Free Questions for 350-201 by dumpshq

Shared by Acevedo on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

Options:

A- Mask PAN numbers

B- Encrypt personal data

C- Encrypt access

D- Mask sales details

Answer:

B

Question 2

Question Type: MultipleChoice

What is the purpose of hardening systems?

Options:

A- to securely configure machines to limit the attack surface

B- to create the logic that triggers alerts when anomalies occur

C- to identify vulnerabilities within an operating system

D- to analyze attacks to identify threat actors and points of entry

Answer:

A

Question 3

Question Type: DragDrop

Refer to the exhibit.

into

Answer Area

Answer:

Execute rapid threat containment	Step 1
Investigate and classify the exposure	Step 2
Investigate infected hosts	Step 3
Search for infected hosts	Step 4

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

Which asset has the highest risk value?

Options:

A- servers

B- website

C- payment process

D- secretary workstation

Answer:

C

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

An employee is a victim of a social engineering phone call and installs remote access software to allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee's laptop and the remote technician's system?

Options:

A- No database files were disclosed

B- The database files were disclosed

C- The database files integrity was violated

D- The database files were intentionally corrupted, and encryption is possible

Answer:

C

Question 6

Question Type: MultipleChoice

A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

Options:

A- DDoS attack

B- phishing attack

C- virus outbreak

D- malware outbreak

Answer:

D

Question 7

Question Type: MultipleChoice

A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The

hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

Options:

A- Run and analyze the DLP Incident Summary Report from the Email Security Appliance

B- Ask the company to execute the payload for real time analysis

C- Investigate further in open source repositories using YARA to find matches

D- Obtain a copy of the file for detonation in a sandbox

Answer:

D

Question 8

Question Type: MultipleChoice

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

Options:

A- Run the sudo sysdiagnose command

B- Run the sh command

C- Run the w command

D- Run the who command

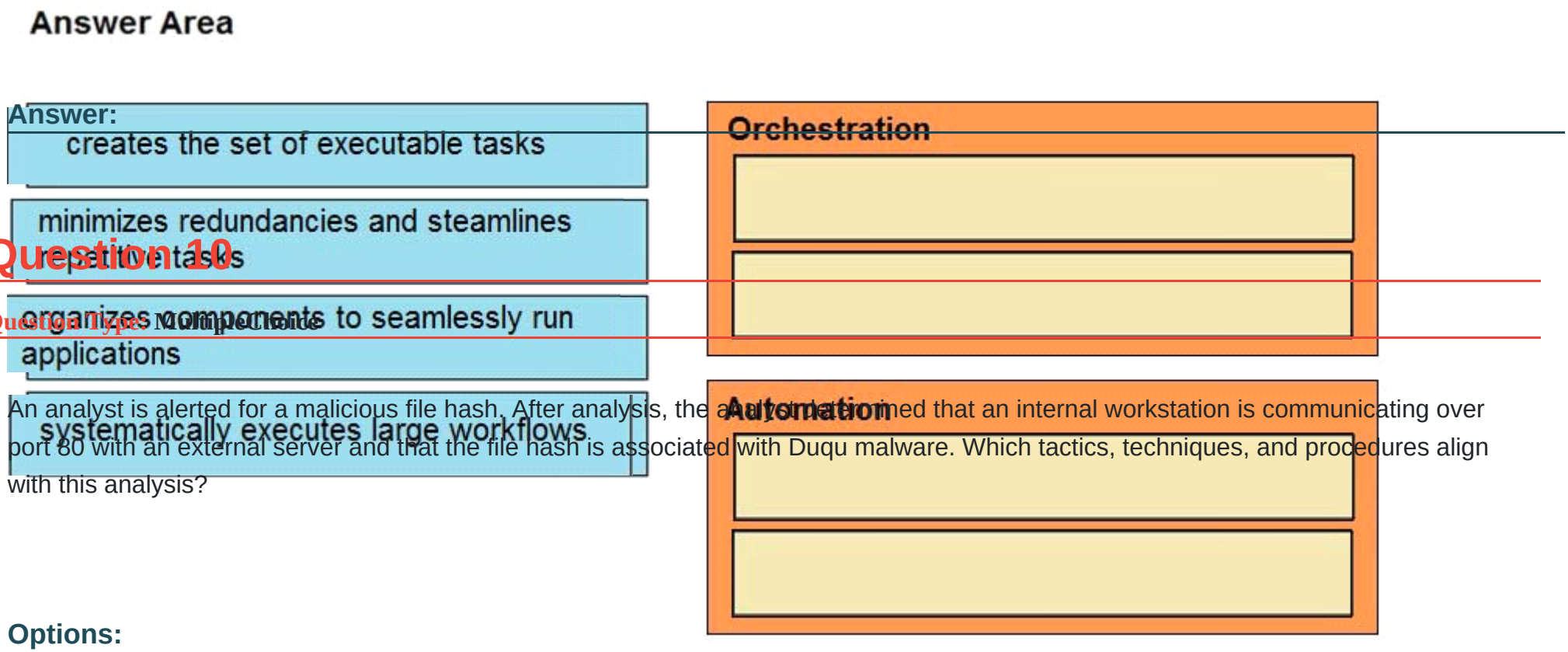
Answer:

A

Question 9

Question Type: DragDrop

Drag and drop the function on the left onto the mechanism on the right.



Question 10

Question Type: Multiple Choice

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

Options:

A- Command and Control, Application Layer Protocol, Duqu

B- Discovery, Remote Services: SMB/Windows Admin Shares, Duqu

C- Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu

D- Discovery, System Network Configuration Discovery, Duqu

Answer:

A

Question 11

Question Type: MultipleChoice

An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

Options:

A- Utilize the SaaS tool team to gather more information on the potential breach

B- Contact the incident response team to inform them of a potential breach

C- Organize a meeting to discuss the services that may be affected

D- Request that the purchasing department creates and sends the payments manually

Answer:

A