Free Questions for SY0-601 by vceexamstest

Shared by Oliver on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization has hired a red team to simulate attacks on its security pos-ture, which Of following will the blue team do after detecting an IOC?

Options:

A- Reimage the impacted workstations.

B- Activate runbooks for incident response.

C- Conduct forensics on the compromised system,

D- Conduct passive reconnaissance to gather information

Answer:

B

Explanation:

A runbook is a set of predefined procedures and steps that guide an incident response team through the process of handling a security incident.It can help the blue team respond quickly and effectively to an indicator of compromise (IOC) by following the best practices and

predefined actions for containment, eradication, recovery and lessons learned.

Question 2

Question Type: MultipleChoice

Which of the following is used to describe discrete characteristics of a potential weakness that results in a seventy number?

Options:

A- CVSS

B- CVE

C- CAR

D- CERT

Answer:

A

Question 3

Question Type: MultipleChoice

An analyst in the human resources organization is responsible for the quality of the company's personnel dat

a. The analyst maintains a data dictionary and ensures it is correct and up to date Which of the following best describes the role of the analyst?

Options:

A- Data steward

B- Data owner

C- Data processor

D- Data protection officer

Answer:

A

Question 4

Question Type: MultipleChoice

An analyst observed an unexpected high number of DE authentication on requests being sent from an unidentified device on the network. Which of the following attacks was most likely executed in this scenario?

Options:

A- Jamming

B- Blue jacking

C- Rogue access point

D- Disassociation

Answer:

D

Question 5

Question Type: MultipleChoice

An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas. The service provider enables direct TCP'IP connection to stream live video footage from each camer

a. The organization wants to ensure this stream is encrypted and authenticated Which of the following protocols should be implemented to best meet this objective?

Options:

A- SSH

B- SRTP

C- S/MIME

D- PPTP

Answer:

B

Question 6

Question Type: **MultipleChoice**

A security analyst reviews web server logs and notices the following line:

```
104.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /profile.php?id=%3cscript%3ealert%28%271%27%29%3cscript%3e HTTP/1.1" 200 11705
"http://www.example.com/downloadreport.php"
104.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /profile.php?id=%3cscript%3ealert%28%27
http%3a%2f%2fwww.evilsite.com%2fupdater.php%27%29%3cscript%3e HTTP/1.1" 200 23713 "http://www.example.com/downloadreport.php"
```

Which of the following vulnerabilities is the attacker trying to exploit?

Options:

A- Token reuse

B- SQL injection

C- Server side request forgery

D- Cross-site scripting

Answer:

D

Question 7

Question Type: **MultipleChoice**

An organization developed a virtual thin client running in kiosk mode mat is used to access various software depending on the users' roles During a security evaluation, the test team identified the ability to exit kiosk mode and access system-level resources which led to privilege escalation Which of the following mitigations addresses this finding?

Options:

A- Using application approved/dented lists

B- Incorporating web content filtering

C- Enforcing additional firewall rules

D- Implementing additional network segmentation

Answer:

A

Question 8

Question Type: **MultipleChoice**

Which of the following technologies can better utilize compute and memory resources for on-premises application workloads?

Options:

A- Containers

B- Microservices

C- Serverless architecture

D- Community clouds

Answer:

A

Question 9

Question Type: MultipleChoice

A security department wants to conduct an exercise that will make many experimental changes to the main virtual server After the exercise is completed, the IT director would like to be able to roll Sack to the state prior to the exercise. Which of the following backup types will allow for the fastest rollback?

Options:

A- Incremental

B- Snapshot

C- Full

D- Differential

Answer:

B

Question 10

Question Type: MultipleChoice

A security administrator is reviewing reports about suspicious network activity occurring on a subnet Users on the network report that connectivity to various websites is intermittent. The administrator logs in to a workstation and reviews the following command output:

```
? (192.168.1.7) at <incomplete> on enp0s25
www.routerlogin.com (192.168.1.1) at 08:03:ee:dd:fb:2b [ether] on enp0s25
? (192.168.1.4) at 6c:3a:ef:7a:cc:dd on enp0s25
server1 (192.168.1.8) at 08:03:ee:dd:fb:2b [ether] on enp0s25
? (192.168.1.5) at 08:03:ee:dd:fb:2b [ether] on enp0s25
? (192.168.1.2) at <incomplete> on enp0s25
server2 (192.168.1.6) at 08:03:ee:dd:fb:2b [ether] on enp0s25
```

Which of the following best describes what is occurring on the network?

Options:

A- ARP poisoning

B- On-path attack

C- URL redirection

D- IP address conflicts

Answer:

A

Question 11

Question Type: **MultipleChoice**

An audit identified Pll being utilized in the development environment of a critical application The Chief Privacy Officer (CPO) is adamant that this data must be removed; however, the developers state that they require real data to perform developmental and functionality tests. Which of the following should a security professional implement to best satisfy both the CPO's and the development team's requirements?

Options:

A- Data purge

B- Data encryption

C- Data masking

D- Data totalization

Answer:

C

Question 12

Question Type: **MultipleChoice**

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include

* A starting baseline of 50% memory utilization

* Storage scalability

* Single circuit failure residence

Which of the following best meets all of these requirements?

Options:

A- Connecting dual PDUs to redundant power supplies

B- Transitioning the platform to an laaS provider

C- Configuring network load balancing for multiple paths

D- Deploying multiple large NAS devices for each host

Answer:

A