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.geekcert.com/200-201.html

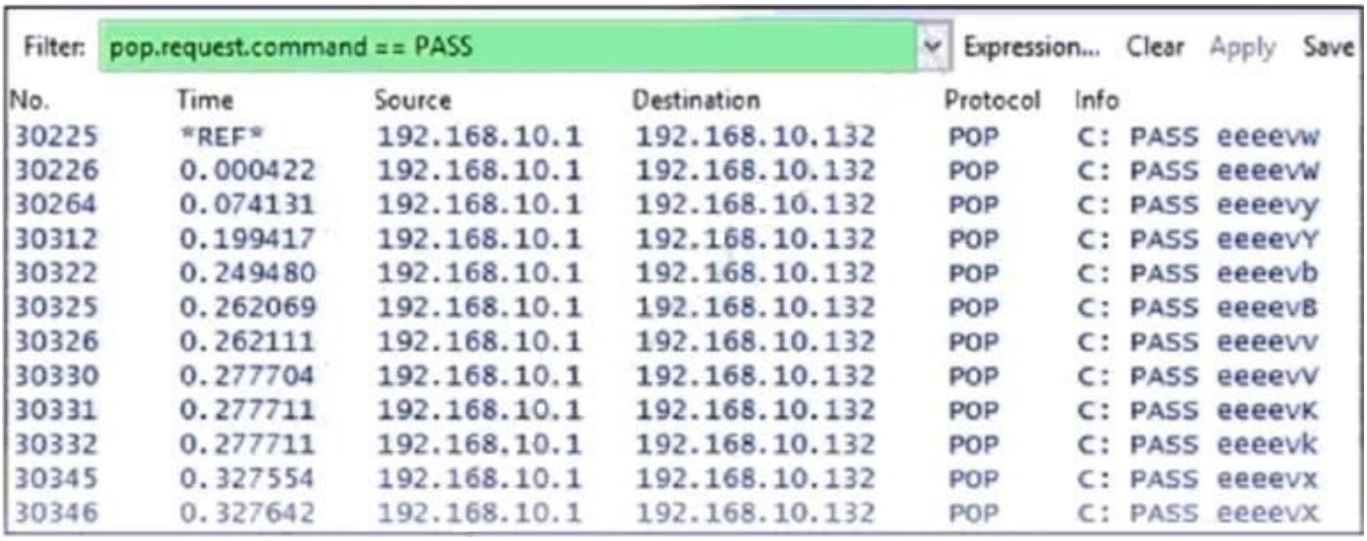
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Info
30225	*REF*	192.168.10.1	192.168.10.132	POP	C: PASS eeeevw
30226	0.000422	192.168.10.1	192.168.10.132	POP	C: PASS eeeevW
30264	0.074131	192.168.10.1	192.168.10.132	POP	C: PASS eeeevy
30312	0.199417	192.168.10.1	192.168.10.132	POP	C: PASS eeeevY
30322	0.249480	192.168.10.1	192.168.10.132	POP	C: PASS eeeevb
30325	0.262069	192.168.10.1	192.168.10.132	POP	C: PASS eeeevB
30326	0.262111	192.168.10.1	192.168.10.132	POP	C: PASS eeeevv
30330	0.277704	192.168.10.1	192.168.10.132	POP	C: PASS eeeevV
30331	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevK
30332	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevk
30345	0.327554	192.168.10.1	192.168.10.132	POP	C: PASS eeeevx
30346	0.327642	192.168.10.1	192.168.10.132	POP	C: PASS eeeevX

Which alert is identified from this packet capture?

A. man-in-the-middle attack

B. brute-force attack

C. ARP poisoning

D. SQL injection

Correct Answer: B

QUESTION 2

What matches the regular expression c(rgr)+e?

A. c(rgr)e

B. crgrrgre

C. crgr+e

D. ce

Correct Answer: B

QUESTION 3

Which process represents the application-level allow list?

A. allowing everything and denying specific executable files

B. allowing everything and denying specific applications protocols

C. allowing specific files and deny everything else

D. allowing specific format files and deny executable files

Correct Answer: C

QUESTION 4

What is the purpose of a ransomware attack?

A. to escalate privileges

B. to make files inaccessible by encrypting the data

C. to send keystrokes to a threat actor

D. to decrypt encrypted data and disks

Correct Answer: B

QUESTION 5

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

A. The average time the SOC takes to register and assign the incident.

B. The total incident escalations per week.

C. The average time the SOC takes to detect and resolve the incident.

D. The total incident escalations per month.

Correct Answer: C