Cisco

300-215

Conducting Forensic Analysis and Incident Response Using Cisco CyberOps Technologies (CBRFIR)

Latest Version: 7.0

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	Source	Destination	Protocol	Length	Info
2708...	351.613329	167.203.102.117	192.168.1.159	TCP	174	15120 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.614781	52.27.161.215	192.168.1.159	TCP	174	15409 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615356	209.92.25.229	192.168.1.159	TCP	174	15701 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615473	149.221.46.147	192.168.1.159	TCP	174	15969 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.616366	192.183.44.102	192.168.1.159	TCP	174	16247 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.617248	152.178.159.141	192.168.1.159	TCP	174	16532 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618094	203.98.141.133	192.168.1.159	TCP	174	16533 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618857	115.48.48.185	192.168.1.159	TCP	174	16718 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.619789	147.29.251.74	192.168.1.159	TCP	174	17009 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.620622	29.158.7.85	192.168.1.159	TCP	174	17304 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.621398	133.119.25.131	192.168.1.159	TCP	174	17599 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.622245	89.99.115.209	192.168.1.159	TCP	174	17874 –> 80 [SYN] Seq=0 Win=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...	351.624003	124.97.107.209	192.168.1.159	TCP	174	18448 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624765	140.147.97.13	192.168.1.159	TCP	174	18740 –> 80 [SYN] Seq=0 Win=64 Len=120 [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.

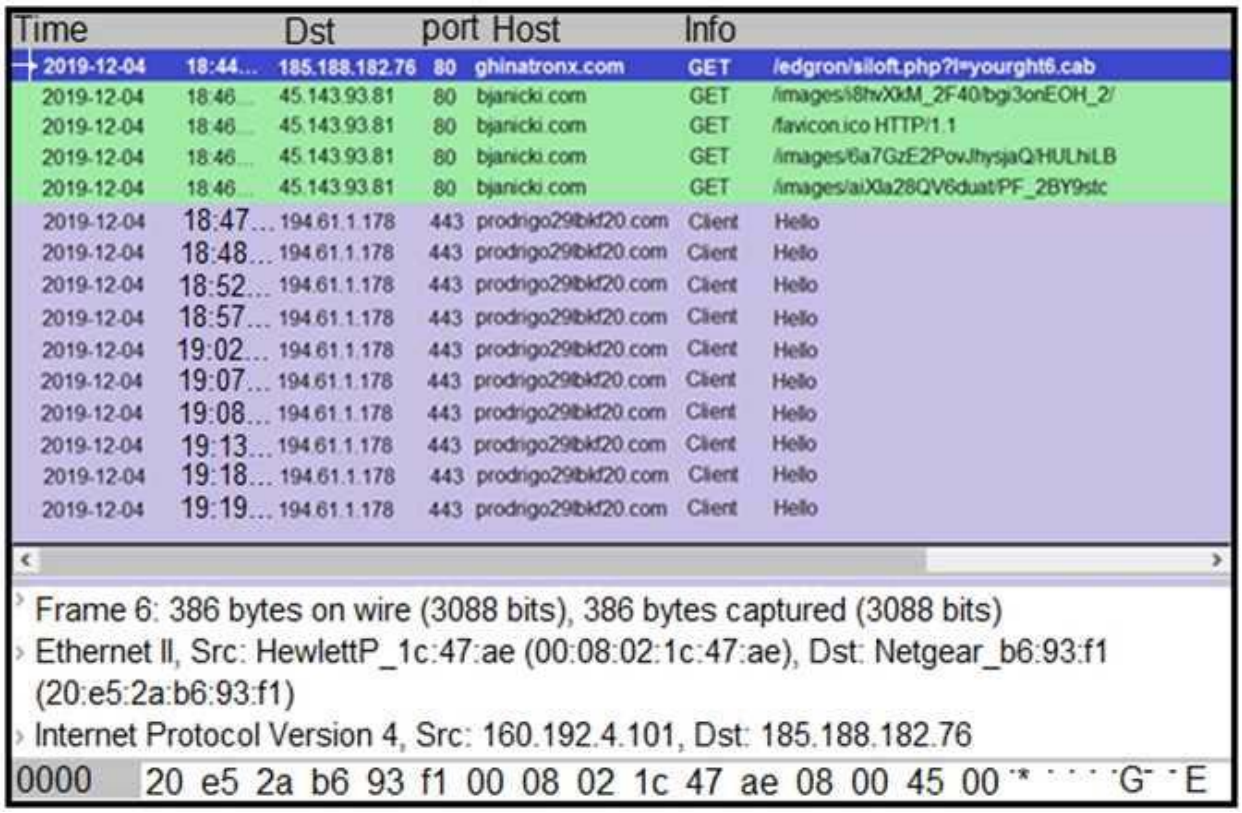
Answer: A

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

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).

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer