



# 350-201<sup>Q&As</sup>

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

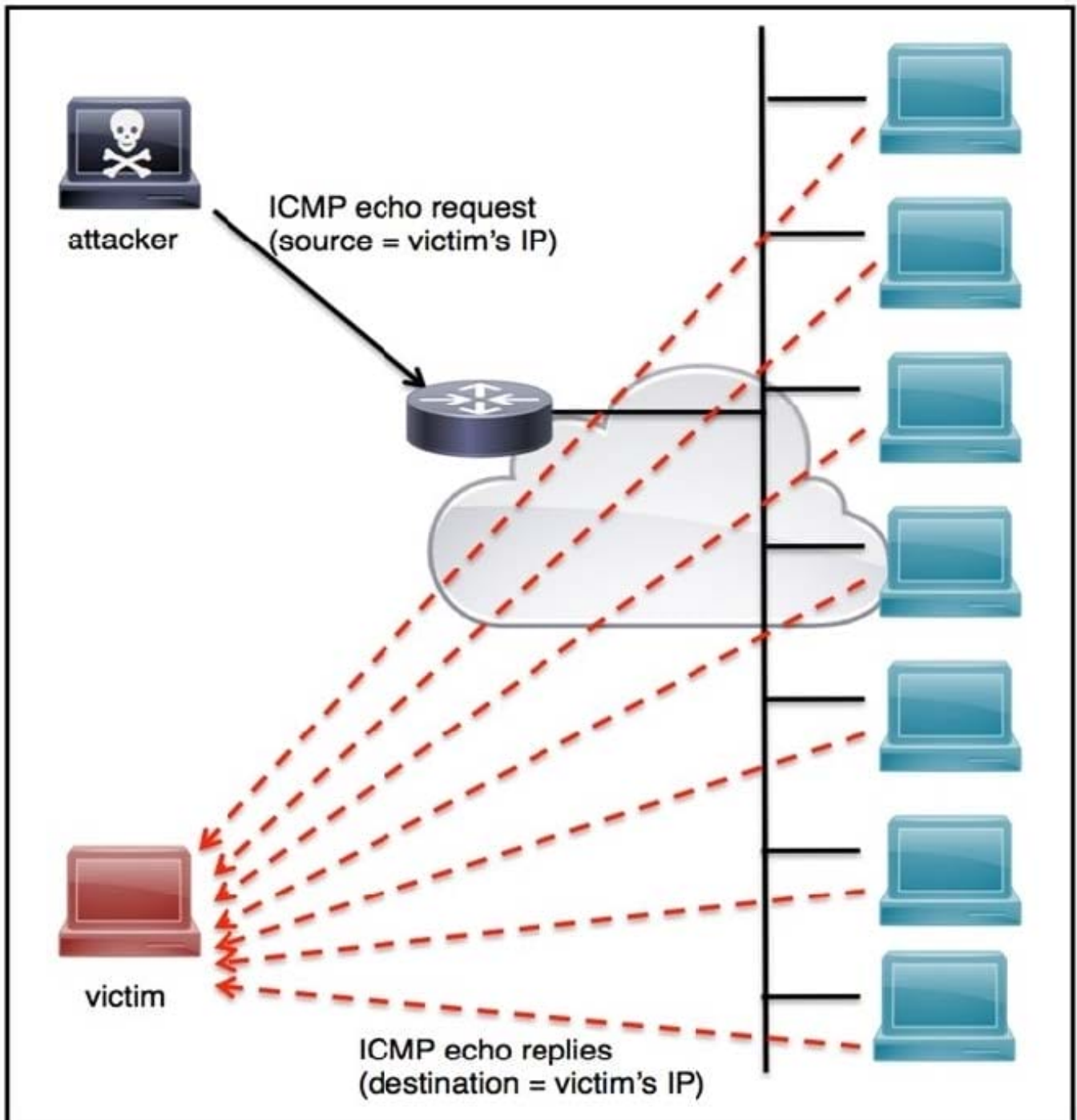
Following Questions and Answers are all new published by Cisco  
Official Exam Center

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





## QUESTION 1



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 2

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

- A. Command and Control, Application Layer Protocol, Duqu
- B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu
- C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu
- D. Discovery, System Network Configuration Discovery, Duqu

Correct Answer: A

---

## QUESTION 3

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server.

Which security solution is needed at this stage to mitigate the attack?

- A. web security solution
- B. email security solution
- C. endpoint security solution
- D. network security solution

Correct Answer: D

---

## QUESTION 4



Refer to the exhibit. A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

- A. packet sniffer
- B. malware analysis
- C. SIEM
- D. firewall manager

Correct Answer: A

## QUESTION 5





2024 Latest passapply 350-201 PDF and VCE dumps Download

The screenshot shows a hex editor window with the following details:

- Menu Bar:** File, Edit, View, Action, Help
- Toolbar:** Includes icons for file operations (New, Open, Save, Print, Find, Copy, Paste, Undo, Redo), a search icon, and a 'Dialog Manager' button.
- Left Pane (File List):**
  - BIN (selected)
  - 102 : 1033
  - Manifest
  - 1 : 1033
- Main Pane (Hex Dump):**

Offset	Hex Data
000198A8	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
000198B8	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
000198C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000198D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000198E8	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
000198F8	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
00019908	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
00019918	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00
00019928	A7 C4 76 F6 E3 A5 18 A5 E3 A5 18 A5 E3 A5 18 A5
00019938	E3 A5 19 A5 EB A5 18 A5 EA DD 8B A5 E6 A5 18 A5
00019948	EA DD 9B A5 E7 A5 18 A5 EA DD 89 A5 E2 A5 18 A5
00019958	52 69 63 68 E3 A5 18 A5 00 00 00 00 00 00 00 00
00019968	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00
00019978	F5 CC 51 56 00 00 00 00 00 00 00 00 00 00 02 01
- Right Pane (ASCII View):**

```

MZ
!
L !Th
is program cannot
be run in DOS
mode. &
v
Rich
PE L
QV
>@

```

Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

- A. a DOS MZ executable format
- B. a MS-DOS executable archive
- C. an archived malware
- D. a Windows executable file

Correct Answer: D

Reference: <https://stackoverflow.com/questions/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll->

```
files#::~text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.andtext=This  
%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.
```

[Latest 350-201 Dumps](#)

## 350-201 Practice Test

## 350-201 Study Guide