# Free Questions for 300-215 by vceexamstest

## Shared by Fry on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

An incident response team is recommending changes after analyzing a recent compromise in which:

a large number of events and logs were involved;

team members were not able to identify the anomalous behavior and escalate it in a timely manner;

several network systems were affected as a result of the latency in detection;

security engineers were able to mitigate the threat and bring systems back to a stable state; and

the issue reoccurred shortly after and systems became unstable again because the correct information was not gathered during the initial identification phase.

Which two recommendations should be made for improving the incident response process? (Choose two.)

## Options:

**A-** Formalize reporting requirements and responsibilities to update management and internal stakeholders throughout the incident-handling process effectively.

**B-** Improve the mitigation phase to ensure causes can be quickly identified, and systems returned to a functioning state.

**C-** Implement an automated operation to pull systems events/logs and bring them into an organizational context.

**D-** Allocate additional resources for the containment phase to stabilize systems in a timely manner and reduce an attack's breadth.

**E-** Modify the incident handling playbook and checklist to ensure alignment and agreement on roles, responsibilities, and steps before an incident occurs.

### Answer:

C, E

## Question 2

**Question Type:** MultipleChoice

What is a use of TCPdump?

### Options:

**A-** to analyze IP and other packets

**B-** to view encrypted data fields

**C-** to decode user credentials

**D-** to change IP ports

### Answer:

A

# Question 3

**Question Type:** MultipleChoice

A network host is infected with malware by an attacker who uses the host to make calls for files and shuttle traffic to bots. This attack went undetected and resulted in a significant loss. The organization wants to ensure this does not happen in the future and needs a security solution that will generate alerts when command and control communication from an infected device is detected. Which network security solution should be recommended?

### Options:

**A-** Cisco Secure Firewall ASA

**B-** Cisco Secure Firewall Threat Defense (Firepower)

**C-** Cisco Secure Email Gateway (ESA)

**D-** Cisco Secure Web Appliance (WSA)

## Answer:

B

# Question 4

**Question Type:** **MultipleChoice**

Refer to the exhibit.

```
00386078   64   44   45   33   4C   6A   41   34   4C   6A   4D   78   4C   6B   5A   44
00386088   4D   44   59   78   4E   79   34   31   4E   54   41   32   4C   6A   55   31
00386098   4D   44   59   75   4E   6A   67   7A   4E   77   3D   3D   00   AB   AB   AB
```

Which encoding technique is represented by this HEX string?

## Options:

**A-** Unicode

**B-** Binary

**C-** Base64

**D-** Charcode

### Answer:

B

# Question 5

**Question Type:** MultipleChoice

Refer to the exhibit.

service

June 3, 2020 at 5:33 PM

Credit Card Refund #186913

To: [removed]

Received: from ([202.142.155.218]) by [removed] for [removed]; Wed, 03 Jub 2020 15:33:03 +0000 (UTC)

Received: from [53.183.109.56] (helo=WEEOWED.lu) by with esmtpa (Exim 4.85) (envelope-from) id 08A56E158516 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Received: from [54.198.90.184] (account cobblergs8@o4.e.notification.intuit.com HELO RUFINEF.GYPUBOT.mcg) by (Postfix) with ESMTPA id mXDmHhpAEoD7.233 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Content-Type: multipart/mixed; boundary= "- -_Part_6483125_09335162.9435849616646"

1

**Cash Refund**

| | |
|---|---|
| **Date** | **6/03/2020** |
| **Refund #** | **186913** |
| **Payment Method** | **Website Payment** |
| **Check #** | **3000679700** |
| **Project** | |
| **Department** | |
| **Phone Number** | |
| **Shipping Method** | **UPS 2nd Day Air®** |
| **Credit Card #** | ********** |
| **Transaction Next Approver** | |

| Item | Quantity | Description | Options | Rate | Amount | Gross Amt | Tax Amount | Tax Details Reference |
|---|---|---|---|---|---|---|---|---|
| 3795326-44 | 1 | 2020 | | 1,397.11 | 1,397.11 | 1,397.11 | | 97810761_1 |
| | | | | Subtotal | 1,397.11 | | | |
| | | | Shipping Cost (UPS 2nd Day Air®) | | 0.00 | | | |
| | | | | **Total** | $1,397.11 | | | |

********CREDIT WILL BE ISSUED TO YOUR CREDIT CARD USED FOR ORIGINAL PURCHASE********

Card_Refund_186913.xlsm

Which element in this email is an indicator of attack?

### Options:

**A-** IP Address: 202.142.155.218

**B-** content-Type: multipart/mixed

**C-** attachment: "Card-Refund"

**D-** subject: "Service Credit Card"

### Answer:

C

## Question 6

**Question Type:** **MultipleChoice**

An attacker embedded a macro within a word processing file opened by a user in an organization's legal department. The attacker used this technique to gain access to confidential financial dat

a. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)

## Options:

**A-** controlled folder access

**B-** removable device restrictions

**C-** signed macro requirements

**D-** firewall rules creation

**E-** network access control

## Answer:

A, C

# Question 7

**Question Type:** **MultipleChoice**

Refer to the exhibit.

84.55.41.57 - -[17/Apr/2016:06:57:24 +0100] “GET/wordpress/wp-login.php HTTP/1.1” 200 1568 “-”
84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] “POST/wordpress/wp-login.php HTTP/1.1” 302 1150
“http://www.example.com/wordpress/wp-login.php”

84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] “GET/wordpress/wp-admin/ HTTP/1.1” 200 12905
“http://www.example.com/wordpress/wp-login.php”
84.55.41.57 - -[17/Apr/2016:07:00:32 +0100] “POST/wordpress/wp-admin/admin-ajax.php HTTP/1.1”
200 454 “http://www.example.com/wordpress/wp-admin/”

84.55.41.57 - -[17/Apr/2016:07:11:48 +0100 “GET/wordpress/wp-admin/plugin-install.php HTTP/1.1”
200 12459 “http://www.example.com/wordpress/wp-admin/plugin-install.php?tab=upload”
84.55.41.57 - -[17/Apr/2016:07:16:06 +0100] “GET /wordpress/wp-admin/update.php? action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca HTTP/1.1” 200 5698

“http://www.example.com/wordpress/wp-admin/plugin install.php?tab=search&s=file+permission”
84.55.41.57 - -[17/Apr/2016:07:18:19 +0100] “GET /wordpress/wp-
admin/plugins.php?action=activat&plugin=file-manager%2Ffile-manager.php&_wpnonce=bf932ee530
HTTP/1.1” 302.451 “http://www.example.com/wordpress/wp-admin/update.php?action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca”

84.55.41.57 - -[17/Apr/2016:07:21:46 +0100] “GET /wordpress/wp-admin/admin-ajax.php?
action=connector&cmd=upload&target=l1_d3AtY29udGVudA&name%5B%5D=r57.php&FILES
=&_=1460873968131 HTTP/1.1” 200 731 “http://www.example.com/wordpress/wp-admin/admin.php?
page=fie-manager_settings”

84.55.41.57 - -[17/Apr/2016:07:22:53+0100] “GET /wordpress/wp-content/r57.php HTTP/1.1” 200 9036 “-”
84.55.41.57- -[17/Apr/2016:07:32:24 +0100] “POST /wordpress/wp-content/r57.php?14 HTTP/1.1” 200
8030 “http://www.example.com/wordpress/wp-content/r57.php?14”
84.55.41.57 - -[17/Apr/2016:07:29:21 +0100] “GET /wordpress/wp-content/r57.php?29 HTTP/1.1” 200
8391 “http://www.example.com/wordpress/wp-content/r57.php?28”

Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

### Options:

**A-** The attacker used r57 exploit to elevate their privilege.

**B-** The attacker uploaded the word press file manager trojan.

**C-** The attacker performed a brute force attack against word press and used sql injection against the backend database.

**D-** The attacker used the word press file manager plugin to upoad r57.php.

**E-** The attacker logged on normally to word press admin page.

### Answer:

C, D

## Question 8

**Question Type:** MultipleChoice

Refer to the exhibit.

<stix:Indicator id= “CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c” timestamp= “2020-04-08T00:44:39.970278+00:00” xsi:type= “indicator:IndicatorType”>
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= “CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89”>
<cybox:Object id= “CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74”>
<cybox:Properties xsi:type= “DomainNameObj:DomainNameObjectType” type= “FQDN”>
<DomainNameObj:Value condition= “Equals” >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= “CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702” timestamp= “2020-04-08T00:44:39.970417+00:00” xsi:type= “indicator:IndicatorType”>
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= “CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c”>
<cybox:Object id= “CISA:Object-7728bd69-e724-4917-9550-9ae853becf28”>
<cybox:Properties xsi:type= “DomainNameObj:DomainNameObjectType” type= “FQDN”>
<DomainNameObj:Value condition= “Equals”>nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= “CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf” timestamp= “2020-04-08T00:44:39.970554+00:00” xsi:type= “indicator:IndicatorType”>
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= “CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254”>
<cybox:Object id= “CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760”>
<cybox:Properties xsi:type= “DomainNameObj:DomainNameObjectType” type= “FQDN”>
<DomainNameObj:Value condition= "Equals”>stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>

Which two actions should be taken based on the intelligence information? (Choose two.)

### Options:

**A-** Block network access to all .shop domains

**B-** Add a SIEM rule to alert on connections to identified domains.

**C-** Use the DNS server to block hole all .shop requests.

**D-** Block network access to identified domains.

**E-** Route traffic from identified domains to block hole.

### Answer:

B, D

## Question 9

**Question Type:** **MultipleChoice**

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?

## Options:

**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

## Answer:

B