な説明をシミュレートすることにより、ユーザーは資格のあるGCIH試験に合格する自信が大きくなります。

GIAC GCIH（GIAC Certified Incident Handler）試験は、個人がセキュリティインシデントを検出、対応、解決する能力とスキルを検証する専門認定です。この認定は、組織内でセキュリティインシデントを管理および対応する責任がある専門家向けに設計されています。GIAC GCIH試験では、インシデント処理プロセス、ネットワークプロトコル、マルウェア解析、およびフォレンジック分析など、幅広いトピックがカバーされます。

GIAC Certified Incident Handler 認定 GCIH 試験問題 (Q206-Q211):

質問 # 206
Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The

packet is correctly encrypted and Adam assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs.
Which of the following types of attack is Adam performing?

- A. Network injection attack
- B. Replay attack
- C. MAC Spoofing attack
- D. Caffe Latte attack

正解：B

質問 # 207
Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

- A. Buffer overflow attack
- B. Evasion attack
- C. Ping of death attack
- D. Denial-of-Service (DoS) attack

正解：A

質問 # 208
John, a part-time hacker, has accessed in unauthorized way to the www.yourbank.com banking Website and stolen the bank account information of its users and their credit card numbers by using the SQL injection attack. Now, John wants to sell this information to malicious person Mark and make a deal to get a good amount of money. Since, he does not want to send the hacked information in the clear text format to Mark; he decides to send information in hidden text. For this, he takes a steganography tool and hides the information in ASCII text by appending whitespace to the end of lines and encrypts the hidden information by using the IDEA encryption algorithm. Which of the following tools is John using for steganography?

- A. 2Mosaic
- B. Image Hide
- C. Snow.exe
- D. Netcat

正解：C

質問 # 209
Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer.
After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting.
for ((i = 0;i<11;i++)); do
dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done
Which of the following actions does Adam want to perform by the above command?

- A. Infecting the hard disk with polymorphic virus strings.
- B. Wiping the contents of the hard disk with zeros.
- C. Deleting all log files present on the system.
- D. Making a bit stream copy of the entire hard disk for later download.

正解：B

質問 # 210
You enter the following URL on your Web browser:
http://www.we-are-secure.com/scripts/..%co%af../..%co%

af../windows/system32/cmd.exe?/c+dir+c:\
What kind of attack are you performing?

- A. URL obfuscating
- B. Directory traversal
- C. Session hijacking
- D. Replay

正解：B

質問 # 211
.....