CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization\\'s network. Which of the following approaches should the security analyst recommend?

A. Use the MITRE ATTandCK framework to develop threat models.

B. Conduct internal threat research and establish indicators of compromise.

C. Review the perimeter firewall rules to ensure rule-set accuracy.

D. Use SCAP scans to monitor for configuration changes on the network.

Correct Answer: A

QUESTION 2

A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverlist. Xml. The host list is provided in a file named werbserverlist,text. Which of the fallowing Nmap commands would BEST accomplish this goal?

A. nmap -iL webserverlist.txt -sC -p 443 -oX webserverlist.xml

B. nmap -iL webserverlist.txt -sV -p 443 -oX webserverlist.xml

C. nmap -iL webserverlist.txt -F -p 443 -oX webserverlist.xml

D. nmap --takefile webserverlist.txt --outputfileasXML webserverlist.xml –scanports 443

Correct Answer: B

QUESTION 3

An organization has two environments: development and production. Development is where applications are developed with unit testing. The development environment has many configuration differences from the production environment. All applications are hosted on virtual machines. Vulnerability scans are performed against all systems before and after any application or configuration changes to any environment. Lately, vulnerability remediation activity has caused production applications to crash and behave unpredictably. Which of the following changes should be made to the current vulnerability management process?

A. Create a third environment between development and production that mirrors production and tests all changes before deployment to the users

B. Refine testing in the development environment to include fuzzing and user acceptance testing so applications are more stable before they migrate to production

C. Create a second production environment by cloning the virtual machines, and if any stability problems occur, migrate users to the alternate production environment

D. Refine testing in the production environment to include more exhaustive application stability testing while continuing to maintain the robust vulnerability remediation activities

Correct Answer: A

QUESTION 4

A security analyst at exampte.com receives a SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream: Winch of the following actions should the security analyst lake NEXT?

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: %{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(#ros.println(31337*31337)).(#ros.flush())}
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center; X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmz.example.local:443
iv_server_name: connect-webseald-revproxy.dmz.example.local
x-
```

A. Review the known Apache vulnerabilities to determine if a compromise actually occurred

B. Contact the application owner for connect example local tor additional information

C. Mark the alert as a false positive scan coming from an approved source.

D. Raise a request to the firewall team to block 203.0.113.15.

Correct Answer: B

An authenticated scan reports weaknesses exposed to the authenticated users of the system, as all the hosted services can be accessed with a right set of credentials. An -unauthenticated scan reports weaknesses from a public viewpoint

(this is what the system looks like to the unauthenticated users) of the system.

So the scan may be valid but instead of concluding asking for additional information from the application owner doesn\\'t hurt and confirms if this activity is done internally.

QUESTION 5

A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline.

Which of the following should the analyst recommend to the company officer?

A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.

B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.

C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised recourse.

D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.

Correct Answer: A