GIAC

Exam GCED

GIAC Certified Enterprise Defender

Version: 7.0

[Total Questions: 88]

Question No : 1

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

A. A network switch
B. A perimeter firewall
C. A RADIUS server
D. A client laptop

Answer: D

Question No : 2

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?

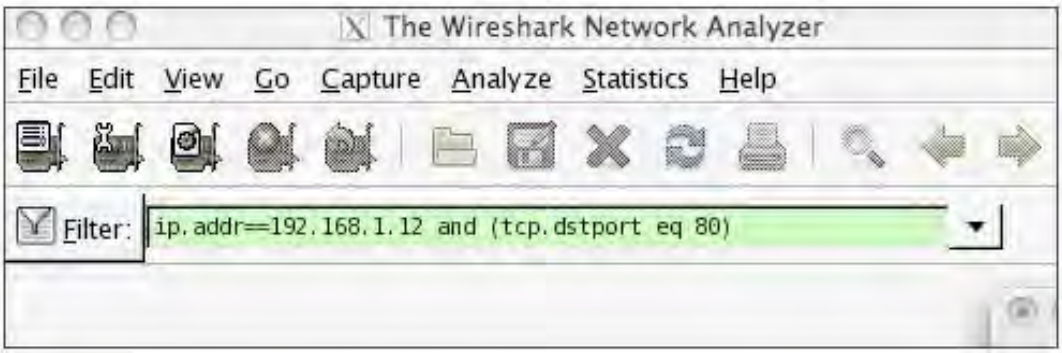
A. Access control
B. Authentication
C. Auditing
D. Rights management

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 No : 3

What information would the Wireshark filter in the screenshot list within the display window?



A. Only HTTP traffic to or from IP address 192.168.1.12 that is also destined for port 80
B. Only traffic to or from IP address 192.168.1.12 and destined for port 80
C. Only traffic with a source address of 192.168.1.12 to or from port 80
D. Only traffic with a destination address of 192.168.1.12 to or from port 80

Answer: B

Question No : 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.

Answer: B

Question No : 5

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?

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.

Question No : 6

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

Answer: A

Question No : 7

A legacy server on the network was breached through an OS vulnerability with no patch available. The server is used only rarely by employees across several business units. The theft of information from the server goes unnoticed until the company is notified by a third party that sensitive information has been posted on the Internet. Which control was the first to fail?

A. Security awareness
B. Access control
C. Data classification
D. Incident response

Answer: C

Explanation:

The legacy system was not properly classified or assigned an owner. It is critical that an organization identifies and classifies information so proper controls and measures should be put in place. The ultimate goal of data classification is to make sure that all information is properly protected at the correct level.

This was not a failure of incident response, access control or security awareness training.

Question No : 8

Following a Digital Forensics investigation, which of the following should be included in the final forensics report?

A. An executive summary that includes a list of all forensic procedures performed.
B. A summary of the verified facts of the incident and the analyst's unverified opinions.
C. A summary of the incident and recommended disciplinary actions to apply internally.

D. An executive summary that includes high level descriptions of the overall findings.

Answer: D

Explanation:

A professional forensic report should include an executive summary, including a description of the incident and the overall findings.

The written report needs to be factually accurate and free from speculation or bias, meaning that an analyst's unverified or unsubstantiated opinions should not be included in the report. Beyond the executive summary, the detailed report should include a description of the data preserved, a detailed explanation of the procedures performed, and a summary of the facts. Disciplinary action, if needed, would be addressed through other channels and not included in the forensic analyst's report.

Question No : 9

From a security perspective, how should the Root Bridge be determined in a Spanning Tree Protocol (STP) environment?

A. Manually selected and defined by the network architect or engineer.
B. Defined by selecting the highest Bridge ID to be the root bridge.
C. Automatically selected by the Spanning Tree Protocol (STP).
D. All switch interfaces become root bridges in an STP environment.

Answer: B

Question No : 10

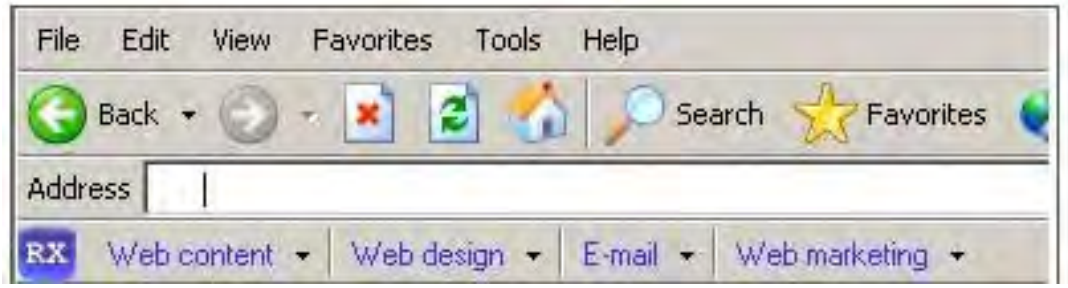
Which of the following would be used in order to restrict software form performing unauthorized operations, such as invalid access to memory or invalid calls to system access?

A. Perimeter Control
B. User Control
C. Application Control
D. Protocol Control
E. Network Control

Answer: C

Question No : 11

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

Answer: B

Question No : 12

Requiring background checks for employees who access protected data is an example of which type of data loss control?

A. Mitigation
B. Prevention
C. Monitoring
D. Identification

Answer: B

Explanation:

Once sensitive data is identified and classified, preventive measures can be taken. Among these are software-based controls, such as auditing and access control, as well as human controls such as background checks, psychological examinations, and such.

Question No : 13

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.

Answer: C

Question No : 14

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

Answer: B

Question No : 15

How would an attacker use the following configuration settings?

```
interface Tunnel0
ip address 192.168.55.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 192.17.250.2
```

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

Answer: C

Question No : 16

What would be the output of the following Google search?

filetype:doc inurl:ws_ftp

A. Websites running ws_ftp that allow anonymous logins
B. Documents available on the ws_ftp.com domain
C. Websites hosting the ws_ftp installation program
D. Documents found on sites with ws_ftp in the web address

Answer: D

Question No : 17

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

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 No : 18

Which tool keeps a backup of all deleted items, so that they can be restored later if need be?

A. ListDLLs
B. Yersinia
C. Ettercap
D. ProcessExplorer
E. Hijack This

Answer: E

Explanation:

After selecting “fix it!” with Hijack This you can always restore deleted items, because Hijack This keeps a backup of them.

Question No : 19