350-201$^{\text{Q\&As}}$

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

QUESTION 1

An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions

B. Unpack the file in a sandbox to see how it reacts

C. Research the malware online to see if there are noted findings

D. Disassemble the malware to understand how it was constructed

Correct Answer: C

QUESTION 2

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 3

An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials.

How should the workflow be improved to resolve these issues?

A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts

B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats

C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts

D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Correct Answer: B

QUESTION 4

An analyst received multiple alerts on the SIEM console of users that are navigating to malicious URLs. The analyst needs to automate the task of receiving alerts and processing the data for further investigations. Three variables are available from the SIEM console to include in an automation script: console_ip, api_token, and reference_set_name. What must be added to this script to receive a successful HTTP response?

#!/usr/bin/pythonimport sysimport requests

A. {1}, {2}

B. {1}, {3}

C. console_ip, api_token

D. console_ip, reference_set_name

Correct Answer: C

QUESTION 5

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates

B. Update the IDS/IPS signatures and reimage the affected hosts

C. Identify the systems that have been affected and tools used to detect the attack

D. Identify the traffic with data capture using Wireshark and review email filters

Correct Answer: C

350-201 VCE Dumps 350-201 Practice Test 350-201 Exam Questions