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

QUESTION 1

Refer to the exhibit. An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable.

What does this STIX indicate?

A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible

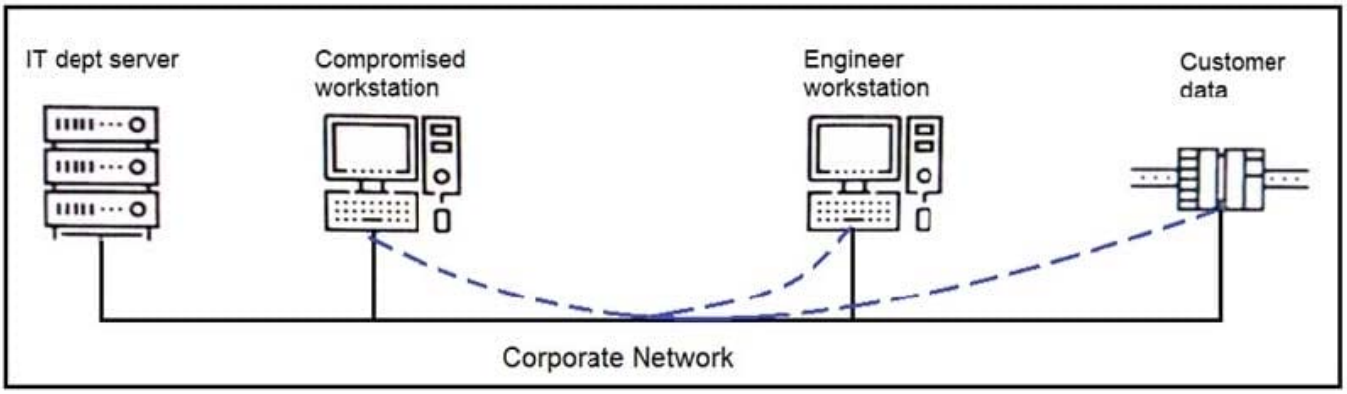
B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information

C. There is a possible data leak because payloads should be encoded as UTF-8 text

D. There is a malware that is communicating via encrypted channels to the command and control server

Correct Answer: C

QUESTION 2



Refer to the exhibit. An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols

B. Deploy a SOAR solution and correlate log alerts from customer zones

C. Deploy IDS within sensitive areas and continuously update signatures

D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Correct Answer: A

QUESTION 3

What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface

B. to create the logic that triggers alerts when anomalies occur

C. to identify vulnerabilities within an operating system

D. to analyze attacks to identify threat actors and points of entry

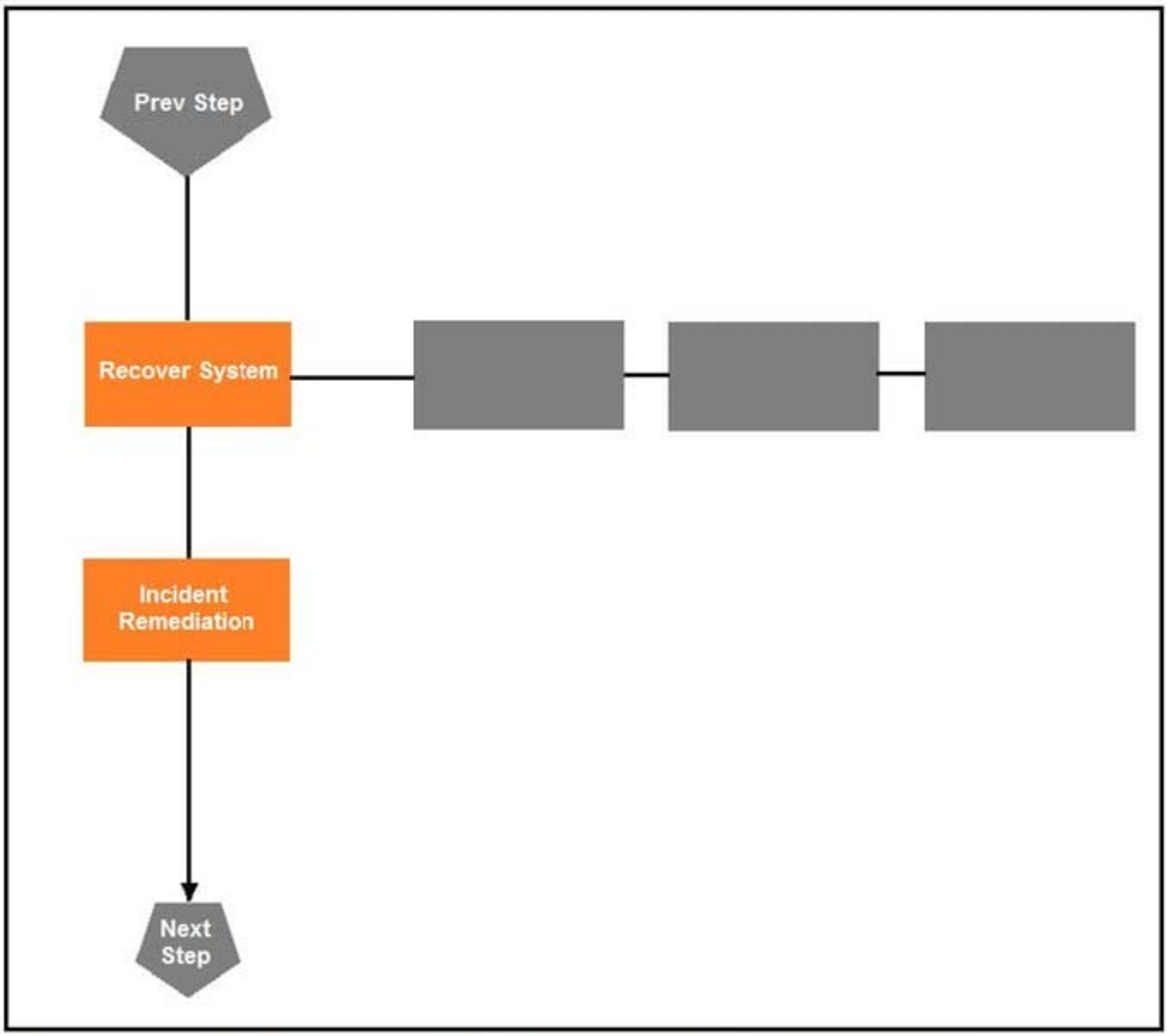
Correct Answer: A

QUESTION 4

DRAG DROP

Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.

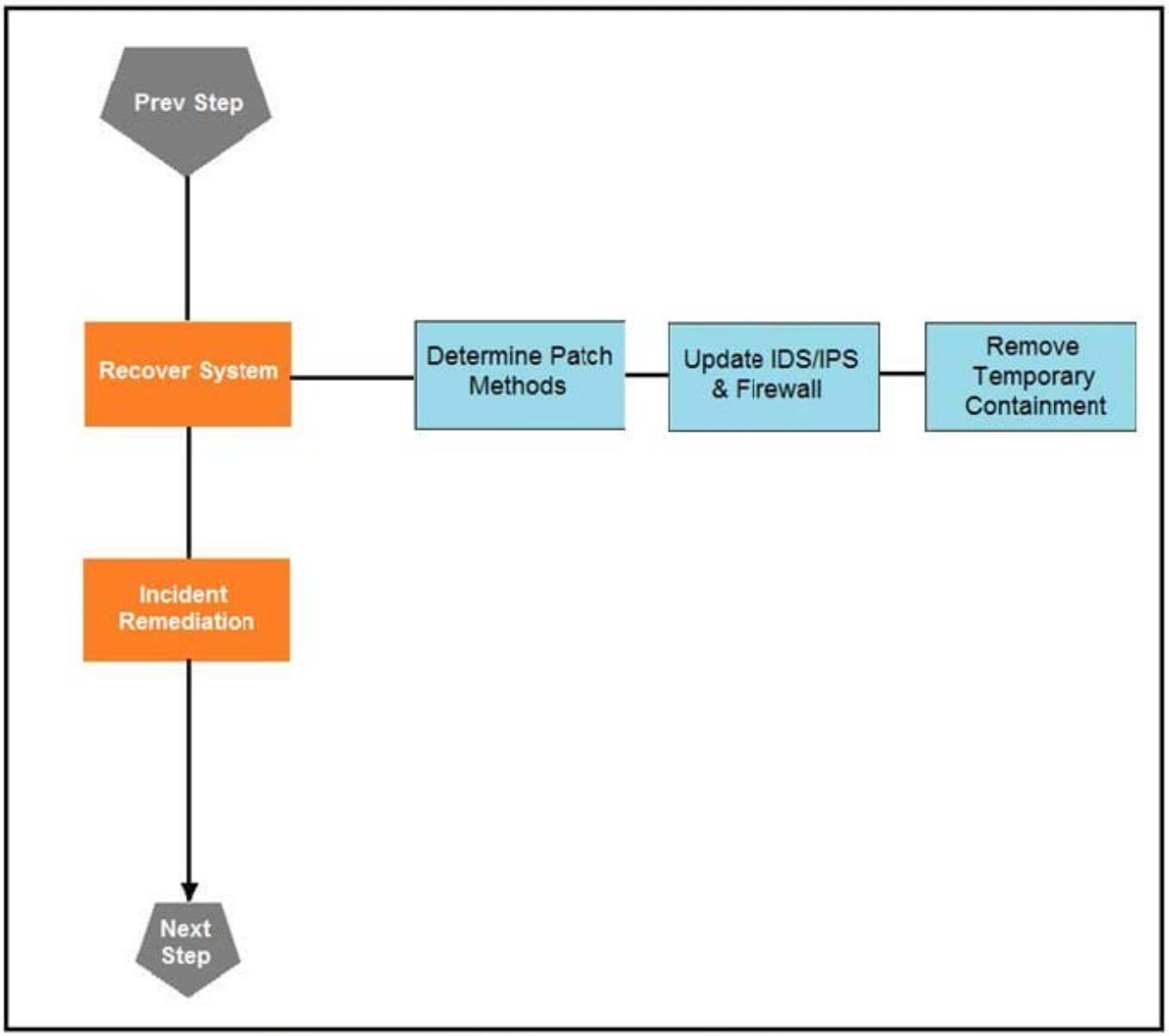
Select and Place:

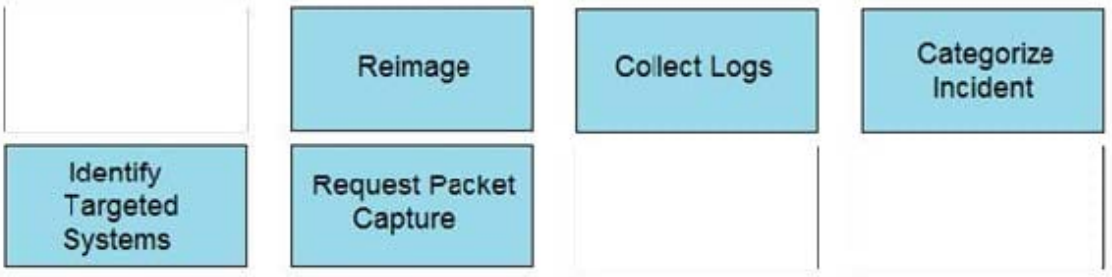


Update IDS/IPS & Firewall | Reimage | Collect Logs | Categorize Incident

Identify Targeted Systems | Request Packet Capture | Remove Temporary Containment | Determine Patch Methods

Correct Answer:





QUESTION 5

An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to prevent this type of attack from reoccurring? (Choose two.)

A. Implement a patch management process.

B. Scan the company server files for known viruses.

C. Apply existing patches to the company servers.

D. Automate antivirus scans of the company servers.

E. Define roles and responsibilities in the incident response playbook.

Correct Answer: DE