GCIH$^{Q\&As}$

GIAC Certified Incident Handler

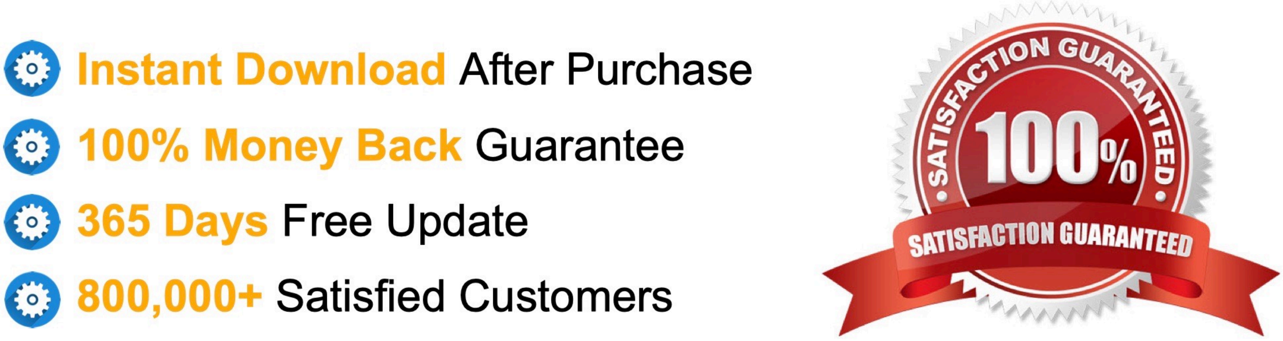
Pass GIAC GCIH Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which command will reveal the contents of slackspace.txt?

C:\> notepad C:\Users\tadams\Documents\GCIH_update.txt:slackspace.txt

A. C:\Users\tadams\Documents> notepad slackspace.txt

B. C:\> type "C:\Users\tadams\Documents\GCIH_update.txt:slackspace.txt"

C. C:\> more

D. C:\Users\tadams\Documents> tail slackspace.txt

Correct Answer: C

Slackspace.txt is an alternate data stream (ADS), a secondary file stream of GCIH_update.txt. The more command will reveal the text content of an ADS if the full path is used.

QUESTION 2

A company\\'s external DNS server was used by an attacker in a DDoS attack against a third party. Which of the following configurations should be changed to prevent this from happening again?

A. Disable recursive DNS queries on the server

B. Do not allow TCP to be used for large DNS queries

C. Require DNSSEC for DNS zone transfers

D. Remove the forward lookup zone on the server

Correct Answer: A

To launch an amplified DNS DoS attack, the bad guys first locate several DNS servers that will perform recursive look-ups on behalf of anyone on the Internet (a large majority of DNS servers have this configuration in the wild). Next, the attacker sends queries to those servers for a DNS record that the attacker controls on the attacker\\'s own DNS server. Because they are configured for recursion, these DNS servers send the request back to the attacker, who responds with a

4000-byte TXT record, which will be cached in the DNS servers that will be used for amplification.

DNSSEC for zone transfers, using TCP for large queries and forward lookup zones do not make a DNS server vulnerable or useful in launching DNS attacks of this nature.

QUESTION 3

Which of the following techniques can malware employ to avoid detection by honey ports installed on virtual machines?

A. The malware can detect the virtual machine by its MAC address and disables certain features

B. The malware can periodically move its host directory in order to evade file integrity monitoring

C. The malware can run under a new user that was previously unknown to the system

D. The malware can spawn a new process for VMware tools and disable the internal communications channel to the host

Correct Answer: A

If malware can detect a virtual machine environment, it may be designed to disable certain features to avoid detection. It may lay dormant or send a signal back to a command and control centre notifying that the host is a VM. By creating new users, new processes or changing host directories, the tool may alert host based IDS or file integrity systems of its presence.

QUESTION 4

Which of the following can be used to perform session hijacking?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Cross-site scripting

B. Session fixation

C. ARP spoofing

D. Session sidejacking

Correct Answer: ABD

QUESTION 5

How would a worm be able to affect hosts running different operating systems be classified?

A. Zero-Day Worm

B. Multi-Platform Worm

C. Polymorphic Worm

D. Fast Flux Worm

Correct Answer: B

While not mainstream (yet), we have already seen a small number of multi-platform worms released against the Internet. For example, in May 2001, the Sadmind/IIS worm mushroomed through the Internet, targeting Sun Solaris and Microsoft

Windows.

Other types of worm classifications or characteristics, such as zero-day, polymorphic and fast flux, do not meet this definition.