[Q193-Q217 Best Quality GIAC GCIH Exam Questions VCEPrep Realistic Practice Exams [2022
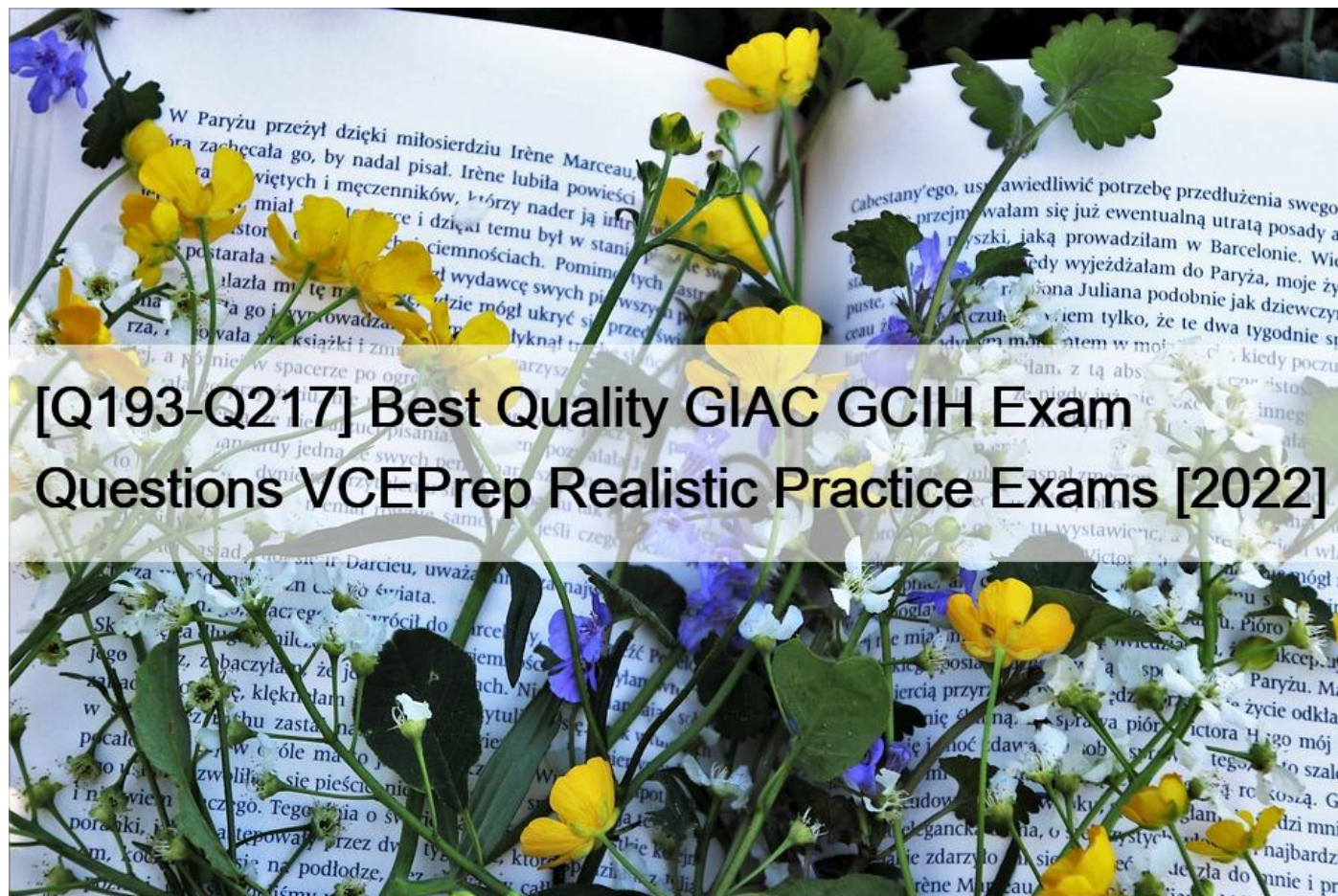

Best Quality GIAC GCIH Exam Questions VCEPrep Realistic Practice Exams [2022]
Critical Information To GIAC Certified Incident Handler Pass the First Time

GCIH Certification Path

There are no prerequisites

Topics of GCIH Exam

Candidates must know the exam topics before they start of preparation. Because it will really help them in hitting the core. Our **GCIH exam dumps** will include the following topics:

- Client Attacks- Session Hijacking and Cache Poisoning- Worms, Bots & Bot-Nets- Network Attacks- Denial of Service Attacks- Worms, Bots & Bot-Nets- Incident Handling: Eradication, Recovery, and Lessons Learned- Scanning: Discovery and Mapping- Techniques for maintaining access- Overflow Attacks **NO.193** Which of the following types of rootkits replaces regular application binaries with Trojan fakes and modifies the behavior of existing applications using hooks, patches, or injected code?

* Application level rootkit

* Hypervisor rootkit

* Kernel level rootkit

* Boot loader rootkit

NO.194 You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linux-based server. Recently,

you have updated the password policy of the company in which the server will disable passwords after four trials.

What type of attack do you want to stop by enabling this policy?
* Brute force
* Replay
* XSS
* Cookie poisoning

NO.195 Which of the following threats is a combination of worm, virus, and Trojan horse characteristics?
* Spyware
* Heuristic
* Blended
* Rootkits

NO.196 A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a

computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers

perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS

attack are as follows:

* Saturation of network resources

* Disruption of connections between two computers, thereby preventing communications between services

* Disruption of services to a specific computer

* Failure to access a Web site

* Increase in the amount of spam

Which of the following can be used as countermeasures against DoS attacks?

Each correct answer represents a complete solution. Choose all that apply.
* Blocking undesired IP addresses
* Applying router filtering
* Disabling unneeded network services
* Permitting network access only to desired traffic

NO.197 You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing.

Recently, your company has assigned you a project to test the security of the we-aresecure.com Web site.

For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping
tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every

query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.

What may be the reason?
* The firewall is blocking the scanning process.
* The zombie computer is not connected to the we-are-secure.com Web server.
* The zombie computer is the system interacting with some other system besides your computer.
* Hping does not perform idle scanning.

NO.198 Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. What steps can be used as a countermeasure of ARP spoofing?

Each correct answer represents a complete solution. Choose all that apply.
* Using smash guard utility
* Using ARP Guard utility
* Using static ARP entries on servers, workstation and routers
* Using ARP watch utility
* Using IDS Sensors to check continually for large amount of ARP traffic on local subnets
Section: Volume B

NO.199 Which of the following statements are true about a keylogger?

Each correct answer represents a complete solution. Choose all that apply.
* It records all keystrokes on the victim’s computer in a predefined log file.
* It can be remotely installed on a computer system.
* It is a software tool used to trace all or specific activities of a user on a computer.
* It uses hidden code to destroy or scramble data on the hard disk.

NO.200 You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the

events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise

network. Which of the following phases of the Incident handling process should you follow next to handle this

incident?
* Containment
* Preparation
* Recovery
* Identification

NO.201 Which of the following types of attacks come under the category of hacker attacks?

Each correct answer represents a complete solution. Choose all that apply.
* Smurf
* IP address spoofing
* Teardrop
* Password cracking

NO.202 Firekiller 2000 is an example of a _____.

* Security software disabler Trojan
* DoS attack Trojan
* Data sending Trojan
* Remote access Trojan

NO.203 Which of the following tools can be used as penetration tools in the Information system auditing process?

Each correct answer represents a complete solution. Choose two.
* Nmap
* Snort
* SARA
* Nessus

NO.204 Which of the following statements about reconnaissance is true?
* It describes an attempt to transfer DNS zone data.
* It is a computer that is used to attract potential intruders or attackers.
* It is any program that allows a hacker to connect to a computer without going through the normal authentication

process.
* It is also known as half-open scanning.

NO.205 John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-

secure.com. On the We-are-secure login page, he enters =’or”=’ as a username and successfully logs in to the user

page of the Web site. The We-are-secure login page is vulnerable to a _____.
* Dictionary attack
* SQL injection attack
* Replay attack
* Land attack

NO.206 Which of the following protocol loggers is used to detect ping sweep?
* lppi
* pitl
* dpsl
* ippl

NO.207 Which of the following statements about buffer overflow is true?
* It manages security credentials and public keys for message encryption.
* It is a collection of files used by Microsoft for software updates released between major service pack releases.
* It is a condition in which an application receives more data than it is configured to accept.
* It is a false warning about a virus.

NO.208 You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linux-based server.

Recently, you have updated the password policy of the company in which the server will disable passwords after four trials. What type of attack do you want to stop by enabling this policy?
* Brute force
* Replay

* XSS
* Cookie poisoning
Section: Volume B

Explanation/Reference:

NO.209 John 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 of the company. On the HTTP servers of

the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks

can be prevented by dropping the user-defined URLs?
* Morris worm
* Code red worm
* Hybrid attacks
* PTC worms and mutations

NO.210 Which of the following attacks come under the category of layer 2 Denial-of-Service attacks?

Each correct answer represents a complete solution. Choose all that apply.
* Spoofing attack
* SYN flood attack
* Password cracking
* RF jamming attack
Section: Volume A

Explanation/Reference:

NO.211 Against which of the following does SSH provide protection?

Each correct answer represents a complete solution. Choose two.
* DoS attack
* IP spoofing
* Password sniffing
* Broadcast storm

NO.212 You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of

various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the

Web site login page and you run the following SQL query:

SELECT email, passwd, login_id, full_name

FROM members

WHERE email = ‘attacker@somehwere.com’; DROP TABLE members; –‘

What task will the above SQL query perform?

* Deletes the database in which members table resides.
* Deletes the rows of members table where email id is ‘attacker@somehwere.com’ given.
* Performs the XSS attacks.
* Deletes the entire members table.

NO.213 Which of the following is spy software that records activity on Macintosh systems via snapshots, keystrokes, and Web site logging?
* Spector
* Magic Lantern
* eblaster
* NetBus

NO.214 Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?
* Spoofing
* Hacking
* SYN attack
* PING attack

NO.215 Which of the following systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?
* US Incident Management System (USIMS)
* National Disaster Management System (NDMS)
* National Emergency Management System (NEMS)
* National Incident Management System (NIMS)

NO.216 Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which

some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the

task:

1. Smoothening and decreasing contrast by averaging the pixels of the area where significant

color transitions occurs.

2. Reducing noise by adjusting color and averaging pixel value.

3. Sharpening, Rotating, Resampling, and Softening the image.

Which of the following Steganography attacks is Victor using?
* Stegdetect Attack
* Chosen-Stego Attack
* Steg-Only Attack
* Active Attacks

NO.217 Which of the following tasks can be performed by using netcat utility?

Each correct answer represents a complete solution. Choose all that apply.
* Checking file integrity
* Creating a Backdoor

* Firewall testing
* Port scanning and service identification

GCIH EXAM DUMPS WITH GUARANTEED SUCCESS: https://www.vceprep.com/GCIH-latest-vce-prep.html]