



300-215^{Q&As}

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

Pass Cisco 300-215 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/300-215.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A security team received reports of users receiving emails linked to external or unknown URLs that are non-returnable and non-deliverable. The ISP also reported a 500% increase in the amount of ingress and egress email traffic received. After detecting the problem, the security team moves to the recovery phase in their incident response plan. Which two actions should be taken in the recovery phase of this incident? (Choose two.)

- A. verify the breadth of the attack
- B. collect logs
- C. request packet capture
- D. remove vulnerabilities
- E. scan hosts with updated signatures

Correct Answer: DE

QUESTION 2

What is the function of a disassembler?

- A. aids performing static malware analysis
- B. aids viewing and changing the running state
- C. aids transforming symbolic language into machine code
- D. aids defining breakpoints in program execution

Correct Answer: A

Reference: https://scholar.google.co.in/scholar?q=disassembler+aids+performing+static+malware+analysisandhl=enanddas_sdt=0anddas_vis=1andoi=scholar

QUESTION 3

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 4



System Number of events: 572				
Level	Date and Time	Source	Event ID	Task Category
Information	4/26/2015 12:42:14 PM	Service Control Man...	7045	None
Information	4/26/2015 12:38:28 PM	Service Control Man...	7045	None
Event 7045, Service Control Manager				
General Details				
A service was installed in the system.				
Service Name: DIIAHHNMPMMRqji				
Service File Name: \\127.0.0.1\admin\$\\EqnBqKWm.exe				
Service Type: user mode service				
Service Start Type: demand start				
Service Account: LocalSystem				

Refer to the exhibit. An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hour prior. Which two indicators of compromise should be determined from this information? (Choose two.)

- A. unauthorized system modification
- B. privilege escalation
- C. denial of service attack
- D. compromised root access
- E. malware outbreak

Correct Answer: AD

QUESTION 5



```
<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>
```

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

- 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.

Correct Answer: BD