



**Vendor:** Cisco

**Exam Code:** 300-220

**Exam Name:** Conducting Threat Hunting and Defending  
using Cisco Technologies for CyberOps

**Version:** DEMO

## QUESTION 1

What triggers unstructured threat hunting?

- A. Indicators of compromise
- B. Tactics, techniques, and procedures
- C. Customized threat identification
- D. Indicators of attack

**Answer: D**

**Explanation:**

The correct answer is Indicators of attack (IOAs). Unstructured threat hunting is typically triggered by weak signals, anomalies, or suspicious behaviors that do not yet meet the threshold of confirmed compromise. These early signals are best described as indicators of attack rather than indicators of compromise.

## QUESTION 2

Refer to the exhibit. A security engineer notices that a Windows Batch script includes calls to suspicious APIs. How will the script affect the system when it is executed?

```
1  sleep
2  encode
3  %02x %s?i=%s&c=%s&p=%s
4  APPDATA
5  Software\Microsoft\Windows\CurrentVersion\Run
6  brbbot
7  Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
8  HTTP/1.1 Connection: close
9  ZwQuerySystemInformation
10 ntdll.dll
11 RegSetValueExA
12 RegOpenKeyExA
13 RegDeleteValueA
14 RegFlushKey
15 RegCloseKey
16 CryptAcquireContextW
17 CryptDeriveKey
18 CryptReleaseContext
19 CryptEncrypt
20 CryptCreateHash
21 CryptDestroyKey
22 CryptDecrypt
23 CryptDestroyHash
24 CryptHashData
25 ADVAPI32.dll
26 InternetQueryDataAvailable
27 InternetReadFile
28 InternetCloseHandle
```

- A. The internet connection is disabled.
- B. The host version is retrieved.
- C. The host is put in sleep mode.
- D. Files are encrypted.

**Answer: D**

**Explanation:**

The correct answer is Files are encrypted. The exhibit shows a collection of API calls and strings that strongly indicate cryptographic operations associated with file encryption, a common behavior in ransomware and data-encrypting malware.

Key indicators in the script include multiple Windows Cryptographic API function calls such as:

CryptAcquireContextW

CryptCreateHash

CryptHashData

CryptDeriveKey

CryptEncrypt

CryptDecrypt

CryptDestroyKey

CryptReleaseContext

These APIs are part of the Windows CryptoAPI, which is explicitly used to generate cryptographic keys, hash data, and encrypt or decrypt content. The presence of ADVAPI32.dll further confirms cryptographic functionality, as this library provides access to Windows security and encryption services.

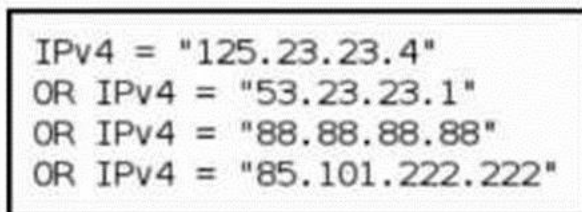
Additionally, registry-related APIs such as RegSetValueExA, RegOpenKeyExA, and references to:

Software\Microsoft\Windows\CurrentVersion\Run

indicate that the script may also establish persistence, ensuring the encryption routine executes again after reboot. However, persistence is secondary; the primary functional behavior shown is encryption.

**QUESTION 3**

Refer to the exhibit. 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?



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

- 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.

#### QUESTION 4

A SOC manager wants to evaluate whether the organization's Cisco-based threat hunting program is improving over time. Which metric BEST reflects increased threat hunting effectiveness?

- A. Number of alerts generated by Cisco security tools
- B. Reduction in attacker dwell time
- C. Number of blocked IP addresses
- D. Volume of threat intelligence feeds consumed

**Answer: B**

**Explanation:**

The correct answer is reduction in attacker dwell time. Dwell time measures how long an attacker remains undetected after initial compromise.

As threat hunting maturity increases:

Behavioral coverage improves

Detection occurs earlier in the attack lifecycle

Attackers are identified before achieving objectives

#### QUESTION 5

A threat hunter wants to detect fileless malware activity using Cisco Secure Endpoint. Which behavior would MOST strongly indicate fileless execution?

- A. Executables running from Program Files

- B. Processes spawning from user-writable directories
- C. Legitimate system processes executing encoded commands
- D. Files with unknown hash reputation

**Answer: C**

**Explanation:**

The correct answer is legitimate system processes executing encoded commands. Fileless malware avoids writing binaries to disk and instead abuses trusted processes such as PowerShell, WMI, or rundll32.

Encoded or obfuscated commands executed by legitimate binaries are a strong indicator of fileless execution and defense evasion. Cisco Secure Endpoint provides deep visibility into command-line arguments and process behavior, enabling detection of this technique.

**QUESTION 6**

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 7

Refer to the exhibit. 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?

```
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. 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.

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**