210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

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

QUESTION 1

Which CVSS Attach Vector metric value means that the vulnerable component is not bound to the network stack and the path of the attacker is via read/write/execute capabilities?

A. network

B. physical

C. local

D. adjacent

Correct Answer: C

Reference: https://www.first.org/cvss/specification-document

QUESTION 2

Which technology is the leading industry approach used to automatically enforce NAC?

A. IGMP

B. SNMP

C. 802.1X

D. Port Security

Correct Answer: C

QUESTION 3

Which Cyber Kill Chain Model category does attacking a vulnerability belong to?

A. Exploitation

B. Action on Objectives

C. Installation

D. Delivery

Correct Answer: A

QUESTION 4

Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?

A. confidentiality

B. integrity

C. availability

D. complexity

Correct Answer: B

QUESTION 5

Which statement about collecting data evidence when performing digital forensics is true?

A. Allowing unrestricted access to impacted devices

B. Not allowing items of evidence to be physically touch

C. Powering off the device after collecting the data

D. It must be preserved and integrity checked

Correct Answer: D

QUESTION 6

Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?

A. data analytics

B. asset attribution

C. threat actor attribution

D. evidence collection

Correct Answer: A

QUESTION 7

Who is responsible for initially analyzing an incident to determine what has happened?

A. IT director

B. CIO

C. server administrator

D. incident handler

Correct Answer: D

QUESTION 8

You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)

A. file size

B. domain names

C. dropped files

D. signatures

E. host IP addresses

Correct Answer: BE

QUESTION 9

How is confidentiality defined in the CVSS v3.0 framework?

A. confidentiality of the information resource managed by person due to an unsuccessfully exploited vulnerability

B. confidentiality of the information resource managed by a person due to a successfully vulnerability

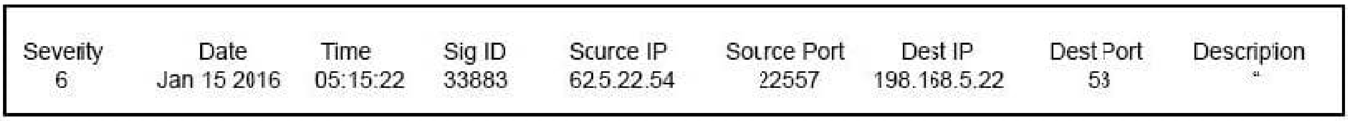
C. confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability

D. confidentiality of the information resource managed by a software component due to an unsuccessfully exploited vulnerability

Correct Answer: C

QUESTION 10

Refer to the exhibit. Which type of log is this an example of?



Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2016	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	"

A. IDS log

B. proxy log

C. NetFlow log

D. syslog

Correct Answer: C

A typical output of a NetFlow command line tool (nfdump in this case) when printing the stored flows may look as follows:

Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Packets Bytes Flows 2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 -> 192.168.0.1:22126 1 46 1 2010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 -> 127.0.0.1:24920 1 80 1

Reference: http://nfdump.sourceforge.net/

QUESTION 11

Which type of analysis is done when all facts are available?

A. probabilistic

B. deterministic

C. static

D. dynamic

Correct Answer: B

QUESTION 12

In addition to cybercrime and attacks, evidence found on a system or network may be presented in a court of law to support accusations of crime or civil action, including which of the following?

A. Fraud, money laundering, and theft

B. Drug-related crime

C. Murder and acts of violence

D. All of the above

Correct Answer: D

QUESTION 13

Why do SOC analysts use 5-tuple?

A. to identify the requirements for creating a functional network connection between two laptops

B. to identify the requirements for creating a wireless network connection between an access point and a host

C. to identify the requirements for creating a data center using best practices

D. to identify the requirements for creating a secure network connection between two or more remote and local machines

Correct Answer: D

QUESTION 14

What is missing from the data correlated by using security intelligence?

A. security intelligence categories

B. time stamps of data transmission at the frame level

C. ports

D. time stamps of data transmission at the packet level

Correct Answer: B

QUESTION 15

Which element is included in an incident response plan?

A. organization mission

B. junior analyst approval

C. day-to-day firefighting

D. siloed approach to communications

Correct Answer: A