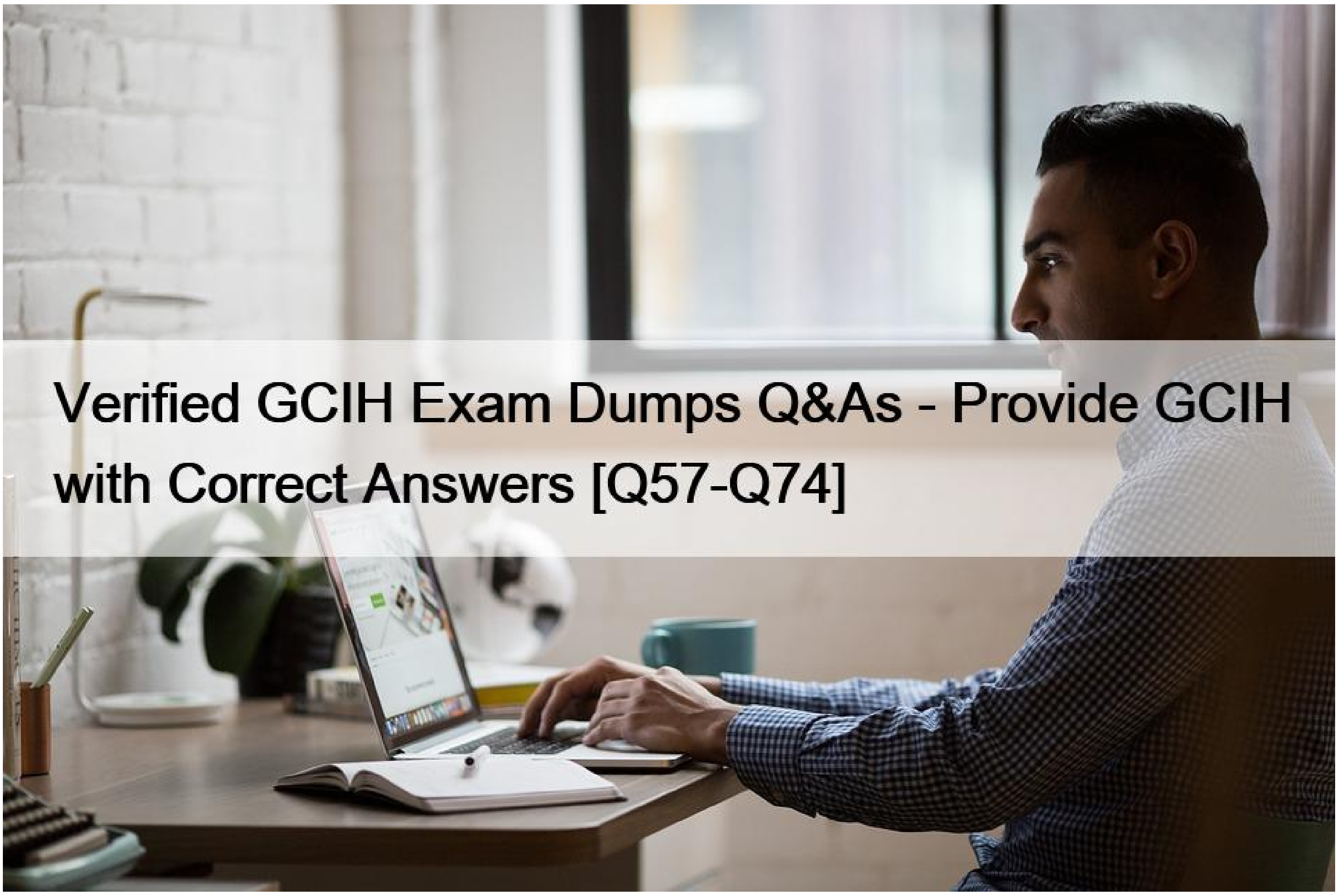
Verified GCIH Exam Dumps Q&As - Provide GCIH with Correct Answers [Q57-Q74


Verified GCIH Exam Dumps Q&As - Provide GCIH with Correct Answers [Q57-Q74]

Verified GCIH Exam Dumps Q&As - Provide GCIH with Correct Answers
Pass Your GCIH Dumps Free Latest GIAC Practice Tests

How to Prepare For GCIH Certification Exam **Preparation Guide for GCIH Certification Exam GCIH: Tips to survive if you don't have time to read all the page**

The GCIH certification is aimed at IT professionals who wish to demonstrate their competence and understanding of typical threats to corporate systems and networks. Workers who would benefit from getting GIAC GCIH certification are likely (or will be seeing for) workstations where information and skills to handle security incidents, understand common attack techniques, know that attack tools are required and how to defend themselves and react to such attacks when they occur.
According to payscale.com, there may be up to $ 100,000 in salary for GCIH certification holders depending on their professional title. You can expect from $ 50,000 to $ 150,000 in roles where a GCIH certification complements the daily professional activities of the owner. Typical job titles for qualified GCIH professionals include
Information Security Analyst
Security engineer Responsible
Information security
Network Administrator / Firewall
Applicants who wish to obtain the GCIH certification must pass an exam consisting of 150 multiple-choice questions. The time

allotted to complete the exam is 4 hours. The passing grade for the GCIH exam is 72%.

The exam is an ?open book?, which means that candidates can bring any printed note, textbooks and any other similar material they want to the exam center (please note that there may be a limited office or space working in the test area). Electronic devices such as smartphones, tablets, USB sticks or similar devices are not allowed in the test area. Applicants will not have access to search files such as Word, PDF and the like, or to open Internet access.

GCIH exams are monitored by Pearson VUE test facilities worldwide. Always check in advance with the nearest exam center to verify current exam costs and the availability of the GCIH exam.

Before setting an exam date, candidates must open an account with SANS / GIAC.

Certified Incident Handler masters have described their ability to handle security incidents by learning attack techniques, vectors, and traditional tools, properly defending and/or responding to such attacks when they occur. The GCIH certification focuses on the methods used to detect, respond and resolve cybersecurity incidents. The professionals in charge of GCIH are qualified for practical and leadership positions within the incident management teams.

Preparation Resources for GCIH Certification Test

A candidate who identifies and uses different preparation resources has a higher chance to pass the GIAC GCIH exam than one individual who doesn't do so. Therefore, those individuals who want to clear the GCIH test can use the following training resources: SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling This training course lasts for 6 days and it can be taken either online or in the classroom. It is conducted by Michael Murr as Principal Instructor and Joshua Wright as the Fellow. During this official class, the candidates will learn about the following concepts: - Preparing most effectively for preventing a security breach;- Developing reactive and preventive defense methods;- Identifying immediately any active attacks and knowing how to understand the compromises;- Understanding how to stop different types of the computer attack vector;- Developing different measures that block attackers from returning;- Learning how to recover from attacks and restoring the systems to avoid business disruptions;- Using and understanding how different types of hacking techniques and tools work;- Developing strategies that help in preventing any hacking attacks;- Discovering vulnerabilities, defenses, and attacks;- Understanding how to handle the legal issues when it comes to handling incidents.**GCIH GIAC Certified Incident Handler All-in-One Exam Guide, 1st Edition**This book has been written **by Nick Mitropoulos** and is available on Amazon in different formats. The candidates can download it in Kindle format for $34.67 or choose the paperback format for $36.49. This material helps you prepare for the challenging exam necessary for getting the GIAC Certified Incident Handler certification and offers detailed information according to the exam blueprint. To know more, the author is a reputable cybersecurity expert who knows the tips and tricks that the candidates should care about when they take the GCIH exam. Plus, such material includes 300 questions offering the exam-takers the opportunity to get used to the exam structure and difficulty level. In particular, this resource offers the candidates the opportunity to learn about the following topics: - How to handle incidents and intrusion analysis;- The way to gather different types of information;- How to identify vulnerabilities through scanning and enumeration;- Means to exploit vulnerabilities;- Preventing and defending against endpoint and infrastructure attacks;- Managing and defending against Network, Web application, and DoS attacks;- How to cover tracks and evade detection;- Learning how to work with botnets, bots, and worms.Another important advantage brought by this material is the fact that each chapter ends with a detailed explanation of the exam domains and puts the candidates in real-world scenarios. So, the exam-takers will consolidate their skills and obtain a lot of practical experience.

Candidates for GCIH Certification Exam

The GCIH test is intended for different categories of specialists such as the incident handlers or the leaders of incident handling teams. System administrators, security architects, or practitioners are also part of the groups of individuals targeted by this exam. Another group of candidates is formed by any individual who has a security-related role as the first responder and wants to leverage his/her skills in incident handling. Then, the GIAC GCIH certification evaluation is suitable for any professional who wants to validate his/her skills in detecting, responding, and finding solutions for any computer security issue and wants to learn how to work with different security tools. Besides, this test is dedicated to any specialists who want to understand different types of attack techniques alongside tools and want to know how to respond quickly and effectively whenever such an attack occurs.

NO.57 John works as a Network Administrator for We-are-secure Inc. He finds that TCP port 7597 of the Weare- secure server is open. He suspects that it may be open due to a Trojan installed on the server. He presents a report to the company describing the symptoms of the Trojan. A summary of the report is given below:

Once this Trojan has been installed on the computer, it searches Notpad.exe, renames it Note.com, and then copies itself to the computer as Notepad.exe. Each time Notepad.exe is executed, the Trojan executes and calls the original Notepad to avoid being noticed.

Which of the following Trojans has the symptoms as the one described above?
* NetBus
* Qaz
* eBlaster
* SubSeven

NO.58 You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?
* Tripwire
* SubSeven
* Netstat
* Fport

NO.59 Which of the following protocols uses only User Datagram Protocol (UDP)?
* POP3
* FTP
* ICMP
* TFTP
Section: Volume C

Explanation/Reference:

NO.60 James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the cause of the performance deterioration?
* Denial-of-Service
* Injection
* Internal attack
* Virus

NO.61 Which of the following is the difference between SSL and S-HTTP?
* SSL operates at the application layer and S-HTTP operates at the network layer.
* SSL operates at the application layer and S-HTTP operates at the transport layer.
* SSL operates at the network layer and S-HTTP operates at the application layer.
* SSL operates at the transport layer and S-HTTP operates at the application layer.
Section: Volume C

NO.62 You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise&#8217;s network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?
* Packet manipulation
* Denial-of-Service

* Spoofing
* Eavesdropping

NO.63 TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard

layer 4 network communications. The combination of parameters may then be used to infer the remote operating

system (OS fingerprinting), or incorporated into a device fingerprint.

Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?
* nmap -sS
* nmap -sU -p
* nmap -O -p
* nmap -sT

NO.64 In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?
* Dos
* DDoS
* Backscatter
* SQL injection

NO.65 Which of the following wireless network security solutions refers to an authentication process in which a user can

connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?
* Remote Authentication Dial-In User Service (RADIUS)
* IEEE 802.1x
* Wired Equivalent Privacy (WEP)
* Wi-Fi Protected Access 2 (WPA2)

NO.66 Which of the following can be used as a Trojan vector to infect an information system?

Each correct answer represents a complete solution. Choose all that apply.
* NetBIOS remote installation
* Any fake executable
* Spywares and adware
* ActiveX controls, VBScript, and Java scripts

Section: Volume B

NO.67 Fill in the blank with the appropriate term.

_______is the practice of monitoring and potentially restricting the flow of information outbound from one network to another.
Egress filtering

NO.68 Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc. Which of the following types of Cross-Site Scripting attack Ryan intends to do?
* Non persistent
* Document Object Model (DOM)
* SAX
* Persistent

Section: Volume A

NO.69 Which of the following attacks can be overcome by applying cryptography?

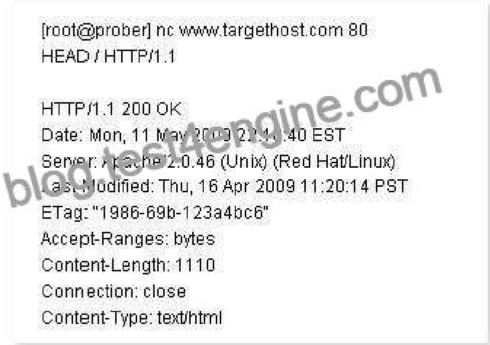
* Buffer overflow
* Web ripping
* Sniffing
* DoS

Section: Volume B

NO.70 Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker&#8217;s intentions?

* Internal attack
* Reconnaissance attack
* Land attack
* DoS attack

NO.71 John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a bad html request in order to retrieve information about the service on the host.



```
[root@prober] nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:14:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

blog.test4engine.com

Which of the following attacks is John using?

* Sniffing
* Eavesdropping
* War driving
* Banner grabbing

Section: Volume C

NO.72 Brutus is a password cracking tool that can be used to crack the following authentications:

l HTTP (Basic Authentication)

l HTTP (HTML Form/CGI)

l POP3 (Post Office Protocol v3)

l FTP (File Transfer Protocol)

l SMB (Server Message Block)

l Telnet

Which of the following attacks can be performed by Brutus for password cracking?

Each correct answer represents a complete solution. Choose all that apply.
* Hybrid attack
* Replay attack
* Dictionary attack
* Brute force attack
* Man-in-the-middle attack
Section: Volume C

NO.73 Which of the following US Acts emphasized a &#8220;risk-based policy for cost-effective security&#8221; and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency&#8217;s information security program and report the results to Office of Management and Budget?
* The Electronic Communications Privacy Act of 1986 (ECPA)
* The Fair Credit Reporting Act (FCRA)
* The Equal Credit Opportunity Act (ECOA)
* Federal Information Security Management Act of 2002 (FISMA)

NO.74 Which of the following threats is a combination of worm, virus, and Trojan horse characteristics?
* Spyware
* Heuristic
* Blended
* Rootkits
Section: Volume C

Get Top-Rated GIAC GCIH Exam Dumps Now: https://www.test4engine.com/GCIH_exam-latest-braindumps.html]