Cisco

300-220

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

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

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: 2

Refer to the exhibit.

```
84.55.41.57 - - [14/Apr/2016:08:22:27 0100]
"GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1
UNION ALL SELECT CONCAT(0x7171787671,x537653544175467a724f,0x71707a7871) ,
NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
```

A forensic team must investigate how the company website was defaced. The team isolates the web server, clones the disk, and analyzes the logs. Which technique was used by the attacker initially to access the website?

A. exploit public-facing application
B. external remote services
C. command and scripting interpreter
D. drive-by compromise

Answer: A

Explanation:
The correct answer is Exploit public-facing application. The log excerpt in the exhibit clearly shows a malicious HTTP GET request targeting a WordPress plugin PHP file with a crafted SQL injection payload:
UNION ALL SELECT CONCAT(...)
This syntax is a classic indicator of SQL injection, a well-documented attack technique used to exploit insufficient input validation in web applications. According to the MITRE ATT&CK framework, this behavior maps to the Initial Access tactic (TA0001) and the technique Exploit Public-Facing Application (T1190). The attacker is directly interacting with a publicly accessible web service and abusing a vulnerability in the application code to gain unauthorized access.
From a threat hunting and forensic standpoint, this is a textbook example of how attackers commonly achieve initial access to web servers. The attacker did not authenticate via remote services (such as SSH or RDP), nor did they rely on user interaction (as in a drive-by compromise). Instead, they sent a specially crafted request to a vulnerable endpoint exposed to the internet. This makes option B incorrect because External Remote Services requires legitimate service access mechanisms. Option C is also incorrect because Command and Scripting Interpreter is typically used after initial access, once code execution is already achieved. Option D does not apply because there is no evidence of malicious content being delivered to end users.
The forensic team's actions—isolating the server, cloning the disk, and analyzing logs—are standard post-incident procedures to reconstruct the attack chain. Web server access logs are especially valuable in these cases, as they often reveal malicious payloads, attacker IP addresses, targeted endpoints, and timestamps.
For defenders and threat hunters, this scenario reinforces the importance of monitoring web logs for anomalous query strings, enforcing secure coding practices, conducting regular vulnerability scans, and promptly patching third-party plugins. Public-facing applications remain one of the most exploited initial access vectors, making this technique a critical focus area in modern threat hunting programs.

Question: 3

The security team detects an alert regarding a potentially malicious file named Financial_Data_526280622.pdf downloaded by a user. Upon reviewing SIEM logs and Cisco Secure Endpoint, the team confirms that the file was obtained from an untrusted website. The hash analysis of the file returns an unknown status. Which action must be done next?

A. Submit the file for sandboxing.
B. Review the directory path where the file is stored.
C. Run a complete malware scan on the user's workstation.
D. Investigate the reputation of the untrusted website.

Answer: A

Explanation:
The correct next action is to submit the file for sandboxing. In professional security operations and threat hunting workflows, sandboxing is the most appropriate step when a file originates from an untrusted source and hash-based reputation checks return an unknown result. An unknown hash means the file has not yet been classified as benign or malicious by threat intelligence databases, which is common with newly created malware or targeted attacks.
Sandboxing allows the security team to perform dynamic analysis by executing the file in an isolated, controlled environment. This process observes runtime behaviors such as process creation, registry modification, network communications, command-and-control callbacks, file system changes, and exploit attempts. These behaviors provide high-fidelity indicators that static analysis or hash lookups cannot reveal.
Option B, reviewing the directory path, is useful for contextual awareness but does not determine whether the file is malicious. Option C, running a full malware scan, is premature; modern malware often evades signature-based scans, especially when the file is previously unknown. Option D, investigating the reputation of the website, is a supporting activity but does not assess the actual behavior or payload of the downloaded file.
From a threat hunting and incident response standpoint, sandboxing bridges the gap between detection and confirmation. If the sandbox analysis confirms malicious behavior, the team can escalate to containment actions such as isolating the endpoint, blocking hashes and domains, and performing scope analysis to identify other affected systems. Additionally, sandbox results can be used to create new SIEM detections and EDR behavioral rules, strengthening future defenses.
This approach aligns with professional best practices: unknown file + untrusted source = dynamic analysis first. It ensures accurate classification while minimizing unnecessary disruption to the user or environment.

Question: 4

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, SMBbased 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 credentialbased
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: 5

The SOC team receives an alert about a user sign-in from an unusual country. After investigating the SIEM logs, the team confirms the user never signed in from that country. The incident is reported to the IT administrator who resets the user's password. Which threat hunting phase was initially used?

A. Collect and process intelligence and data
B. Response and resolution
C. Hypothesis
D. Post-incident review

Answer: A

Explanation:
The correct answer is Collect and process intelligence and data. In this scenario, the initial threat hunting phase occurred when the SOC team received the alert and began analyzing SIEM logs to validate whether the activity was legitimate or malicious. This aligns directly with the first phase of the threat hunting lifecycle, which focuses on gathering, normalizing, and analyzing security-relevant data.
Threat hunting is a structured, hypothesis-driven process, but it always begins with data collection and intelligence processing. This includes ingesting logs from identity providers, authentication systems, cloud platforms, VPNs, and endpoint telemetry into a SIEM. In this case, the alert regarding a sign-in from an unusual country triggered analysts to examine historical login patterns and geolocation data. By confirming that the user had never authenticated from that country, the team established that the event was anomalous and likely malicious.
Option B (Response and resolution) occurred after the initial phase, when the IT administrator reset the user's password to contain the threat. Option C (Hypothesis) would involve formulating a theory such as "the account may be compromised due to credential theft," but this step requires validated data first. Option D (Post-incident review) only happens after the incident has been fully resolved and lessons learned are documented.
From a professional cybersecurity operations perspective, this phase is critical because high-quality data determines hunt effectiveness. Poor log coverage or incomplete identity telemetry would prevent analysts from confidently confirming the anomaly. This example also highlights why identityrelated telemetry is foundational to modern threat hunting—compromised credentials remain one of the most common initial access vectors.
In short, before a SOC can hypothesize, respond, or improve controls, it must first collect and process accurate intelligence and data, making option A the correct answer.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/