

100% Money Back Guarantee

Vendor: Cisco

Exam Code: 210-255

Exam Name: Implementing Cisco Cybersecurity Operations

Version: Demo

QUESTION 1

Which network device creates and sends the initial packet of a session?

- A. source
- B. origination
- C. destination
- D. network

Correct Answer: A

QUESTION 2

In the context of incident handling phases, which two activities fall under scoping? (Choose two.)

- A. determining the number of attackers that are associated with a security incident
- B. ascertaining the number and types of vulnerabilities on your network
- C. identifying the extent that a security incident is impacting protected resources on the network
- D. determining what and how much data may have been affected
- E. identifying the attackers that are associated with a security incident

Correct Answer: DE

QUESTION 3

Which string matches the regular expression $r(ege)+x$?

- A. rx
- B. regeegex
- C. r(ege)x
- D. rege+x

Correct Answer: A

QUESTION 4

Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?

- A. Analysis Center
- B. National CSIRT
- C. Internal CSIRT
- D. Physical Security

Correct Answer: C

QUESTION 5

From a security perspective, why is it important to employ a clock synchronization protocol on a network?

- A. so that everyone knows the local time
- B. to ensure employees adhere to work schedule
- C. to construct an accurate timeline of events when responding to an incident
- D. to guarantee that updates are pushed out according to schedule

Correct Answer: D

QUESTION 6

Which element is part of an incident response plan?

- A. organizational approach to incident response
- B. organizational approach to security
- C. disaster recovery
- D. backups

Correct Answer: A

QUESTION 7

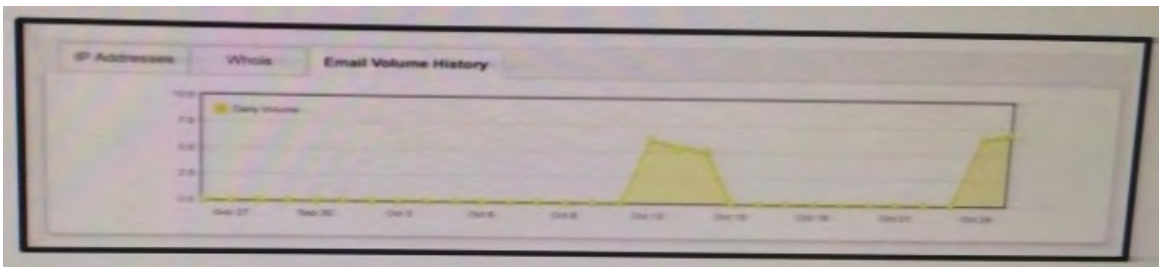
What mechanism does the Linux operating system provide to control access to files?

- A. privileges required
- B. user interaction
- C. file permissions
- D. access complexity

Correct Answer: C

QUESTION 8

Refer to the exhibit.



You notice that the email volume history has been abnormally high. Which potential result is true?

- A. Email sent from your domain might be filtered by the recipient.
- B. Messages sent to your domain may be queued up until traffic dies down.
- C. Several hosts in your network may be compromised.
- D. Packets may be dropped due to network congestion.

Correct Answer: C

QUESTION 9

Refer to the exhibit.

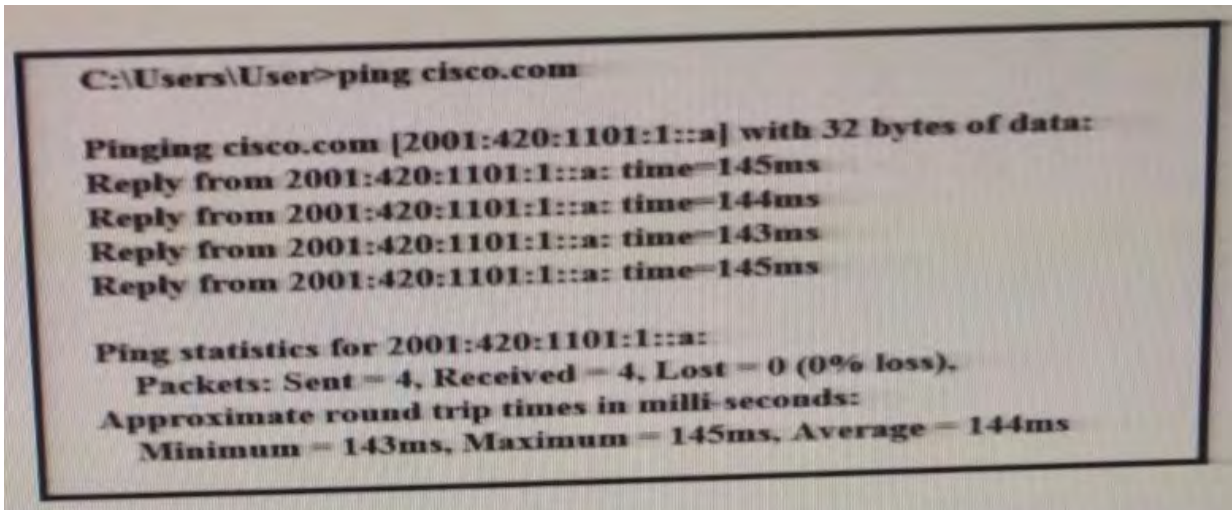
Date	FlowStart	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2016-10-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

Which type of log is this an example of?

- A. IDS log
- B. proxy log
- C. NetFlow log
- D. syslog

Correct Answer: A

QUESTION 10



Refer to the exhibit. What can be determined from this ping result?

- A. The public IP address of cisco.com is 2001:420:1101:1::a.
- B. The Cisco.com website is down.
- C. The Cisco.com website is responding with an internal IP.
- D. The public IP address of cisco.com is an IPv4 address.

Correct Answer: D

QUESTION 11

Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

- A. true positive
- B. true negative
- C. false positive
- D. false negative

Correct Answer: C

QUESTION 12

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: AE

QUESTION 13

Which goal of data normalization is true?

- A. Reduce data redundancy.
- B. Increase data redundancy.
- C. Reduce data availability.
- D. Increase data availability

Correct Answer: A

QUESTION 14

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

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying 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 **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

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.
---	---	--

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.