# 200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

## Pass Cisco 200-201 Exam with 100% Guarantee

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

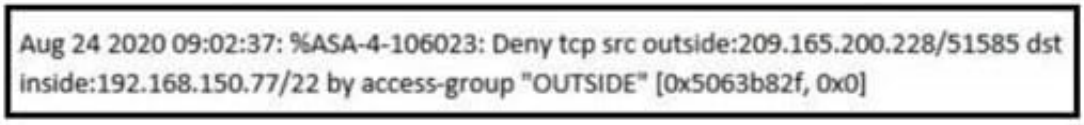
**https://www.leads4pass.com/200-201.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

Refer to the exhibit.




An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?

A. indirect

B. circumstantial

C. corroborative

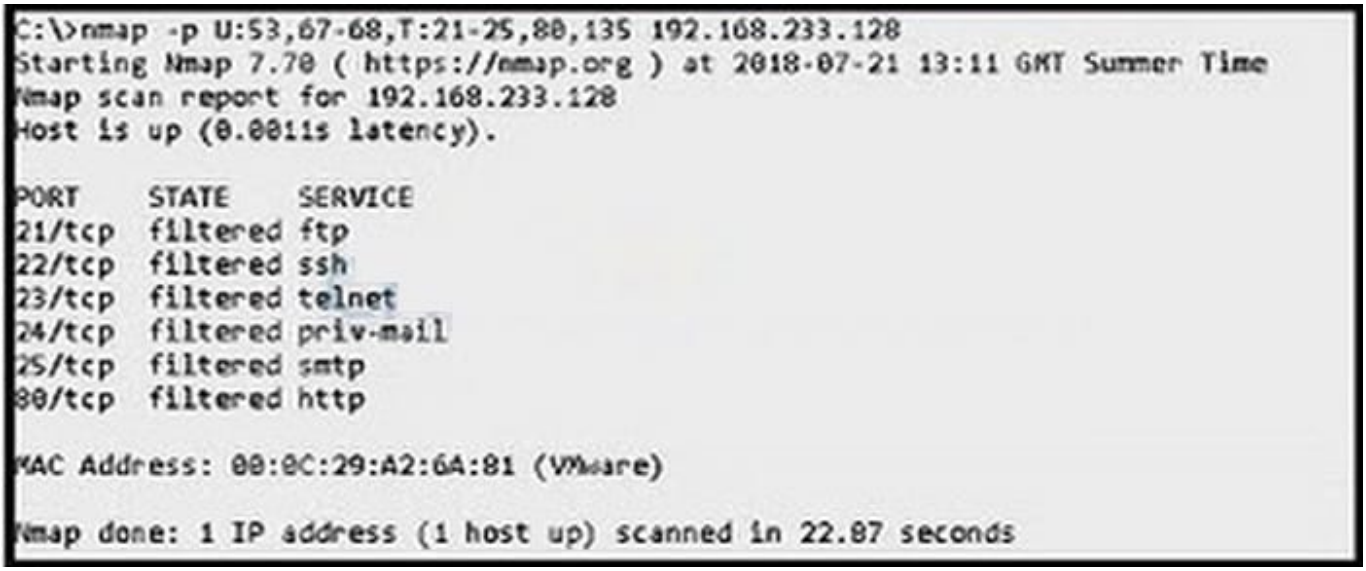
D. best

Correct Answer: C

Indirect=circumstantail so there is no posibility to match A or B (only one answer is needed in this question). For suer it\\'s not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it\\'s mean nothing.

**QUESTION 2**

Refer to the exhibit.




An attacker scanned the server using Nmap. What did the attacker obtain from this scan?

A. Identified a firewall device preventing the pert state from being returned.

B. Identified open SMB ports on the server

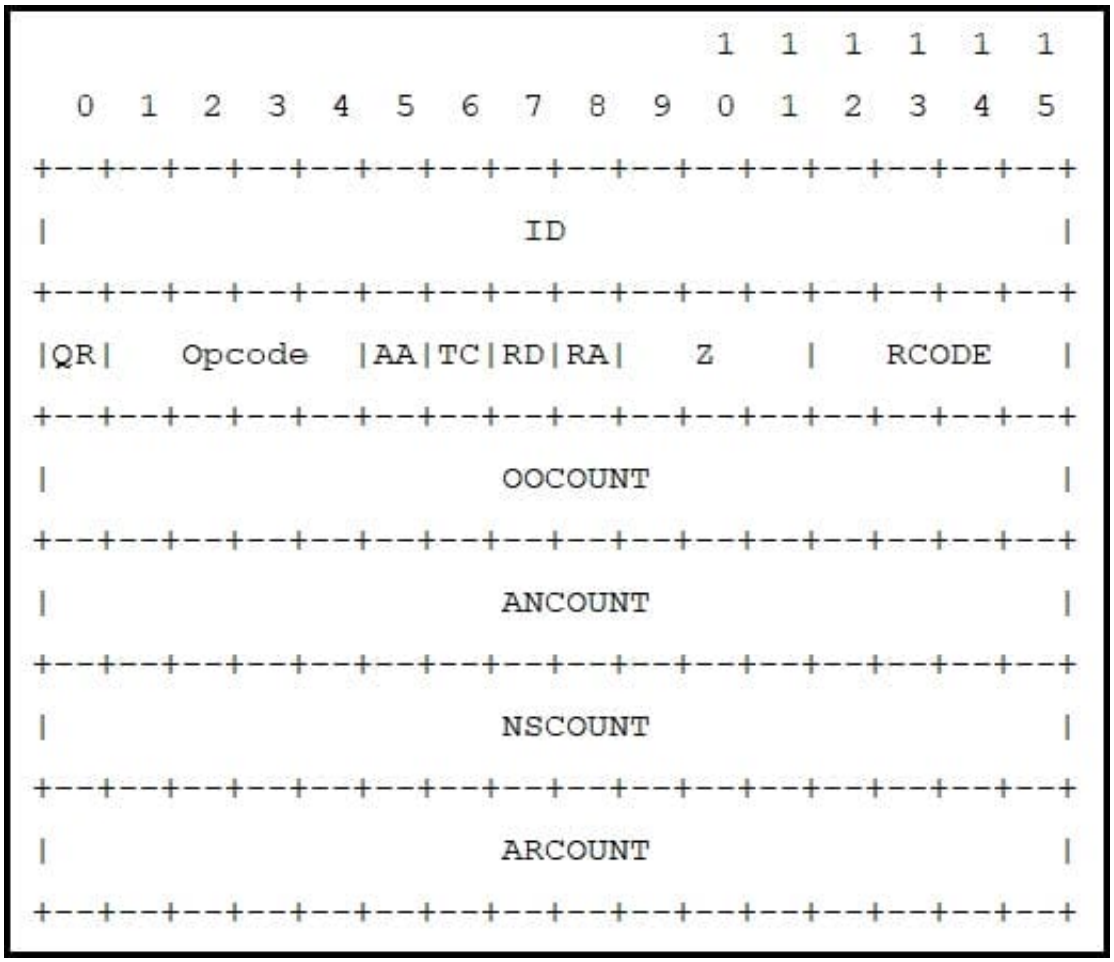
C. Gathered information on processes running on the server

D. Gathered a list of Active Directory users

Correct Answer: C

**QUESTION 3**

Refer to the exhibit.




Which field contains DNS header information if the payload is a query or response?

A. ID

B. Z

C. QR

D. TC

Correct Answer: C

**QUESTION 4**

A system administrator is ensuring that specific registry information is accurate.

Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

A. file extension associations

B. hardware, software, and security settings for the system

C. currently logged in users, including folders and control panel settings

D. all users on the system, including visual settings

Correct Answer: B

https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows- registry-advanced-users

**QUESTION 5**

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.

What is the initial event called in the NIST SP800-61?

A. online assault

B. precursor

C. trigger

D. instigator

Correct Answer: B

A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it\\'s important to know where you can find

both precursor and indicator sources of information.

The following are common sources of precursor and indicator information:

Security Information and Event Management (SIEM) Anti-virus and anti-spam software

File integrity checking applications/software

Logs from various sources (operating systems, devices, and applications) People who report a security incident

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf