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.certbus.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

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 2

An incident response team is handling a worm infection among their user workstations. They created an

IPS signature to detect and block worm activity on the border IPS, then removed the worm\\'s artifacts or

workstations triggering the rule.

Despite this action, worm activity continued for days after. Where did the incident response team fail?

A. The team did not adequately apply lessons learned from the incident

B. The custom rule did not detect all infected workstations

C. They did not receive timely notification of the security event

D. The team did not understand the worm\\'s propagation method

Correct Answer: B

Explanation: Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didn\\'t detect all the infected workstations.

QUESTION 3

The creation of a filesystem timeline is associated with which objective?

A. Forensic analysis

B. First response

C. Access control

D. Incident eradication

Correct Answer: A

QUESTION 4

In order to determine if network traffic adheres to expected usage and complies with technical standards, an organization would use a device that provides which functionality?

A. Stateful packet filtering

B. Signature matching

C. Protocol anomaly detection

D. CRC checking

E. Forward error correction

Correct Answer: C

Explanation: In addition to standards compliance, Protocol Anomaly Detection determines whether data within the protocol adheres to expected usage. Even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be inconsistent with what is expected. Perimeter devices that perform protocol anomaly detection contain in-depth knowledge of protocol standards and expected usage and are able to detect traffic that does not comply with those guidelines.

QUESTION 5

Which of the following tools is the most capable for removing the unwanted add-on in the screenshot below?

A. ProcessExplorer

B. Taskkill

C. Paros

D. Hijack This

Correct Answer: B

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

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

A. ARP cache poisoning

B. CDP sniffing

C. SNMP man in the middle

D. TFTP brute force

Correct Answer: D

Explanation: TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.

QUESTION 8

What piece of information would be recorded by the first responder as part of the initial System Description?

A. Copies of log files

B. System serial number

C. List of system directories

D. Hash of each hard drive

Correct Answer: B

QUESTION 9

An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?

A. They did not eradicate tools left behind by the attacker

B. They did not properly identify the source of the breach

C. They did not lock the account after changing the password

D. They did not patch the database server after the event

Correct Answer: D

QUESTION 10

An analyst will capture traffic from an air-gapped network that does not use DNS. The analyst is looking for unencrypted Syslog data being transmitted. Which of the following is most efficient for this purpose?

A. tcpdump –s0 –i eth0 port 514

B. tcpdump –nnvvX –i eth0 port 6514

C. tcpdump –nX –i eth0 port 514

D. tcpdump –vv –i eth0 port 6514

Correct Answer: B

When using tcpdump, a –n switch will tell the tool to not resolve hostnames; as this network makes no use of DNS this is efficient. The –vv switch increases the tools output verbosity. The –s0 increases the snaplength to “all” rather than the default of 96 bytes. The –nnvvX would make sense here except that the port in the filter is 6514 which is the default port for encrypted Syslog transmissions.

QUESTION 11

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 12

You have been tasked with searching for Alternate Data Streams on the following collection of Windows partitions; 2GB FAT16, 6GB FAT32, and 4GB NTFS. How many total Gigabytes and partitions will you need to search?

A. 4GBs of data, the NTFS partition only.

B. 12GBs of data, the FAT16, FAT32, and NTFS partitions.

C. 6GBs of data, the FAT32 partition only.

D. 10GBs of data, both the FAT32 and NTFS partitions.

Correct Answer: C

QUESTION 13

Network administrators are often hesitant to patch the operating systems on CISCO router and switch operating systems, due to the possibility of causing network instability, mainly because of which of the following?

A. Having to rebuild all ACLs

B. Having to replace the kernel

C. Having to re-IP the device

D. Having to rebuild ARP tables

E. Having to rebuild the routing tables

Correct Answer: B

Explanation: Many administrators are hesitant to upgrade the IOS on routers based on past experience with the code introducing instability into the network. It is often difficult to completely test an IOS software upgrade in a production environment because the monolithic kernel requires that the IOS be replaced before the device can be tested. Because of these reasons, IOS upgrades to resolve security flaws are often left undone in many organizations.

QUESTION 14

When an IDS system looks for a pattern indicating a known worm, what type of detection method is it using?

A. Signature-based

B. Anomaly-based

C. Statistical

D. Monitored

Correct Answer: A

QUESTION 15

An outside vulnerability assessment reveals that users have been routinely accessing Gmail from work for over a year, a clear violation of this organization\\'s security policy. The users report "it just started working one day". Later, a network administrator admits he meant to unblock Gmail for just his own IP address, but he made a mistake in the firewall rule.

Which security control failed?

A. Access control

B. Authentication

C. Auditing

D. Rights management

Correct Answer: C

Explanation: Audits are used to identify irregular activity in logged (after-the-fact) records. If this activity went unnoticed or uncorrected for over a year, the internal audits failed because they were either incomplete or inaccurate. Authentication, access control and managing user rights would not apply as a network admin could be expected to have the ability to configure firewall rules.