350-201^{Q&As}

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

https://www.passapply.com/350-201.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

A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

A. DLP for data in motion

B. DLP for removable data

C. DLP for data in use

D. DLP for data at rest

Correct Answer: C

Reference: https://www.endpointprotector.com/blog/what-is-data-loss-prevention-dlp/

QUESTION 2
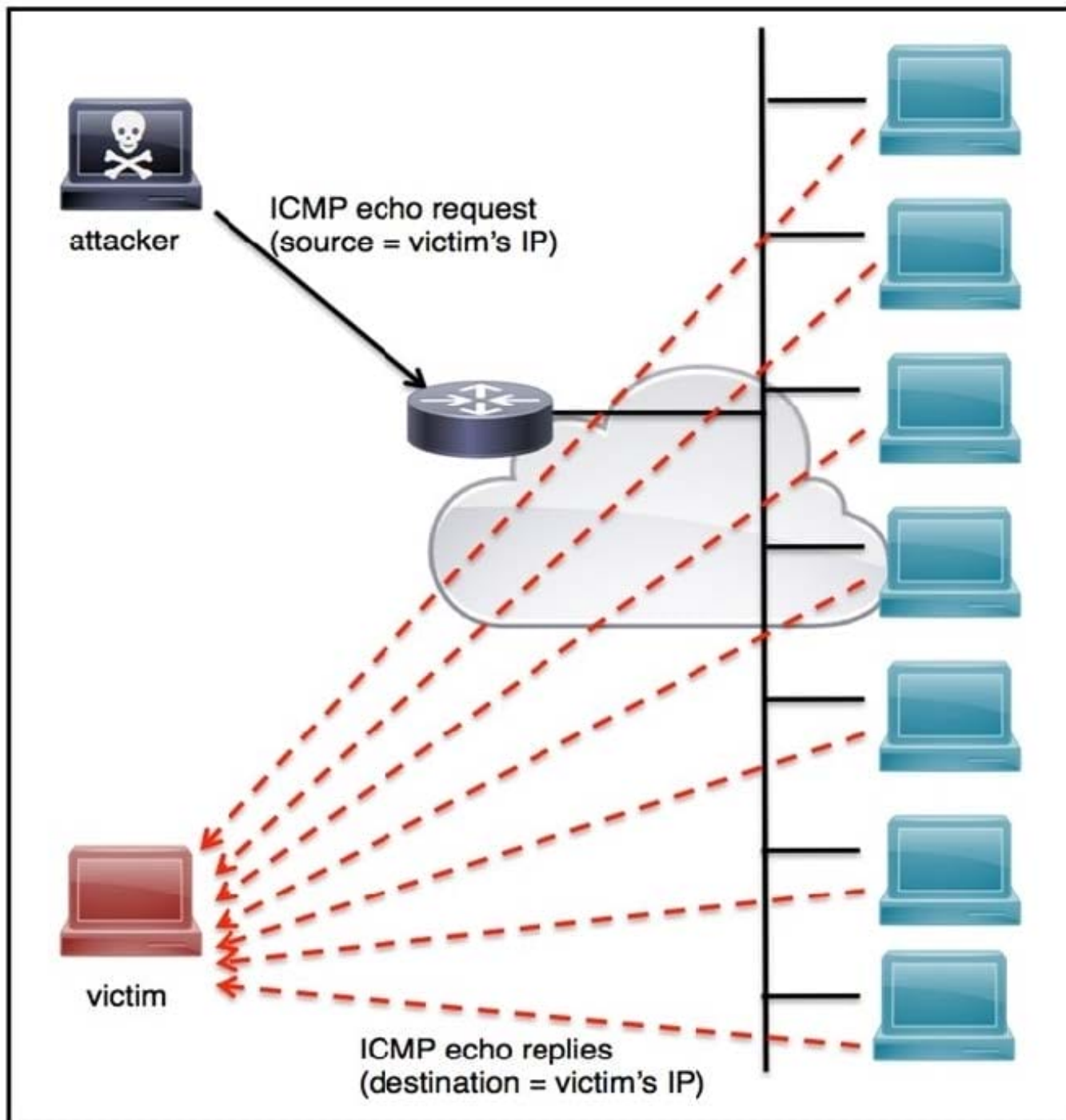
Refer to the exhibit. An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim\'s spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address.

Which action does the engineer recommend?

A. Use command ip verify reverse-path interface

B. Use global configuration command service tcp-keepalives-out

C. Use subinterface command no ip directed-broadcast

D. Use logging trap 6

Correct Answer: A

Reference: https://www.ccexpert.us/pix-firewall/ip-verify-reversepath-command.html

QUESTION 3

Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

A. customer data

B. internal database

C. internal cloud

D. Internet

Correct Answer: D

QUESTION 4

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal data. Which type of attack is occurring?

A. Address Resolution Protocol poisoning

B. session hijacking attack

C. teardrop attack

D. Domain Name System poisoning

Correct Answer: D

QUESTION 5

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

A. incident response playbooks

B. asset vulnerability assessment

C. report of staff members with asset relations

D. key assets and executives

E. malware analysis report

Correct Answer: BE

Reference: https://cloudogre.com/risk-assessment/