200-201$^{Q\&As}$

Threat Hunting and Defending using Cisco Technologies for CyberOps (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

QUESTION 1

What is the function of a command and control server?

A. It enumerates open ports on a network device

B. It drops secondary payload into malware

C. It is used to regain control of the network after a compromise

D. It sends instruction to a compromised system

Correct Answer: D

QUESTION 2

One of the objectives of information security is to protect the CIA of information and systems.

What does CIA mean in this context?

A. confidentiality, identity, and authorization

B. confidentiality, integrity, and authorization

C. confidentiality, identity, and availability

D. confidentiality, integrity, and availability

Correct Answer: D

QUESTION 3

Which attack method intercepts traffic on a switched network?

A. denial of service

B. ARP cache poisoning

C. DHCP snooping

D. command and control

Correct Answer: C

QUESTION 4

What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset

B. the sum of all paths for data into and out of the environment

C. an exploitable weakness in a system or its design

D. the individuals who perform an attack

Correct Answer: B

QUESTION 5

Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required

B. user interaction

C. attack complexity

D. attack vector

Correct Answer: A

QUESTION 6

What causes events on a Windows system to show Event Code 4625 in the log messages?

A. The system detected an XSS attack

B. Someone is trying a brute force attack on the network

C. Another device is gaining root access to the system

D. A privileged user successfully logged into the system

Correct Answer: B

QUESTION 7

An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

A. management and reporting

B. traffic filtering

C. adaptive AVC

D. metrics collection and exporting

E. application recognition

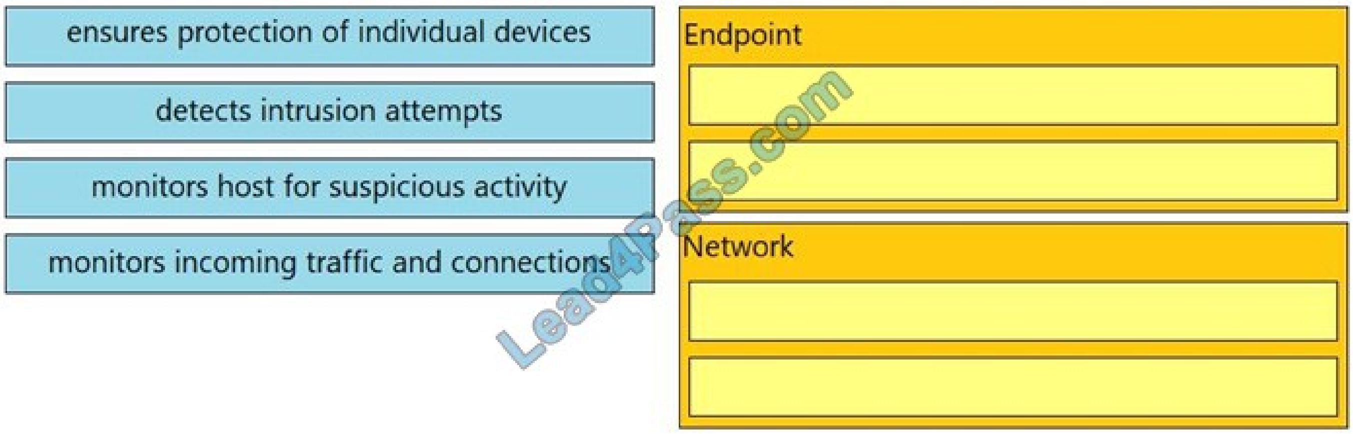
Correct Answer: DE

QUESTION 8

DRAG DROP

Drag and drop the uses on the left onto the type of security system on the right.

Select and Place:



ensures protection of individual devices

detects intrusion attempts

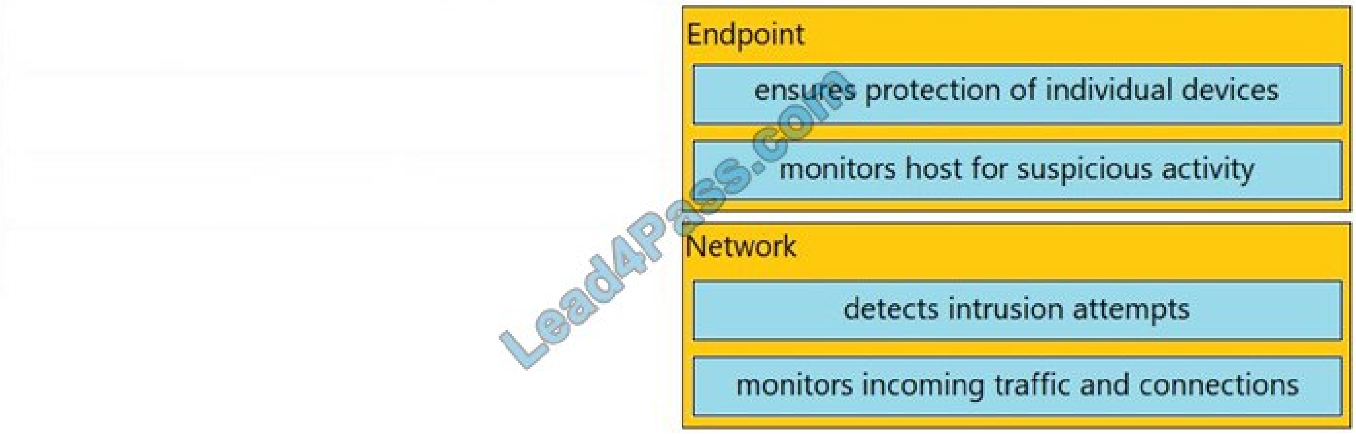
monitors host for suspicious activity

monitors incoming traffic and connections

Endpoint

Network

Correct Answer:



Endpoint

- ensures protection of individual devices
- monitors host for suspicious activity

Network

- detects intrusion attempts
- monitors incoming traffic and connections

QUESTION 9

Why is encryption challenging to security monitoring?

A. Encryption analysis is used by attackers to monitor VPN tunnels.

B. Encryption is used by threat actors as a method of evasion and obfuscation.

C. Encryption introduces additional processing requirements by the CPU.

D. Encryption introduces larger packet sizes to analyze and store.

Correct Answer: B

QUESTION 10

Which two elements are used for profiling a network? (Choose two.)

A. session duration

B. total throughput

C. running processes

D. listening ports

E. OS fingerprint

Correct Answer: DE

QUESTION 11

What is personally identifiable information that must be safeguarded from unauthorized access?

A. date of birth

B. driver\\'s license number

C. gender

D. zip code

Correct Answer: B

QUESTION 12

Which action prevents buffer overflow attacks?

A. variable randomization

B. using web based applications

C. input sanitization

D. using a Linux operating system

Correct Answer: C

QUESTION 13

A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows

B. CD data copy prepared in Mac-based system

C. CD data copy prepared in Linux system

D. CD data copy prepared in Android-based system

Correct Answer: A

QUESTION 14

An engineer needs to fetch logs from a proxy server and generate actual events according to the data received. Which technology should the engineer use to accomplish this task?

A. Firepower

B. Email Security Appliance

C. Web Security Appliance

D. Stealthwatch

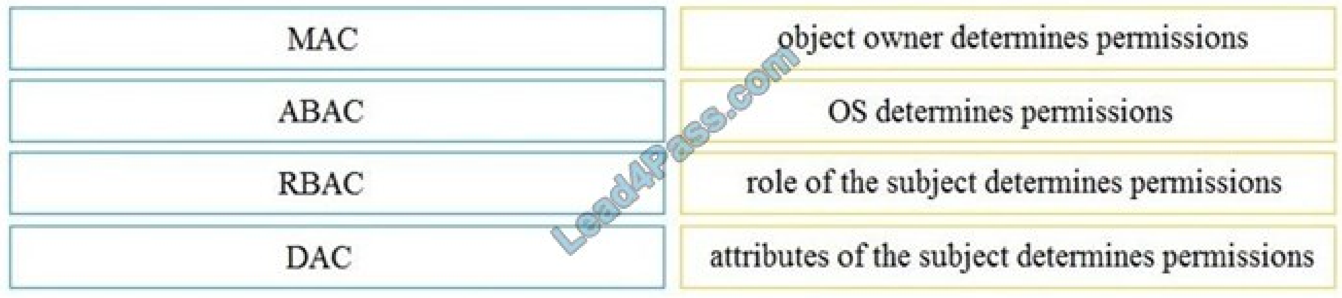
Correct Answer: D

QUESTION 15

DRAG DROP

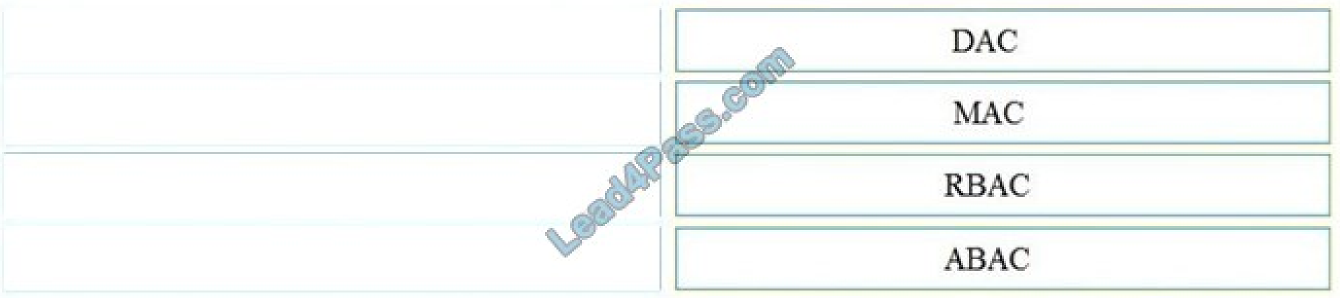
Drag and drop the access control models from the left onto the correct descriptions on the right.

Select and Place:



MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

Correct Answer:



	DAC
	MAC
	RBAC
	ABAC

[200-201 Practice Test](https://www.lead4pass.com/200-201.html) [200-201 Study Guide](https://www.lead4pass.com/200-201.html) [200-201 Exam Questions](https://www.lead4pass.com/200-201.html)

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

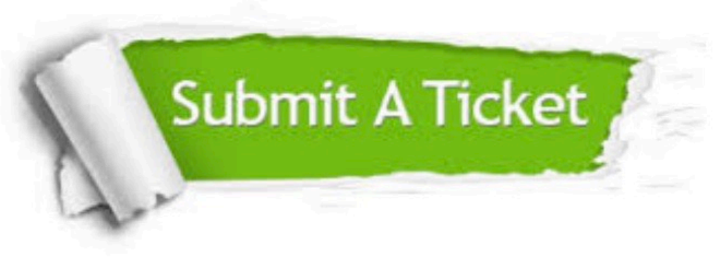
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.