Vendor: Cisco

Exam Code:210-255

Exam Name: Cisco Cybersecurity Operations

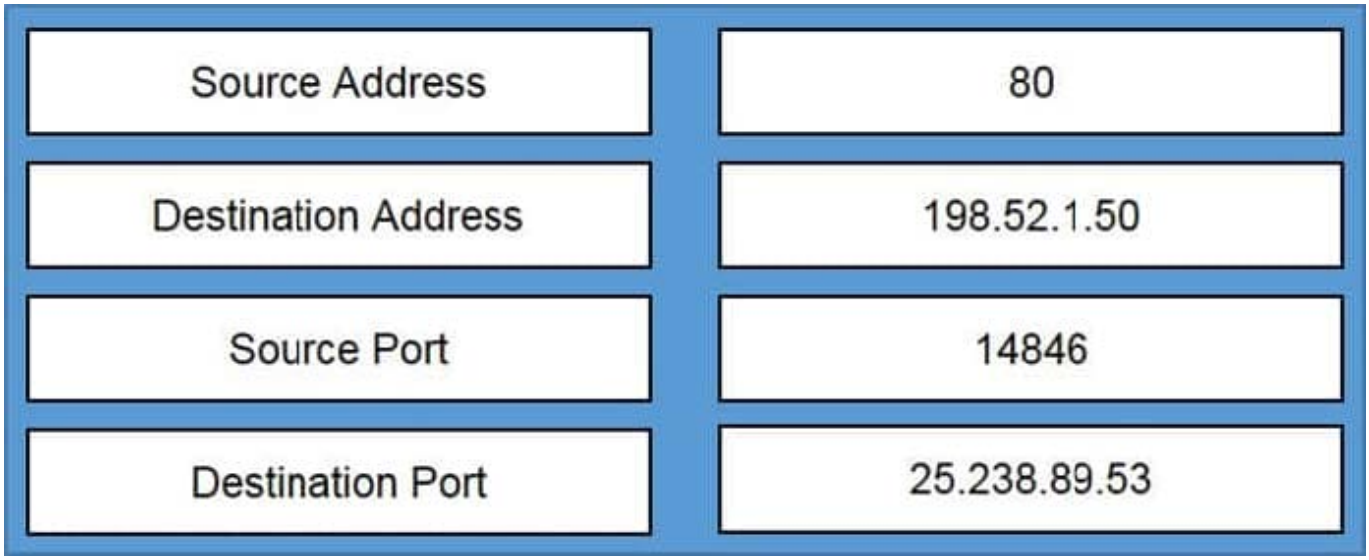
Version: Demo

QUESTION 1

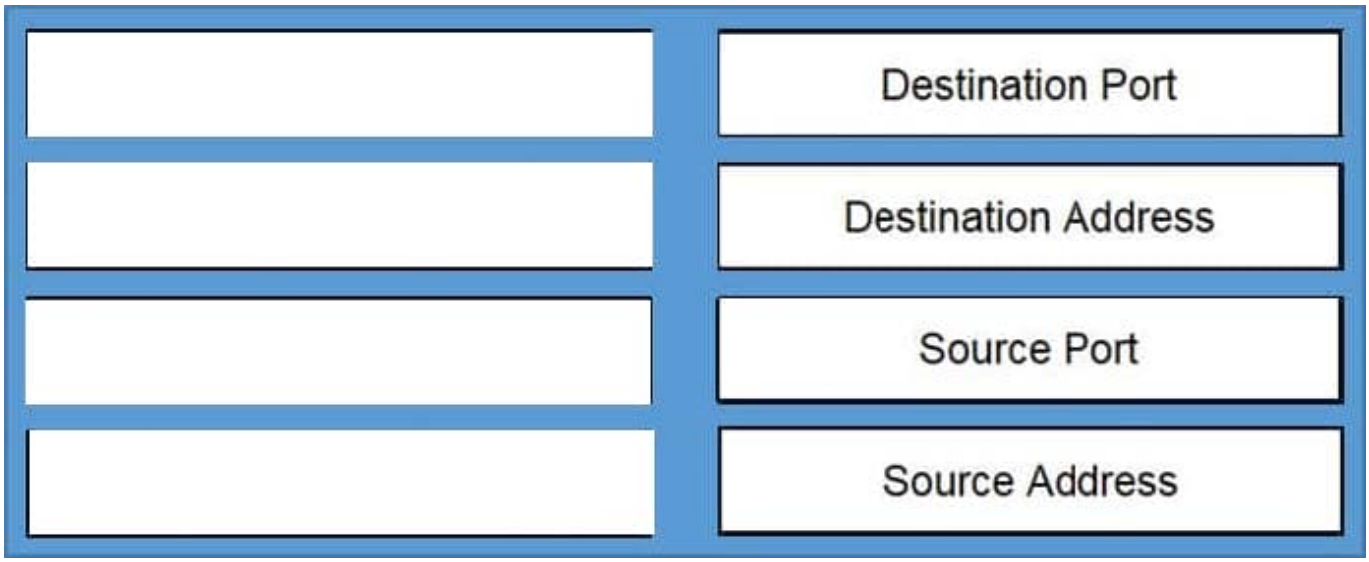
Drag and Drop

Built inbound TCP connection 463879 for outside: (25.238.89.53/14846) to DMZ: WWW_Server/80 (198.52.1.50/80)

Select and Place:



Correct Answer:



QUESTION 2

What is a common artifact used to uniquely identify a detected file?

A. file size

B. file extension

C. file timestamp

D. file hash

Correct Answer: D

QUESTION 3

What is the definition of integrity according to CVSSv3 framework?

A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.

B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.

C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

Correct Answer: B

QUESTION 4

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

A. It must be preserved and its integrity verified.

B. It must be copied to external storage media and immediately distributed to the CISO.

C. It must be deleted as soon as possible due to PCI compliance.

D. It must be stored in a forensics lab only by the data custodian.

Correct Answer: A

QUESTION 5

What do the Security Intelligence Events within the FMC allow an administrator to do?

A. See if a host is connecting to a known-bad domain.

B. Check for host-to-server traffic within your network.

C. View any malicious files that a host has downloaded.

D. Verify host-to-host traffic within your network.

Correct Answer: A

QUESTION 6

What is the process of remediation the network and systems and/or reconstructing so the responsible threat actor can be revealed?

A. Data analysis

B. Assets distribution

C. Evidence collection

D. Threat actor distribution

Correct Answer: D

QUESTION 7

What does the CSIRT incident response provider usually do?

A. provide incident handling services to their parent organization.

B. provide incident handling services to a country

C. coordinate and facilitate the handling of incidents across various CSIRTs

D. focus on synthesizing data from various sources to determine trends and patterns in incident activity

E. handle reports of vulnerabilities in their software or hardware products

F. offer incident handling services as a for-fee service to other organizations

Correct Answer: D

QUESTION 8

According to NIST-SP800-61R2, which option should be contained in the issue tracking system?

A. incidents related to the current incident

B. incident unrelated to the current incident

C. actions taken by nonincident handlers

D. latest public virus signatures

Correct Answer: A

QUESTION 9

What information from HTTP logs can be used to find a threat actor?

A. referer

B. IP address

C. user-agent

D. URL

Correct Answer: B

QUESTION 10

Which type of intrusion event is an attacker retrieving the robots. txt file from target site?

A. exploitation

B. weaponization

C. scanning

D. reconnaissance

Correct Answer: D

QUESTION 11

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800- 61 r2?

A. instigator

B. precursor

C. online assault

D. trigger

Correct Answer: B

QUESTION 12

Which two compliance frameworks require that data be encrypted when it is transmitted over a public network? (Choose two.)

A. PCI

B. GLBA

C. HIPAA

D. SOX

E. COBIT

Correct Answer: AC