GCED[Q&As]

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

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

https://www.geekcert.com/gced.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

QUESTION 1

If a Cisco router is configured with the "service config" configuration statement, which of the following tools could be used by an attacker to apply a new router configuration?

A. TFTPD

B. Hydra

C. Ettercap

D. Yersinia

Correct Answer: A

QUESTION 2

Which action would be the responsibility of the First Responder once arriving at the scene of a suspected incident as part of a Computer Security Incident Response Plan (CSIRP)?

A. Making the decision of whether or not to notify law enforcement on behalf of the organization.

B. Performing timeline creation on the system files in order to identify and remove discovered malware.

C. Copying critical data from suspected systems to known good systems so productivity is not affected by the investigation.

D. Conducting initial interviews and identifying the systems involved in the suspected incident.

Correct Answer: D

Explanation: The First Responder plays a critical role in the Incident Response process on the CSIRT

(Computer Security Incident Response Team).

Here is a list of some typical responder tasks:

Make sure that the correct system is identified and photograph the scene, if necessary.

Conduct an initial interview (not an interrogation) of any witnesses.

The decision to notify law enforcement requires explicit approval and direction form management and/or

counsel. While a First Responder may collect initial data while minimally intruding on the system, no major

changes, or indepth media analysis should be performed by the First Responder when initially responding

to a suspected incident.

QUESTION 3

Which of the following applies to newer versions of IOS that decrease their attack surface?

A. Telnet cannot be enabled or used

B. The Cisco Discovery Protocol has been removed

C. More services are disabled by default

D. Two-factor authentication is default required

Correct Answer: C

Explanation: Recent versions of IOS have less services enabled by default, older versions vary but generally have more services (even those not needed) enabled by default; this increases the attack surface on the device.

QUESTION 4

Which of the following is a major problem that attackers often encounter when attempting to develop or use a kernel mode rootkit?

A. Their effectiveness depends on the specific applications used on the target system.

B. They tend to corrupt the kernel of the target system, causing it to crash.

C. They are unstable and are easy to identify after installation

D. They are highly dependent on the target OS.

Correct Answer: B

QUESTION 5

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

Correct Answer: A

Explanation: By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

QUESTION 6

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command? C:\ >dir / s / a dhsra d: \ > a: \ IRCD.txt

A. To create a file on the USB drive that contains a listing of the C: drive

B. To show hidden and archived files on the C: drive and copy them to the USB drive

C. To copy a forensic image of the local C: drive onto the USB drive

D. To compare a list of known good hashes on the USB drive to files on the local C: drive

Correct Answer: C

Explanation: This command will create a text file on the collection media (in this case you would probably be using a USB flash drive) named IRCD.txt that should contain a recursive directory listing of all files on the desk.

QUESTION 7

When identifying malware, what is a key difference between a Worm and a Bot?

A. A Worm gets instructions from an external control channel like an IRC server.

B. A Worm, unlike a Bot, is installed silently as an add-on to a legitimate program.

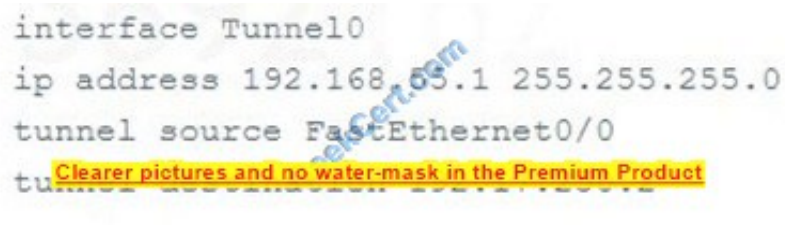
C. A Bot, unlike a Worm, is frequently spread through email attachments.

D. A Bot gets instructions from an external control channel like an IRC server.

Correct Answer: D

QUESTION 8

How would an attacker use the following configuration settings?



A. A client based HIDS evasion attack

B. A firewall based DDoS attack

C. A router based MITM attack

D. A switch based VLAN hopping attack

Correct Answer: C

QUESTION 9

Which of the following attacks would use ".." notation as part of a web request to access restricted files and directories, and possibly execute code on the web server?

A. URL directory

B. HTTP header attack

C. SQL injection

D. IDS evasion

E. Cross site scripting

Correct Answer: A

QUESTION 10

How does data classification help protect against data loss?

A. DLP systems require classification in order to protect data

B. Data at rest is easier to protect than data in transit

C. Digital watermarks can be applied to sensitive data

D. Resources and controls can be appropriately allocated

Correct Answer: A

QUESTION 11

What is the most common read-only SNMP community string usually called?

A. private

B. mib

C. open

D. public

Correct Answer: D

QUESTION 12

Which could be described as a Threat Vector?

A. A web server left6 unpatched and vulnerable to XSS

B. A coding error allowing remote code execution

C. A botnet that has infiltrated perimeter defenses

D. A wireless network left open for anonymous use

Correct Answer: A

A threat vector is the method (crafted packet) that would be used to exercise a vulnerability (fragmentation to bypass IDS signature). An unpatched web server that is susceptible to XSS simply describes a vulnerability (unpatched) paired with a specific threat (XSS) and does not touch on the method to activate the threat. Similarly, the coding error that allows remote code execution is simply describing the pairing of a vulnerability with a threat, respectively. The botnet is an unspecified threat; there is no indication of how the threat was activated (or it\\'s intention/capabilities; the threat).

QUESTION 13

What attack was indicated when the IDS system picked up the following text coming from the Internet to

the web server?

select user, password from user where user= "jdoe" and password= `myp@55!\\' union select "text",2 into

outfile "/tmp/file1.txt" - - \\'

A. Remote File Inclusion

B. URL Directory Traversal

C. SQL Injection

D. Binary Code in HTTP Headers

Correct Answer: C

Explanation: An example of manipulating SQL statements to perform SQL injection includes using the

semi-colon to perform multiple queries. The following example would delete the users table:

Username: ` or 1=1; drop table users; - Password: [Anything]

QUESTION 14

Why might an administrator not be able to delete a file using the Windows del command without specifying additional command line switches?

A. Because it has the read-only attribute set

B. Because it is encrypted

C. Because it has the nodel attribute set

D. Because it is an executable file

Correct Answer: A

QUESTION 15

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

Correct Answer: A

GCED PDF Dumps GCED Exam Questions GCED Braindumps

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

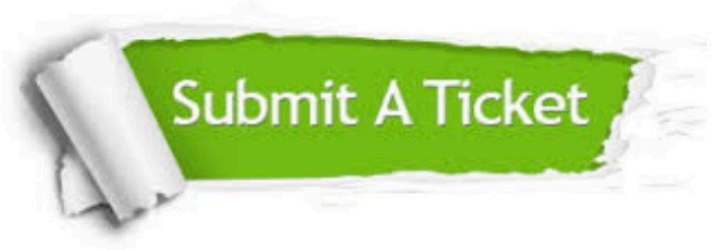
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.geekcert.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © geekcert, All Rights Reserved.