CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the

environment. Given the following output:

Which of the following choices should the analyst look at first?

A. wh4dc-748gy.lan (192.168.86.152)

B. lan (192.168.86.22)

C. imaging.lan (192.168.86.150)

D. xlaptop.lan (192.168.86.249)

E. p4wnp1_aloa.lan (192.168.86.56)

Correct Answer: E

The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official https://github.com/mame82/P4wnP1_aloa

QUESTION 2

A security analyst is monitoring a company\\'s network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.

B. Isolate the system and begin a forensic investigation to determine what was compromised.

C. Recommend network segmentation to the management team as a way to secure the various environments.

D. Implement host-based firewalls on all systems to prevent ping sweeps in the future.

Correct Answer: A

Reporting this activity as a false positive, as the activity is legitimate, is the best way for the security analyst to respond. A false positive is a condition in which harmless traffic is classified as a potential network attack by a security monitoring tool. Ping requests are a common network diagnostic tool that can be used to test network connectivity issues. The technician who responded to potential network connectivity issues was performing a legitimate task and did not pose any threat to the accounting and human resources servers . https://www.techopedia.com/definition39/memory-dump

QUESTION 3

A new prototype for a company\\'s flagship product was leaked on the internet As a result, the management team has locked out all USB drives Optical drive writers are not present on company computers The sales team has been granted an exception to share sales presentation files with third parties Which of the following would allow the IT team to determine which devices are USB enabled?

A. Asset tagging

B. Device encryption

C. Data loss prevention

D. SIEMIogs

Correct Answer: D

A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A SIEM system can help the IT team to

determine which devices are USB enabled by querying the log data for events related to USB device insertion, removal, or usage. The other options are not relevant or effective for this purpose. CompTIA Cybersecurity Analyst (CySA+)

Certification Exam Objectives (CS0-002), page 15;

https://www.sans.org/reading-room/whitepapers/analyst/securityinformation-event-management-siem-implementation-33969

QUESTION 4

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network. Which of the following metrics should the team lead include in the briefs?

A. Mean time between failures

B. Mean time to detect

C. Mean time to remediate

D. Mean time to contain

Correct Answer: D

Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

QUESTION 5

A security analyst is reviewing the network security monitoring logs listed below:

Count: 2 Event#3.3505 2020-01-30 10:40 UTC GPL WEB SERVER robots. txt access

10.1.1.128 -> 10.0.0.10 IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 tt1=0 chksum=22704 Protocol: 6 sport=45260 => dport=80 Sec=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=23415 chksum=0

Count: 22 Event#3.3507 2020-01-30 10:40 UTC ET WEB SPECIFIC APPS PHPStudy Remote Code Execution Backdoor

10.1.1.129 -> 10.0.0.10 IPVer=4 hen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 tt1=0 chksum=22704 Protocol: 6 sport=65200 -> dport=80 Sea=0 Ack=0 off=5 Res=0 Flags=******** win=0 urp=26814 chksum=0

Count: 30 Event#3.3522 2020-01-30 10:40 UTC ET WEB SERVER WEB-PHP phpinfo access

10.1.1.130 -> 10.0.0.10 IPVer=4 hen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 tt1=0 chksum=22704 Protocol: 6 sport=58175 -> dport=80 Sec=0 Ack=0 Off=5 Res=0 Flags=******** win=0 urp=22875 chksum=0

Count: 22 Event#3.3728 2020-01-30 10:40 UTC GPL WEB SERVER 403 Forbidden

10.0.0.10 -> 10.1.1.129 IPVer=4 hen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 tt1=0 chksum=20471 Protocol: 6 sport=80 -> dport=65200 Sea=0 Ack=0 Off=5 Res=0 Flags=******** win=0 urp=59638 chksum=0

Which of the following is the analyst MOST likely observing? (Choose two.)

A. 10.1.1.128 sent potential malicious traffic to the web server.

B. 10.1.1.128 sent malicious requests, and the alert is a false positive

C. 10.1.1.129 successfully exploited a vulnerability on the web server

D. 10.1.1.129 sent potential malicious requests to the web server

E. 10.1.1.129 can determine mat port 443 is being used

F. 10.1.1.130 can potentially obtain information about the PHP version

Correct Answer: DF

A security analyst is reviewing the network security monitoring logs listed below and is most likely observing that 10.1.1.129 sent potential malicious requests to the web server and that 10.1.1.130 can potentially obtain information about the

PHP version. The logs show that 10.1.1.129 sent two requests to the web server with suspicious parameters, such as " " , which are commonly used for SQL injection attacks. The logs also show that 10.1.1.130 sent a request to the " , which

is a function that displays information about the PHP configuration and environment, which can be useful for attackers to find vulnerabilities or exploit them. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002),

page 8;

https://owasp.org/www-community/attacks/SQL_Injection;

https://www.php.net/manual/en/function.phpinfo.php

QUESTION 6

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA

B. LOI

C. MOU

D. KPI

Correct Answer: A

QUESTION 7

A new prototype for a company\\'s flagship product was leaked on the internet. As a result, the management team has locked out all USB dives. Optical drive writers are not present on company computers. The sales team has been granted an exception to share sales presentation files with third parties. Which of the following would allow the IT team to determine which devices are USB enabled?

A. Asset tagging

B. Device encryption

C. Data loss prevention

D. SIEM logs

Correct Answer: D

QUESTION 8

Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org - d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT (0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(C.0179s) ICMP SCANNABLE > SCANNER echo reply(type-0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seg=713 checksum=16000
massping done: num_host:1 num response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER: 63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER: 63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER: 63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCB SCANNER:60517 > SCANNADLE:139 iplen=40 seq=1040604
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT          STATE       SERVICE
22/tcp        open        ssh
113/tcp       closed      auth
139/tcp       filtered    netbios-ssh
1433/tcp      closed      ms-sql

Nmap done:1 10.155.187.1 (1 host)
```

Which of the following actions will an attacker be able to initiate directly against this host?

A. Password sniffing

B. ARP spoofing

C. A brute-force attack

D. An SQL injection

Correct Answer: C

The Nmap command given in the question performs a TCP SYN scan (-sS), a service version detection scan (-sV), an OS detection scan (-O), and a port scan for ports 1-1024 (-p 1-1024) on the host 192.168.1.1. This command will reveal information about the hos" and running services, which can be used by an attacker to launch a brute-force attack against the host. A brute-force attack is a method of guessing passwords or encryption keys by trying many possible combinations until finding the correct one. An attacker can use the information from the Nmap scan to target specific services or protocols that may have weak or default credentials, such as FTP, SSH, Telnet, or HTTP.

QUESTION 9

Which of the following BEST explains the function of a managerial control?

A. To scope the security planning, program development, and maintenance of the security life cycle

B. To guide the development of training, education, security awareness programs, and system maintenance

C. To implement data classification, risk assessments, security control reviews, and contingency planning

D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of

audit trails

Correct Answer: C

https://www.examtopics.com/discussions/comptia/view/84935-exam-cs0-002-topic-1-question-191-discussion/

QUESTION 10

An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

A. A DLP system

B. DNS sinkholing

C. IP address allow list

D. An inline IDS

Correct Answer: B

DNS sinkholing is a mechanism that can prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains by returning a false or controlled IP address for those domains. This can

reduce the load on the firewall by intercepting the DNS requests before they reach the firewall and diverting them to a sinkhole server. The other options are not relevant or effective for this purpose. CompTIA Cybersecurity Analyst (CySA+)

Certification Exam Objectives (CS0-002), page 9;

https://www.enisa.europa.eu/topics/incidentresponse/glossary/dns-sinkhole

QUESTION 11

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

A. Implementing multifactor authentication on the server OS

B. Hashing user passwords on the web application

C. Performing input validation before allowing submission

D. Segmenting the network between the users and the web server

Correct Answer: C

Input validation is a critical security measure to prevent various types of web application attacks, including SQL injection, cross-site scripting (XSS), and data manipulation. It helps ensure that user inputs are sanitized and do not contain malicious or unexpected data.

QUESTION 12

A recent audit of the vulnerability management program outlined the finding for increased awareness of secure coding practices. Which of the following would be best to address the finding?

A. Establish quarterly SDLC training on the top vulnerabilities for developers

B. Conduct a yearly inspection of the code repositories and provide the report to management.

C. Hire an external penetration test of the network

D. Deploy more vulnerability scanners for increased coverage

Correct Answer: A

The finding in the audit suggests a need to improve awareness of secure coding practices. The most appropriate action to address this finding is to provide training to the development team on secure coding practices.

QUESTION 13

While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report:

```
The following certificates are part of the certificate chain but using insecure signature algorithms:
Subject: CN=10.200.20.1,OU=HTTPS Management Certificate for SonicWALL (self-
-signed),O=HTTPS Management Certificate for SonicWALL (self-signed),L=Sunnyvale,ST=Califor-
nia,C=US
Signature Algorithm: sha1WithRSAEncryption
```

this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?

A. Reconfigure the device to support only connections leveraging TLSv1.2.

B. Obtain a new self-signed certificate and select AES as the hashing algorithm.

C. Replace the existing certificate with a certificate that uses only MD5 for signing.

D. Use only signed certificates with cryptographically secure certificate sources.

Correct Answer: D

QUESTION 14

A. SIEM

B. XDR

C. SOAR

D. EDR

Correct Answer: C

QUESTION 15

During an investigation, an analyst discovers the following rule in an executive\\'s email client:

```
IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com>
SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>
```

The executive is not aware of this rule. Which of the following should the analyst do first to evaluate the potential impact of this security incident?

A. Check the server logs to evaluate which emails were sent to .

B. Use the SIEM to correlate logging events from the email server and the domain server.

C. Remove the rule from the email client and change the password.

D. Recommend that the management team implement SPF and DKIM.

Correct Answer: C