Free Questions for GCED by go4braindumps

Shared by Rutledge on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement below is the MOST accurate about insider threat controls?

Options:

A- Classification of information assets helps identify data to protect.

B- Security awareness programs have a minimal impact on reducing the insider threat.

C- Both detective and preventative controls prevent insider attacks.

D- Rotation of duties makes an insider threat more likely.

E- Separation of duties encourages one employee to control a great deal of information.

Answer:

A

Explanation:

A company needs to classify its information as a key step in valuing it and knowing where to focus its protection.

Rotation of duties and separation of duties are both key elements in reducing the scope of information access and the ability to conceal malicious behavior.

Separation of duties helps minimize "empire building" within a company, keeping one individual from controlling a great deal of information, reducing the insider threat.

Security awareness programs can help other employees notice the signs of an insider attack and thus reduce the insider threat.

Detection is a reactive method and only occurs after an attack occurs. Only preventative methods can stop or limit an attack.

Question 2

Question Type: **MultipleChoice**

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

Options:

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 3

Question Type: MultipleChoice

A compromised router is reconfigured by an attacker to redirect SMTP email traffic to the attacker's server before sending packets on to their intended destinations. Which IP header value would help expose anomalies in the path outbound SMTP/Port 25 traffic takes compared to outbound packets sent to other ports?

Options:

A- Checksum

B- Acknowledgement number

C- Time to live

D- Fragment offset

Answer:

C

Explanation:

In a case study of a redirect tunnel set up on a router, some anomalies were noticed while watching network traffic with the TCPdump packet sniffer.

Packets going to port 25 (Simple Mail Transfer Protocol [SMTP] used by mail servers and other Mail Transfer Agents [MTAs] to send and receive e-mail) were apparently taking a different network path. The TLs were consistently three less than other destination ports, indicating another three network hops were taken.

Other IP header values listed, such as fragment offset. The acknowledgement number is a TCP, not IP, header field.

Question 4

Question Type: MultipleChoice

What is needed to be able to use taskkill to end a process on remote system?

Options:

A- Svchost.exe running on the remote system

B- Domain login credentials

C- Port 445 open

D- Windows 7 or higher on both systems

Answer:

B

Explanation:

Domain login credentials are needed to kill a process on a remote system using taskkill.

Question 5

Question Type: MultipleChoice

What are Browser Helper Objects (BHO)s used for?

Options:

A- To provide multi-factor authentication support for Firefox

B- To provide a more feature-rich interface for Internet Explorer

C- To allow Internet Explorer to process multi-part URLs

D- To allow Firefox to process JavaScript in a sandbox

Answer:

B

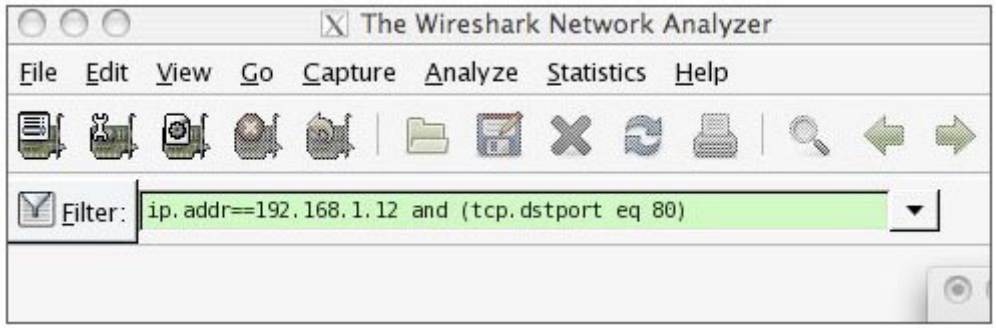
Explanation:

When scanning your system, you may notice many BHOs since they are widely used by software developers to provide a more feature rich interface for Microsoft Internet Explorer.

Question 6

Question Type: MultipleChoice

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



Options:

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 7

Question Type: MultipleChoice

What would the output of the following command help an incident handler determine?

cscript manage-bde . wsf --status

Options:

A- Whether scripts can be run from the command line

B- Which processes are running on the system

C- When the most recent system reboot occurred

D- Whether the drive has encryption enabled

Answer:

D