Free Questions for GCED by braindumpscollection

Shared by Mclean on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Copies of log files

B- System serial number

C- List of system directories

D- Hash of each hard drive

Answer:

B

Question 2

Question Type: MultipleChoice

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?

Options:

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.

Answer:

C

Question 3

Question Type: **MultipleChoice**

In an 802.1x deployment, which of the following would typically be considered a Supplicant?

Options:

A- A network switch

B- A perimeter firewall

C- A RADIUS server

D- A client laptop

Answer:

D

Question 4

Question Type: **MultipleChoice**

Although the packet listed below contained malware, it freely passed through a layer 3 switch. Why didn't the switch detect the malware in this packet?

```
0000 00 17 a4 99 41 02 00 08 e3 ff fd 90 08 00 45 00 ....A.........E.
0010 01 0a f4 73 40 00 3b 06 96 dd 92 39 f8 47 ac 19 ...s@.;....9.G..
0020 7d 02 00 50 08 6b 3c 57 60 4b 24 6f 77 53 50 18 }..P.k
0030 01 a1 05 1f 00 00 48 54 54 50 2f 31 2e 31 20 33 ......HTTP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not Modified.
0050 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 .Content-Type: a
0060 70 70 6c 69 63 61 74 69 6f 6e 2f 70 6b 69 78 2d pplication/pkix-
0070 63 72 6c 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 crl..Last-Modifi
0080 65 64 3a 20 4d 6f 6e 2c 20 31 37 20 4f 63 74 20 ed: Mon, 17 Oct
0090 32 30 31 32 20 31 37 3a 33 36 3a 33 33 20 47 4d 2012 17:36:33 GM
00a0 54 0d 0a 45 54 61 67 3a 20 22 37 38 62 33 33 35 T..ETag: "78b335
00b0 30 66 33 38 63 63 63 31 3a 30 22 0d 0a 43 61 63 0f38ccc1:0"..Cac
00c0 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d he-Control: max-
00d0 61 67 65 3d 39 30 30 0d 0a 44 61 74 65 3a 20 4d age=900..Date: M
00e0 6f 6e 2c 20 33 31 20 4f 63 74 20 32 30 31 32 20 on, 31 Oct 2012
00f0 31 34 3a 35 31 3a 34 32 20 47 4d 54 0d 0a 43 6f 14:51:42 GMT..Co
0100 6e 6e 65 63 74 69 6f 6e 3a 20 6d 61 6c 77 61 72 nnection: malwar
0110 65 2e 65 78 65 2e 2e 2e                         e.exe...
```

Options:

A- The packet was part of a fragmentation attack

B- The data portion of the packet was encrypted

C- The entire packet was corrupted by the malware

D- It didn't look deeply enough into the packet

Answer:

D

Explanation:

Routers, layer 3 switches, some firewalls, and other gateways are packet filtering devices that use access control lists (ACLs) and perform packet inspection. This type of device uses a small subset of the packet to make filtering decisions, such as source and destination IP address and protocol. These devices will then allow or deny protocols based on their associated ports. This type of packet inspection and access control is still highly susceptible to malicious attacks, because payloads and other areas of the packet are not being inspected. For example, application level attacks that are tunneled over open ports such as HTTP (port 80) and HTTPS (port 443).

Question 5

Question Type: MultipleChoice

A company classifies data using document footers, labeling each file with security labels "Public", "Pattern", or "Company Proprietary". A new policy forbids sending "Company Proprietary" files via email. Which control could help security analysis identify breaches of this policy?

Options:

A- Monitoring failed authentications on a central logging device

B- Enforcing TLS encryption for outbound email with attachments

C- Blocking email attachments that match the hashes of the company's classification templates

D- Running custom keyword scans on outbound SMTP traffic from the mail server

Answer:

D

Question 6

Question Type: **MultipleChoice**

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)?

Options:

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.

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 7

Question Type: MultipleChoice

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?

Options:

A- Access control

B- Authentication

C- Auditing

D- Rights management

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.

Question 8

Question Type: MultipleChoice

Which of the following is best defined as "anything that has the potential to target known or existing vulnerabilities in a system?"

Options:

A- Vector

B- Gateway

C- Threat

D- Exploit

Answer:

A

Question 9

Question Type: MultipleChoice

Throughout the week following a new IPS deployment, nearly every user on the protected subnet submits helpdesk tickets regarding network performance and not being able to access several critical resources. What is the most likely reason for the performance issues?

Options:

A- The incoming traffic is overflowing the device's TAP buffer

B- The in-line TAP experienced a hardware failure

C- The IPS sensor was changed from test mode to production mode

D- The IPS sensor was powered off or moved out of band

Answer:

A

Explanation:

When deploying an IPS, you should carefully monitor and tune your systems and be aware of the risks involved. You should also have an in-depth understanding of your network, its traffic, and both its normal and abnormal characteristics. It is always recommended to run IPS and active response technologies in test mode for a while to thoroughly understand their behavior.

If the IPS had been previously powered off the performance issues would have impacted all network traffic, not just critical resources, and the issue would have begun on day 1 of deployment.

A hardware failure of the TAP would bring connectivity to a stop, not just impact users access to critical resources.

If the IPS and/or TAP cannot keep up with traffic, the user's issues would have been more sporadic, rather than focused on a sudden loss to critical resources.