

# 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.pass2lead.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

Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)

- A. Evaluate the intrusion detection system alerts to determine the threat source and attack surface.
- B. Communicate with employees to determine who opened the link and isolate the affected assets.
- C. Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.
- D. Review the mail server and proxy logs to identify the impact of a potential breach.
- E. Check the email header to identify the sender and analyze the link in an isolated environment.

Correct Answer: CE

---

### QUESTION 2

Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?

SEARCH RESULTS FOR "malware distribution"

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	
malware malicious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2019 10:08:58 GMT-05:00	NEW
malware malicious host in 2 CONFIRMED	192.168.1.227	57 days long 66 days ago	Nov 16, 2019 10:07:23 GMT-05:00	NEW
malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2019 10:06:56 GMT-05:00	NEW

---

DASHBOARD CONFIRMED DETECTED

**MALWARE MALICIOUS HOST**  
 100% confidence, in #CSAL01  
 ★ NEW / TRIAGE

**AFFECTING**  
 unknown username  
 192.168.1.209

**OCCURRENCE**  
 3 days  
 Nov 13 – Nov 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

Activities (9 out of 10)	Domains (16 out of 17)	IPs (14 out of 15)	Autonomous systems (13 out of 14)
malicious host	accuro.cz	77.78.99.55	Casablanca INT
malicious server ip	alicanhotel.com	45.63.92.238	Choopa, LLC
malicious host from passive DNS	bay-bee.co.uk	185.119.173.220	UK Webhosting Ltd
malicious host	karakutid.com	31.192.214.161	Netinternet Bilisim Teknolojileri AS
malicious host	limkokwing-tomorrow.org	54.251.109.4	Amazon.com, Inc.
malicious host	manysernajd.com	212.76.85.26	Sahara Network
malicious host	barakamediaproduction.c... (48%)	68.158.222.206	NEW_JERSEY INTERNATIONAL INTC...
anomalous periodic communicat...	conserse.com.br	64.8.117.67	The Aldridge Company
	ymonline.com	69.49.115.40	

Time: 2 days, 18 hrs

- A. high risk level, anomalous periodic communication, quarantine with antivirus
- B. critical risk level, malicious server IP, run in a sandboxed environment
- C. critical risk level, data exfiltration, isolate the device
- D. high risk level, malicious host, investigate further

Correct Answer: A

**QUESTION 3**

An engineer detects an intrusion event inside an organization's network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?

- A. Disconnect the affected server from the network.
- B. Analyze the source.
- C. Access the affected server to confirm compromised files are encrypted.

D. Determine the attack surface.

Correct Answer: C

**QUESTION 4**

Refer to the exhibit. What is the connection status of the ICMP event?

Distribution Port/ICMP Code	Message	Classification	Application Protocol	Client	Application Risk	Business Relevance	Access Control Rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129.2.2)	Generic Protocol Command Decode	□ ICMP	□ ICMP client	Medium	Medium	rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129.2.2)	Generic Protocol Command Decode	□ DNS	□ DNS client	Very Low	Very High	Default Action
0 (No Code) / icmp	PROTOCOL-ICMP Echo Reply (1:408:8)	Misc Activity	□ DNS	□ DNS client	Very Low	Very High	Allow ICMP
54107 / udp	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt (3:19187:7)	Attempted User Privilege Gain	□ DNS	□ DNS client	Very Low	Very High	
49367 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
57477 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
54879 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
60999 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
52240 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
54359 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
52489 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
60169 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
52250 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
52485 / up	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
49940 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
57214 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
51608 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
52652 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
55528 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
61222 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
55640 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	
55991 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	□ DNS	□ DNS client	Very Low	Very High	

- A. blocked by a configured access policy rule
- B. allowed by a configured access policy rule
- C. blocked by an intrusion policy rule
- D. allowed in the default action

Correct Answer: B

---

#### QUESTION 5

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 6

A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross-correlated log analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?

- A. Disable BIND forwarding from the DNS server to avoid reconnaissance.
- B. Disable affected assets and isolate them for further investigation.
- C. Configure affected devices to disable NETRJS protocol.
- D. Configure affected devices to disable the Finger service.

Correct Answer: D

---

#### QUESTION 7

How does Wireshark decrypt TLS network traffic?

- A. with a key log file using per-session secrets
- B. using an RSA public key
- C. by observing DH key exchange
- D. by defining a user-specified decode-as

Correct Answer: A

Reference: <https://wiki.wireshark.org/TLS>

**QUESTION 8**

<p><b><u>Vulnerability #1</u></b> A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:</p> <ul style="list-style-type: none"><li>a) Be logged in to the device over telnet or SSH, or through the local console</li><li>b) Be logged in as a high-privileges administrative user</li></ul> <p>In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.</p> <p>All software versions are affected Fixes are available now There are no workarounds or mitigations</p>	<p><b><u>Vulnerability #2</u></b> A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to:</p> <ul style="list-style-type: none"><li>a) Be able to reach port 80/tcp on an affected device</li><li>b) The web-based management interface needs to be enabled on the device</li></ul> <p>The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack.</p> <p>All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.</p>
--	---

Refer to the exhibit. How must these advisories be prioritized for handling?

- A. The highest priority for handling depends on the type of institution deploying the devices
- B. Vulnerability #2 is the highest priority for every type of institution
- C. Vulnerability #1 and vulnerability #2 have the same priority
- D. Vulnerability #1 is the highest priority for every type of institution

Correct Answer: D

**QUESTION 9**



**QUESTION 11**

The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?

- A. eradication and recovery
- B. post-incident activity
- C. containment
- D. detection and analysis

Correct Answer: A

**QUESTION 12**

DRAG DROP

Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

Select and Place:

**Answer Area**

build	Phase 1
release	Phase 2
deploy	Phase 3
operate	Phase 4
monitor	Phase 5
test	Phase 6
plan	Phase 7
develop	Phase 8



Correct Answer:

**Answer Area**


- plan
- develop
- build
- test
- release
- deploy
- operate
- monitor

**QUESTION 13**

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight.

Which type of compromise is indicated?

- A. phishing
- B. dumpster diving
- C. social engineering
- D. privilege escalation

Correct Answer: C

**QUESTION 14**

A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?

- A. Create a follow-up report based on the incident documentation.
- B. Perform a vulnerability assessment to find existing vulnerabilities.
- C. Eradicate malicious software from the infected machines.
- D. Collect evidence and maintain a chain-of-custody during further analysis.

Correct Answer: D

---

**QUESTION 15**

A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

- A. Determine the systems involved and deploy available patches
- B. Analyze event logs and restrict network access
- C. Review access lists and require users to increase password complexity
- D. Identify the attack vector and update the IDS signature list

Correct Answer: B

[Latest 350-201 Dumps](#)

[350-201 Study Guide](#)

[350-201 Exam Questions](#)