Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

https://www.2passeasy.com/dumps/CS0-003/

NEW QUESTION 1
- (Exam Topic 1)
A security analyst is reviewing the following log from an email security service.

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

Answer: C

Explanation:
Reference: https://www.webopediA.com/TERM/R/RBL.html

NEW QUESTION 2
- (Exam Topic 1)
It is important to parameterize queries to prevent:

A. the execution of unauthorized actions against a database.
B. a memory overflow that executes code with elevated privileges.
C. the esrtablishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Answer: A

Explanation:
Reference: https://stackoverflow.com/QUESTION NO:s/4712037/what-is-parameterized-query

NEW QUESTION 3
- (Exam Topic 1)
Which of the following types of policies is used to regulate data storage on the network?

A. Password
B. Acceptable use
C. Account management
D. Retention

Answer: D

Explanation:

Reference:
http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION 4
- (Exam Topic 1)
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

A. Reverse engineering
B. Fuzzing
C. Penetration testing
D. Network mapping

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee Pll on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

A. the public relations department
B. senior leadership
C. law enforcement
D. the human resources department

Answer: D

NEW QUESTION 6
- (Exam Topic 1)
A security analyst received an email with the following key: Xj3XJ3LLc
A second security analyst received an email with following key: 3XJ3xjcLLC
The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance.
This is an example of:

A. dual control
B. private key encryption
C. separation of duties
D. public key encryption
E. two-factor authentication

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
Which of the following is the MOST important objective of a post-incident review?

A. Capture lessons learned and improve incident response processes
B. Develop a process for containment and continue improvement efforts
C. Identify new technologies and strategies to remediate
D. Identify a new management strategy

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

A. Motion detection
B. Perimeter fencing
C. Monitored security cameras
D. Badged entry

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

A. Data encoding
B. Data masking
C. Data loss prevention
D. Data classification

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

A. Self-encrypting drive
B. Bus encryption
C. TPM
D. HSM

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

A. Post of the company blog
B. Corporate-hosted encrypted email
C. VoIP phone call
D. Summary sent by certified mail
E. Externally hosted instant message

Answer: C

NEW QUESTION 13
- (Exam Topic 1)
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised.
Which of the following is the value of this risk?

A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Answer: A

NEW QUESTION 16
- (Exam Topic 1)
A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.
Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

A. Development of a hypothesis as part of threat hunting
B. Log correlation, monitoring, and automated reporting through a SIEM platform
C. Continuous compliance monitoring using SCAP dashboards
D. Quarterly vulnerability scanning using credentialed scans

Answer: A

NEW QUESTION 20
- (Exam Topic 1)
An organization developed a comprehensive modern response policy Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

A. A simulated breach scenario evolving the incident response team
B. Completion of annual information security awareness training by ail employees
C. Tabtetop activities involving business continuity team members
D. Completion of lessons-learned documentation by the computer security incident response team
E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 24
- (Exam Topic 1)
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.
Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating datA.

Answer: D

NEW QUESTION 28
- (Exam Topic 1)
A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

A. Begin blocking all IP addresses within that subnet.
B. Determine the attack vector and total attack surface.
C. Begin a kill chain analysis to determine the impact.
D. Conduct threat research on the IP addresses

Answer: D

NEW QUESTION 33
- (Exam Topic 1)
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)

B)

C)

D)

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

Answer: B

NEW QUESTION 34
- (Exam Topic 1)
An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:
The source of the breach is linked to an IP located in a foreign country.
The breach is isolated to the research and development servers.
The hash values of the data before and after the breach are unchanged.
The affected servers were regularly patched, and a recent scan showed no vulnerabilities.
Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

A. The confidentiality of the data is unaffected.
B. The threat is an APT.
C. The source IP of the threat has been spoofed.
D. The integrity of the data is unaffected.
E. The threat is an insider.

Answer: BD

NEW QUESTION 35
- (Exam Topic 1)
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.
Which of the following BEST describes this attack?

A. Injection attack
B. Memory corruption
C. Denial of service
D. Array attack

Answer: C

Explanation:
Reference: https://economictimes.indiatimes.com/definition/memory-corruption

NEW QUESTION 37
- (Exam Topic 1)
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

Which of the following IP addresses does the analyst need to investigate further?

A. 192.168.1.1
B. 192.168.1.10
C. 192.168.1.12
D. 192.168.1.193

Answer: C

NEW QUESTION 41
- (Exam Topic 1)
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its us
B. Provide PII training to all employees at the compan
C. Encrypt PII information.
D. Enforce encryption on all emails sent within the compan
E. Create a PII program and policy on how to handle dat
F. Train all human resources employees.
G. Train all employee
H. Encrypt data sent on the company networ
I. Bring in privacy personnel to present a plan on how PII should be handled.
J. Install specific equipment to create a human resources policy that protects PII dat
K. Train company employees on how to handle PII dat
L. Outsource all PII to another compan
M. Send the human resourcesdirector to training for PII handling.

Answer: A

NEW QUESTION 42
- (Exam Topic 1)
After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

Which of the following suggests the system that produced output was compromised?

A. Secure shell is operating of compromise on this system.
B. There are no indicators of compromise on this system.

C. MySQL services is identified on a standard PostgreSQL port.
D. Standard HTP is open on the system and should be closed.

Answer: A

NEW QUESTION 45
- (Exam Topic 1)
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?

A. The system memory
B. The hard drive
C. Network packets
D. The Windows Registry

Answer: A

Explanation:
Reference: https://resources.infosecinstitute.com/memory-forensics/#gref https://www.computerhope.com/jargon/d/data-carving.htm

NEW QUESTION 49
- (Exam Topic 1)
Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

A. Reverse engineering
B. Application log collectors
C. Workflow orchestration
D. API integration
E. Scripting

Answer: D

NEW QUESTION 50
- (Exam Topic 1)
A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
B. Depending on system criticality remove each affected device from the network by disabling wired and wireless connections
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addressesIdentify potentially affected systems by creating a correlation
D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 51
- (Exam Topic 1)
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:

Which of the following should the analyst review to find out how the data was exfilltrated?

A. Monday's logs
B. Tuesday's logs
C. Wednesday's logs
D. Thursday's logs

Answer: D

NEW QUESTION 53
- (Exam Topic 1)
For machine learning to be applied effectively toward security analysis automation, it requires.

A. relevant training data.
B. a threat feed API.
C. a multicore, multiprocessor system.
D. anomalous traffic signatures.

Answer: A

NEW QUESTION 55
- (Exam Topic 1)
An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

A. Use SSO across all applications

B. Perform a manual privilege review
C. Adjust the current monitoring and logging rules
D. Implement multifactor authentication

Answer: A

NEW QUESTION 60
- (Exam Topic 1)
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

Reduce the number of potential findings by the auditors.
Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
Prevent the external-facing web infrastructure used by other teams from coming into scope.
Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.
Which of the following would be the MOST effective way for the security team to meet these objectives?

A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 61
- (Exam Topic 1)
As part of a review of modern response plans, which of the following is MOST important for an organization lo understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

NEW QUESTION 66
- (Exam Topic 1)
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

A. Write detection logic.
B. Establish a hypothesis.
C. Profile the threat actors and activities.
D. Perform a process analysis.

Answer: C

Explanation:
Reference: https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting

NEW QUESTION 70
- (Exam Topic 1)
During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.
E. DST 175.35.20.5.

Answer: A

NEW QUESTION 71
- (Exam Topic 1)
During an investigation, an incident responder intends to recover multiple pieces of digital mediA. Before removing the media, the responder should initiate:
A. malware scans.
B. secure communications.
C. chain of custody forms.
D. decryption tools.

Answer: C

NEW QUESTION 72
- (Exam Topic 1)
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes lo enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automaton
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 77
- (Exam Topic 1)
While preparing of an audit of information security controls in the environment an analyst outlines a framework control that has the following requirements:
• All sensitive data must be classified
• All sensitive data must be purged on a quarterly basis
• Certificates of disposal must remain on file for at least three years This framework control is MOST likely classified as:

A. prescriptive
B. risk-based
C. preventive
D. corrective

Answer: A

Explanation:
prescrcriptiveitive. now look at definition of prescriptive. The definition of prescriptive is the imposition of rules, or something that has become established because it has been going on a long time and has become customary. A handbook dictating the rules for proper behavior is an example of something that would be described as a prescriptive handbookules are being implimented.
Preventative controls describe any security measure that's designed to stop unwanted or unauthorized activity from occurring. Examples include physical controls such as fences, locks, and alarm systems; technical controls such as antivirus software, firewalls, and IPSs; and administrative controls like separation of duties, data classification, and auditing. https://www.f5.com/labs/articles/education/what-are-security-controls

NEW QUESTION 82
- (Exam Topic 1)
Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery
B. Cross-site scripting
C. SQL injection
D. Command injection
E. Cross-site request forgery
F. Directory traversal

Answer: B

NEW QUESTION 83
- (Exam Topic 1)
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
B. Examine the server logs for further indicators of compromise of a web application.
C. Run kill -9 1325 to bring the load average down so the server is usable again.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Answer: B

NEW QUESTION 84
- (Exam Topic 1)
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:

A. enables remote code execution that is being exploited in the wild.
B. enables data leakage but is not known to be in the environment
C. enables lateral movement and was reported as a proof of concept
D. affected the organization in the past but was probably contained and eradicated

Answer: C

NEW QUESTION 85
- (Exam Topic 1)
A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?

A. Virtualize the system and decommission the physical machine.
B. Remove it from the network and require air gapping.
C. Only allow access to the system via a jumpbox
D. Implement MFA on the specific system.

Answer: A

NEW QUESTION 87
- (Exam Topic 1)
Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:
File access auditing is turned off.

When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
All processes running appear to be legitimate processes for this user and machine.
Network traffic spikes when the space is cleared on the laptop.
No browser is open.
Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.
C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer: B

NEW QUESTION 91
- (Exam Topic 1)
A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application.
Which of the following is a security concern when using a PaaS solution?

A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
B. Patching the underlying application server becomes the responsibility of the client.
C. The application is unable to use encryption at the database level.
D. Insecure application programming interfaces can lead to data compromise.

Answer: D

NEW QUESTION 94
- (Exam Topic 1)
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 98
- (Exam Topic 1)
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

Which of the following BEST describes what the analyst has found?

A. This is an encrypted GET HTTP request
B. A packet is being used to bypass the WAF
C. This is an encrypted packet
D. This is an encoded WAF bypass

Answer: D

NEW QUESTION 103
- (Exam Topic 1)
A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.
Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: D

Explanation:
Reference: https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/#

NEW QUESTION 106
- (Exam Topic 1)
A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware.
Which of the following is the MOST appropriate action to take in the situation?

A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

Answer: C

NEW QUESTION 109

- (Exam Topic 1)
During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.
Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

A. An IPS signature modification for the specific IP addresses
B. An IDS signature modification for the specific IP addresses
C. A firewall rule that will block port 80 traffic
D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

NEW QUESTION 114
- (Exam Topic 1)
An information security analyst is compiling data from a recent penetration test and reviews the following output:

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would MOST likely provide the needed information?

A. ping -t 10.79.95.173.rdns.datacenters.com
B. telnet 10.79.95.173 443
C. ftpd 10.79.95.173.rdns.datacenters.com 443
D. tracert 10.79.95.173

Answer: B

NEW QUESTION 119
- (Exam Topic 1)
Which of the following software assessment methods would be BEST for gathering data related to an application’s availability during peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Answer: B

NEW QUESTION 123
- (Exam Topic 1)
During a cyber incident, which of the following is the BEST course of action?

A. Switch to using a pre-approved, secure, third-party communication system.
B. Keep the entire company informed to ensure transparency and integrity during the incident.
C. Restrict customer communication until the severity of the breach is confirmed.
D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Answer: D

NEW QUESTION 127
- (Exam Topic 1)
A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.
To BEST mitigate this risk, the analyst should use.

A. an 802.11ac wireless bridge to create an air gap.
B. a managed switch to segment the lab into a separate VLAN.
C. a firewall to isolate the lab network from all other networks.
D. an unmanaged switch to segment the environments from one another.

Answer: C

NEW QUESTION 129
- (Exam Topic 1)
A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

Which of the following can the analyst conclude?

A. Malware is attempting to beacon to 128.50.100.3.
B. The system is running a DoS attack against ajgidwle.com.
C. The system is scanning ajgidwle.com for PII.
D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 134
- (Exam Topic 1)
Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

A. Unauthorized, unintentional, benign
B. Unauthorized, intentional, malicious
C. Authorized, intentional, malicious
D. Authorized, unintentional, benign

Answer: C

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/insider-attack

NEW QUESTION 137
- (Exam Topic 1)
A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.
Which of the following is the MOST appropriate threat classification for these incidents?

A. Known threat
B. Zero day
C. Unknown threat
D. Advanced persistent threat

Answer: D

NEW QUESTION 140
- (Exam Topic 1)

Which of the following MOST accurately describes an HSM?

A. An HSM is a low-cost solution for encryption.
B. An HSM can be networked based or a removable USB
C. An HSM is slower at encrypting than software
D. An HSM is explicitly used for MFA

Answer: B

NEW QUESTION 141
- (Exam Topic 1)
An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Which of the following should be the focus of the investigation?

A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A

NEW QUESTION 145
- (Exam Topic 1)
Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

A. Agile
B. Waterfall
C. SDLC
D. Dynamic code analysis

Answer: A

Explanation:
Reference: https://www.cleverism.com/software-development-life-cycle-sdlc-methodologies/

NEW QUESTION 147
- (Exam Topic 1)
A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

A. Create a full disk image of the server's hard drive to look for the file containing the malware.
B. Run a manual antivirus scan on the machine to look for known malicious software.
C. Take a memory snapshot of the machine to capture volatile information stored in memory.
D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer: D

NEW QUESTION 151
- (Exam Topic 1)
A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization To

BEST resolve the issue, the organization should implement

A. federated authentication
B. role-based access control.
C. manual account reviews
D. multifactor authentication.

Answer: A

NEW QUESTION 155
- (Exam Topic 1)
Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2.
Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

Answer: A

NEW QUESTION 159
- (Exam Topic 1)
A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.
Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
B. Remove the servers reported to have high and medium vulnerabilities.
C. Tag the computers with critical findings as a business risk acceptance.
D. Manually patch the computers on the network, as recommended on the CVE website.
E. Harden the hosts on the network, as recommended by the NIST framework.
F. Resolve the monthly job issues and test them before applying them to the production network.

Answer: CE

NEW QUESTION 163
- (Exam Topic 1)
Which of the following should be found within an organization's acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.
B. Customer data must be handled properly, stored on company servers, and encrypted when possible
C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
D. Consequences of violating the policy could include discipline up to and including termination.

Answer: D

NEW QUESTION 165
- (Exam Topic 1)
An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.
Which of the following would be the MOST appropriate to remediate the controller?

A. Segment the network to constrain access to administrative interfaces.
B. Replace the equipment that has third-party support.
C. Remove the legacy hardware from the network.
D. Install an IDS on the network between the switch and the legacy equipment.

Answer: A

NEW QUESTION 168
- (Exam Topic 1)
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

Which of the following is MOST likely a false positive?

A. ICMP timestamp request remote date disclosure
B. Windows SMB service enumeration via \srvsvc
C. Anonymous FTP enabled
D. Unsupported web server detection

Answer: B

NEW QUESTION 172

- (Exam Topic 1)
A security analyst is reviewing the following web server log:

Which of the following BEST describes the issue?

A. Directory traversal exploit
B. Cross-site scripting
C. SQL injection
D. Cross-site request forgery

Answer: A

NEW QUESTION 173
- (Exam Topic 1)
Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A. Human resources
B. Public relations
C. Marketing
D. Internal network operations center

Answer: B

NEW QUESTION 178
- (Exam Topic 1)
A security team wants to make SaaS solutions accessible from only the corporate campus Which of the following would BEST accomplish this goal?

A. Geofencing
B. IP restrictions
C. Reverse proxy
D. Single sign-on

Answer: A

Explanation:
Reference: https://bluedot.io/library/what-is-geofencing/

NEW QUESTION 179
- (Exam Topic 1)
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the

security posture of the organization in the shortest amount of time?

A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
B. Incorporate prioritization levels into the remediation process and address critical findings first.
C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.

Answer: B

NEW QUESTION 183
- (Exam Topic 1)
A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet.
Which of the following solutions would meet this requirement?

A. Establish a hosted SSO.
B. Implement a CASB.
C. Virtualize the server.
D. Air gap the server.

Answer: D

NEW QUESTION 186
- (Exam Topic 1)
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?

A. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
D. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
E. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

Answer: E

NEW QUESTION 187
- (Exam Topic 1)
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported. The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
B. This is a true negative, and the new computers have the correct version of the software.
C. This is a true positive, and the new computers were imaged with an old version of the software.
D. This is a false negative, and the new computers need to be updated by the desktop team.

Answer: C

NEW QUESTION 190
- (Exam Topic 1)
A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.
Which of the following BEST describes the security analyst's goal?

A. To create a system baseline
B. To reduce the attack surface
C. To optimize system performance
D. To improve malware detection

Answer: B

Explanation:
Reducing the attack surface area means limiting the features and functions that are available to an attacker. For example, if I lock all doors to the facility with the exception of one, I have reduced the attack surface. Another term for reducing the attack surface area is system hardening because it involves ensuring that all systems have been hardened to the extent that is possible and still provide functionality

NEW QUESTION 191
- (Exam Topic 1)
A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?

A. Run an anti-malware scan on the system to detect and eradicate the current threat
B. Start a network capture on the system to look into the DNS requests to validate command and control traffic.
C. Shut down the system to prevent further degradation of the company network
D. Reimage the machine to remove the threat completely and get back to a normal running state.
E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

Answer: B

NEW QUESTION 193
- (Exam Topic 1)
A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

A. Establish an alternate site with active replication to other regions
B. Configure a duplicate environment in the same region and load balance between both instances
C. Set up every cloud component with duplicated copies and auto scaling turned on
D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

NEW QUESTION 196
- (Exam Topic 1)
While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.
To provide the MOST secure access model in this scenario, the jumpbox should be.

A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
C. bridged between the IT and operational technology networks to allow authenticated access.
D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Answer: A

NEW QUESTION 200
- (Exam Topic 1)
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-the-middle attack .The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,
B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

Answer: A

NEW QUESTION 205
- (Exam Topic 1)
A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.
Which of the following should be done to correct the cause of the vulnerability?

A. Deploy a WAF in front of the application.
B. Implement a software repository management tool.
C. Install a HIPS on the server.
D. Instruct the developers to use input validation in the code.

Answer: B

NEW QUESTION 209
- (Exam Topic 1)
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

Which of the following commands should the analyst investigate FIRST?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: B

NEW QUESTION 213

- (Exam Topic 1)
A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

A. Nikto
B. Aircrak-ng
C. Nessus
D. tcpdump

Answer: B

NEW QUESTION 214
- (Exam Topic 1)
As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

A. qualitative probabilities.
B. quantitative probabilities.
C. qualitative magnitude.
D. quantitative magnitude.

Answer: D

NEW QUESTION 219
- (Exam Topic 1)
A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.
Which of the following should be done to prevent this issue from reoccurring?

A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Answer: A

NEW QUESTION 221
- (Exam Topic 1)
Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Answer: A

NEW QUESTION 223
- (Exam Topic 1)
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

A. It enables the team to prioritize the focus area and tactics within the company’s environment.
B. It provide critically analyses for key enterprise servers and services.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It supports rapid response and recovery during and followed an incident.

Answer: A

NEW QUESTION 227
- (Exam Topic 1)
A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

A. Apply a firewall application server rule.
B. Whitelist the application server.
C. Sandbox the application server.
D. Enable port security.
E. Block the unauthorized networks.

Answer: B

NEW QUESTION 230
- (Exam Topic 1)
A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the

following code snippet of results:

Which of the following describes the output of this scan?

A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Answer: B

NEW QUESTION 231
- (Exam Topic 1)
A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.
Which of the following will remediate this software vulnerability?

A. Enforce unique session IDs for the application.
B. Deploy a WAF in front of the web application.
C. Check for and enforce the proper domain for the redirect.
D. Use a parameterized query to check the credentials.
E. Implement email filtering with anti-phishing protection.

Answer: C

NEW QUESTION 236
- (Exam Topic 1)
A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation
D. Perform a code review

Answer: B

NEW QUESTION 237
- (Exam Topic 1)
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking

http://<malwaresource>/A.php in a phishing email.
To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the.

A. email server that automatically deletes attached executables.
B. IDS to match the malware sample.
C. proxy to block all connections to <malwaresource>.
D. firewall to block connection attempts to dynamic DNS hosts.

Answer: C

NEW QUESTION 242
- (Exam Topic 1)
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

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

Answer: B

NEW QUESTION 247
- (Exam Topic 1)
Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient.
Which of the following controls would have MOST likely prevented this incident?

A. SSO
B. DLP
C. WAF
D. VDI

Answer: B

Explanation:
Reference: https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after- incident-to-do-list/

NEW QUESTION 249
- (Exam Topic 1)
A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains Management at an organization wants to know if it is a victim Which of the following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested
B. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried
C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

Answer: D

NEW QUESTION 250
- (Exam Topic 1)
A hybrid control is one that:

A. is implemented differently on individual systems
B. is implemented at the enterprise and system levels
C. has operational and technical components
D. authenticates using passwords and hardware tokens

Answer: B

NEW QUESTION 253
- (Exam Topic 1)
A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:

In which of the following phases is this APT MOST likely to leave discoverable artifacts?

A. Data collection/exfiltration
B. Defensive evasion
C. Lateral movement
D. Reconnaissance

Answer: A

NEW QUESTION 256
- (Exam Topic 1)
A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer datA. Developers use personal workstations, giving the company little to no visibility into the development activities.
Which of the following would be BEST to implement to alleviate the CISO's concern?

A. DLP
B. Encryption
C. Test data
D. NDA

Answer: D

NEW QUESTION 260
- (Exam Topic 1)
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

The analyst runs the following command next:

Which of the following would explain the difference in results?

A. ICMP is being blocked by a firewall.
B. The routing tables for ping and hping3 were different.
C. The original ping command needed root permission to execute.
D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 261

- (Exam Topic 1)
An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

A. Data deduplication
B. OS fingerprinting
C. Digital watermarking
D. Data loss prevention

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
A contained section of a building is unable to connect to the Internet A security analyst. A security analyst investigates me issue but does not see any connections to the corporate web proxy However the analyst does notice a small spike in traffic to the Internet. The help desk technician verifies all users are connected to the connect SSID. but there are two of the same SSIDs listed in the network connections. Which of the following BEST describes what is occurring?

A. Bandwidth consumption
B. Denial of service
C. Beaconing
D. Rogue device on the network

Answer: A

NEW QUESTION 264
- (Exam Topic 2)
While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful?

A. Implement MFA on the email portal using out-of-band code delivery.
B. Create a new rule in the IDS that triggers an alert on repeated login attempts
C. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
D. Alter the lockout policy to ensure users are permanently locked out after five attempts.
E. Configure a WAF with brute force protection rules in block mode

Answer: A

NEW QUESTION 265
- (Exam Topic 2)
Which of the following is MOST closely related to the concept of privacy?

A. An individual's control over personal information
B. A policy implementing strong identity management processes
C. A system's ability to protect the confidentiality of sensitive information
D. The implementation of confidentiality, integrity, and availability

Answer: A

Explanation:
"Privacy refers to whatever control you have over your personal information and how it is utilized."

NEW QUESTION 269
- (Exam Topic 2)
A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?

A. Web content filter
B. Access control list
C. Network access control
D. Data loss prevention

Answer: B

NEW QUESTION 270
- (Exam Topic 2)
To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

A. The workstation of a developer who is installing software on a web server
B. A new test web server that is in the process of initial installation
C. The laptop of the vice president that is on the corporate LAN
D. An accounting supervisor's laptop that is connected to the VPN

Answer: C

NEW QUESTION 274
- (Exam Topic 2)

An information security analyst on a threat-hunting team Is working with administrators to create a hypothesis related to an internally developed web application The working hypothesis is as follows:
• Due to the nature of the industry, the application hosts sensitive data associated with many clients and Is a significant target.
• The platform Is most likely vulnerable to poor patching and Inadequate server hardening, which expose vulnerable services.
• The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.
As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks Which of the following BEST represents the technique in use?

A. Improving detection capabilities
B. Bundling critical assets
C. Profiling threat actors and activities
D. Reducing the attack surface area

Answer: D

NEW QUESTION 276
- (Exam Topic 2)
A security analyst receives an alert from the SIEM about a possible attack happening on the network The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66. which is part of the network 192 168 54 0/24. The analyst then pulls all the command history logs from that server and sees the following

Which of the following activities is MOST likely happening on the server?

A. A MITM attack
B. Enumeration
C. Fuzzing
D. A vulnerability scan

Answer: A

NEW QUESTION 279
- (Exam Topic 2)
A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

A. Scrum
B. loC feeds
C. ISAC
D. VSS scores

Answer: C

NEW QUESTION 283
- (Exam Topic 2)
A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

A. Establish a recovery time objective and a recovery point objective for the systems being moved
B. Calculate the resource requirements for moving the systems to the cloud
C. Determine recovery priorities for the assets being moved to the cloud-based systems
D. Identify the business processes that will be migrated and the criticality of each one
E. Perform an inventory of the servers that will be moving and assign priority to each one

Answer: D

NEW QUESTION 286
- (Exam Topic 2)
A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verity that a user's data is not altered without the user's consent Which of the following would be an appropriate course of

action?

A. Use a DLP product to monitor the data sets for unauthorized edits and changes.
B. Use encryption first and then hash the data at regular, defined times.
C. Automate the use of a hashing algorithm after verified users make changes to their data
D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Answer: D

NEW QUESTION 287
- (Exam Topic 2)
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive and the scanning plugin needs to be updated by the vendor
B. This is a true negative and the new computers have the correct version of the software
C. This is a true positive and the new computers were imaged with an old version of the software
D. This is a false negative and the new computers need to be updated by the desktop team

Answer: C

NEW QUESTION 288
- (Exam Topic 2)
A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following loC:
../../../../bin/bash
Which of the following commands can be used to determine if the string is present in the log?

A. echo access.log | grep "../../../../bin/bash"
B. grep "../../../../bin/bash" 1 cat access.log
C. grep "../../../. ./bin/bash" < access.log
D. cat access.log > grep "../../../ ../bin/bash"

Answer: C

NEW QUESTION 289
- (Exam Topic 2)
A security analyst is reviewing the network security monitoring logs listed below:

Which of the following is the analyst MOST likely observing? (Select TWO).

A. 10.1.1.128 sent malicious requests, and the alert is a false positive.
B. 10.1.1.129 sent potential malicious requests to the web server.
C. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.
D. 10.1.1.128 sent potential malicious traffic to the web server.
E. 10.1.1 .129 successfully exploited a vulnerability on the web server.

Answer: AC

NEW QUESTION 291
- (Exam Topic 2)

Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

A. Open threat exchange
B. H-ISAC
C. Dark web chatter
D. Dental forums

Answer: B

NEW QUESTION 294
- (Exam Topic 2)
A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?

A. Implement IPSec rules on the application servers through a GPO that limits RDP access from only the jump hos
B. Patch the jump hos
C. Since it does not run the application natively, it will not affect the software's operation and functionalit
D. Do not patch the application servers until the compatibility issue is resolved.
E. Implement IPSec rules on the jump host server through a GPO that limits RDP access from only the other application server
F. Do not patch the jump hos
G. Since it does not run the application natively, it is at less risk of being compromise
H. Patch the application servers to secure them.
I. Implement IPSec rules on the application servers through a GPO that limits RDP access to only other application server
J. Do not patch the jump hos
K. Since it does not run the application natively, it is at less risk of being compromise
L. Patch the application servers to secure them.
M. Implement firewall rules on the application servers through a GPO that limits RDP access to only other application server
N. Manually check the jump host to see if it has been compromise
O. Patch the application servers to secure them.

Answer: A

NEW QUESTION 296
- (Exam Topic 2)
A security analyst needs to perform a search for connections with a suspicious IP on the network traffic. The company collects full packet captures at the Internet gateway and retains them for one week. Which of the following will enable the analyst to obtain the BEST results?

A. tcpdump –n –r internet.pcap host <suspicious ip>
B. strings internet.pcap | grep <suspicious ip>
C. grep –a <suspicious ip> internet.pcap
D. npcapd internet.pcap | grep <suspicious ip>

Answer: A

NEW QUESTION 298
- (Exam Topic 2)
A security analyst is conceded that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst's concern?

A. SAML
B. MFA
C. SHA-1
D. LADPS

Answer: A

NEW QUESTION 300
- (Exam Topic 2)
An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?

A. Perform a vulnerability scan against a test instance.
B. Download the product security white paper.
C. Check industry news feeds for product reviews.
D. Ensure a current non-disclosure agreement is on file

Answer: D

NEW QUESTION 303
- (Exam Topic 2)
Massivelog log has grown to 40GB on a Windows server At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10.000 lines of the loq for review?

A. tail -10000 Massivelog.log > extract.txt
B. info tail n -10000 Massivelog.log | extract.txt;

C. get content './Massivelog.log' –Last 10000 | extract.txt
D. get-content './Massivelog.log' –Last 10000 > extract.txt;

Answer: D

Explanation:
https://social.technet.microsoft.com/Forums/en-US/d7a84189-fa3f-4431-8b03-30a7d57d076a/getcontent-read-la

NEW QUESTION 308
- (Exam Topic 2)
In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. Burp Suite
C. OWASP ZAP
D. Unauthenticated

Answer: D

NEW QUESTION 312
- (Exam Topic 2)
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content Which of the following is the NEXT step the analyst should take?

A. Only allow whitelisted binaries to execute.
B. Run an antivirus against the binaries to check for malware.
C. Use file integrity monitoring to validate the digital signature.
D. Validate the binaries' hashes from a trusted source.

Answer: B

NEW QUESTION 316
- (Exam Topic 2)
A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

A. Dissemination
B. Analysis
C. Feedback
D. Requirements
E. Collection

Answer: E

NEW QUESTION 317
- (Exam Topic 2)
An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: "cat access.log.1 | grep "union". The output shown below appears:
<68.71.54.117> – – [31/Jan/2020:10:02:31 –0400] "Get
/cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1" Which of the following attacks has occurred on the server?

A. Cross-site request forgery
B. SQL injection
C. Cross-site scripting
D. Directory traversal

Answer: C

NEW QUESTION 322
- (Exam Topic 2)
The management team assigned the following values to an inadvertent breach of privacy regulations during the original risk assessment:
Probability = 25%
Magnitude = $1,015 per record Total records = 10,000
Two breaches occurred during the fiscal year. The first compromised 35 records, and the second compromised 65 records. Which of the following is the value of the records that were compromised?

A. $10,150
B. $25,375
C. $101,500
D. $2,537,500

Answer: A

NEW QUESTION 325
- (Exam Topic 2)
An organization's network administrator uncovered a rogue device on the network that is emulating the charactenstics of a switch. The device is trunking protocols and inserting tagging va the flow of traffic at the data link layer

Which of the following BEST describes this attack?

A. VLAN hopping
B. Injection attack
C. Spoofing
D. DNS pharming

Answer: A

NEW QUESTION 327
- (Exam Topic 2)
While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Select TWO).

A. Configure /etc/sshd_config to deny root logins and restart the SSHD service.
B. Add a rule on the network IPS to block SSH user sessions
C. Configure /etc/passwd to deny root logins and restart the SSHD service.
D. Reset the passwords for all accounts on the affected system.
E. Add a rule on the perimeter firewall to block the source IP address.
F. Add a rule on the affected system to block access to port TCP/22.

Answer: CE

NEW QUESTION 329
- (Exam Topic 2)
Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night.
Which of the following actions should the analyst take NEXT?

A. Initiate the incident response plan.
B. Disable the privileged account
C. Report the discrepancy to human resources.
D. Review the activity with the user.

Answer: D

NEW QUESTION 333
- (Exam Topic 2)
Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?

A. Information sharing and analysis membership
B. Open-source intelligence, such as social media and blogs
C. Real-time and automated firewall rules subscriptions
D. Common vulnerability and exposure bulletins

Answer: A

NEW QUESTION 334
- (Exam Topic 2)
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

A. Input validation
B. Output encoding
C. Parameterized queries
D. Tokenization

Answer: D

NEW QUESTION 337
- (Exam Topic 2)
A large insurance company wants to outsource its claim-handling operations to an overseas third-party organization Which of the following would BEST help to reduce the chance of highly sensitive data leaking?

A. Configure a VPN between the third party organization and the internal company network
B. Set up a VDI that the third party must use to interact with company systems.
C. Use MFA to protect confidential company information from being leaked.
D. Implement NAC to ensure connecting systems have malware protection
E. Create jump boxes that are used by the third-party organization so it does not connect directly.

Answer: D

NEW QUESTION 340
- (Exam Topic 2)
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Create a WAF rule In block mode for SQL injection
D. Ask the developers to implement parameterized SQL queries.

Answer: A

NEW QUESTION 343
- (Exam Topic 2)
A security analyst is reviewing the following log entries to identify anomalous activity:

Which of the following attack types is occurring?

A. Directory traversal
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Answer: A

NEW QUESTION 345
- (Exam Topic 2)
D18912E1457D5D1DDCBD40AB3BF70D5D
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.
Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?

A. Port 22
B. Port 135
C. Port 445
D. Port 3389

Answer: B

NEW QUESTION 346
- (Exam Topic 2)
A security analyst receives a CVE bulletin, which lists several products that are used in the enterprise. The analyst immediately deploys a critical security patch.
Which of the following BEST describes the reason for the analyst's immediate action?

A. A known exploit was discovered.
B. There is an insider threat.
C. Nation-state hackers are targeting the region.
D. A new zero-day threat needs to be addressed.
E. A new vulnerability was discovered by a vendor.

Answer: E

NEW QUESTION 348
- (Exam Topic 2)

An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

A. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans
B. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
C. Monthly host discovery scans; biweekly vulnerability scans, monthly topology scans
D. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans

Answer: D

NEW QUESTION 351
- (Exam Topic 2)
A company wants to outsource a key human-resources application service to remote employees as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:

A. DLP procedures.
B. logging and monitoring capabilities.
C. data protection capabilities.
D. SLA for system uptime.

Answer: C

NEW QUESTION 356
- (Exam Topic 2)
A security analyst reviews SIEM logs and detects a well-known malicious executable running in a Windows machine The up-to-date antivirus cannot detect the malicious executable Which of the following is the MOST likely cause of this issue?

A. The malware is being executed with administrative privileges.
B. The antivirus does not have the mltware's signature.
C. The malware detects and prevents its own execution in a virtual environment.
D. The malware is fileless and exists only in physical memory.

Answer: A

NEW QUESTION 358
- (Exam Topic 2)
A security analyst inspects the header of an email that is presumed to be malicious and sees the following:

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

A. The subject line
B. The sender's email address
C. The destination email server
D. The use of a TLS cipher

Answer: C

NEW QUESTION 361
- (Exam Topic 2)
While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst's supervisor to use additional controls?

A. FPGAs are vulnerable to malware installation and require additional protections for their codebase.
B. FPGAs are expensive to produc
C. Anti-counterierting safeguards are needed.
D. FPGAs are expensive and can only be programmed onc
E. Code deployment safeguards are needed.
F. FPGAs have an inflexible architectur
G. Additional training for developers is needed

Answer: B

Explanation:
Ethernet switches are mass-produced and offered at discounts on not so widely-used chips with massive economies of scale. While in case of FPGAs,they are used as Ethernet switches and hence cost more since the expense of development and infrastructure are distributed among fewer clients.

NEW QUESTION 365
- (Exam Topic 2)
During an investigation, an analyst discovers the following rule in an executive’s email client: IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM ‘sent’ THEN DELETE FROM <executive@anycompany.com>
The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

A. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
B. Use the SIEM to correlate logging events from the email server and the domain server
C. Remove the rule from the email client and change the password
D. Recommend that management implement SPF and DKIM

Answer: A

NEW QUESTION 366
- (Exam Topic 2)
Understanding attack vectors and integrating intelligence sources are important components of:

A. proactive threat hunting
B. risk management compliance.
C. a vulnerability management plan.
D. an incident response plan.

Answer: C

Explanation:
threat hunting activities.
* 1. Establishing a hypothesis,
* 2. Profile threat actors/activities,
* 3. Threat hunting tactics,
* 4. Reducing attack surface,
* 5. Bundle critical systems/assets into groups/protected zones,
* 6. Attack vectors understood, assessed and addressed
* 7. Integrated intelligence
* 8. Improving detection capabilities.

NEW QUESTION 367
- (Exam Topic 2)
A security analyst is researching an incident and uncovers several details that may link to other incidents. The security analyst wants to determine if other incidents are related to the current incident Which of the followinq threat research methodoloqies would be MOST appropriate for the analyst to use?

A. Reputation data
B. CVSS score
C. Risk assessment
D. Behavioral analysis

Answer: D

NEW QUESTION 369
- (Exam Topic 2)
An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected A security analyst reviews the DNS entry and sees the following:
v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com –all
The organization's primary mail server IP is 180.10 6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com.
Which of the following is the MOST likely reason for the rejected emails?

A. The wrong domain name is in the SPF record.
B. The primary and secondary email server IP addresses are out of sequence.
C. SPF version 1 does not support third-party providers
D. An incorrect IP version is being used.

Answer: A

NEW QUESTION 372
- (Exam Topic 2)
The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

A. Whitelisting authorized IP addresses
B. Enforcing more complex password requirements
C. Blacklisting unauthorized IP addresses
D. Establishing a sinkhole service

Answer: C

NEW QUESTION 374
- (Exam Topic 2)
A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level
authentication is enabled
Which of the following is the BEST remediation for this vulnerability?

A. Verify the latest endpoint-protection signature is in place.
B. Verify the corresponding patch for the vulnerability is installed^
C. Verify the system logs do not contain indicator of compromise.
D. Verify the threat intelligence feed is updated with the latest solutions

Answer: A

NEW QUESTION 377
- (Exam Topic 2)
Employees of a large financial company are continuously being Infected by strands of malware that are not detected by EDR tools. When of the following Is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

A. MFA on the workstations
B. Additional host firewall rules
C. VDI environment
D. Hard drive encryption
E. Network access control
F. Network segmentation

Answer: C

NEW QUESTION 380
- (Exam Topic 2)
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

A. Focus on incidents that may require law enforcement support.
B. Focus on common attack vectors first.
C. Focus on incidents that have a high chance of reputation harm.
D. Focus on incidents that affect critical systems.

Answer: D

NEW QUESTION 384
- (Exam Topic 2)
A security analyst needs to develop a brief that will include the latest incidents and the attack phases of the incidents. The goal is to support threat intelligence and identify whether or not the incidents are linked.
Which of the following methods would be MOST appropriate to use?

A. An adversary capability model
B. The MITRE ATT&CK framework
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: B

NEW QUESTION 386
- (Exam Topic 2)
A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

A. Data masking
B. Data loss prevention
C. Data minimization
D. Data sovereignty

Answer: A

NEW QUESTION 387
- (Exam Topic 2)
A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment Conditionally other processes will need to be created based on input from prior processes
Which of the following is the BEST method for accomplishing this task?

A. Machine learning and process monitoring
B. API integration and data enrichment
C. Workflow orchestration and scripting
D. Continuous integration and configuration management

Answer: C

NEW QUESTION 391
- (Exam Topic 2)
An organization is experiencing issues with emails that are being sent to external recipients Incoming emails to the organization are working fine. A security analyst receives the following screenshot ot email error from the help desk.

The analyst the checks the email server and sees many of the following messages in the logs. Error 550 - Message rejected
Which of the following is MOST likely the issue?

A. The DMARC queue is full
B. SPF is failing.
C. Port 25 is not open.
D. The DKIM private key has expired

Answer: A

NEW QUESTION 395
- (Exam Topic 2)
The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded
and has revealed a worm is spreading
Which of the following should be the NEXT step in this incident response?

A. Enable an ACL on all VLANs to contain each segment
B. Compile a list of loCs so the IPS can be updated to halt the spread.
C. Send a sample of the malware to the antivirus vendor and request urgent signature creation.
D. Begin deploying the new anti-malware on all uninfected systems.

Answer: A

NEW QUESTION 400
- (Exam Topic 2)
A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

A. Static analysis
B. Dynamic analysis
C. Regression testing
D. User acceptance testing

Answer: C

NEW QUESTION 404
- (Exam Topic 2)
The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network.
Which of the following would work BEST to prevent the issue?

A. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
B. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.

Answer: A

NEW QUESTION 408
- (Exam Topic 2)
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

A. Operational
B. Corrective
C. Managerial
D. Technical

Answer: B

NEW QUESTION 411
- (Exam Topic 2)
As part of an organization’s information security governance process, a Chief Information Security Officer (CISO) is working with the compliance officer to update policies to include statements related to new regulatory and legal requirements. Which of the following should be done to BEST ensure all employees are appropriately aware of changes to the policies?

A. Conduct a risk assessment based on the controls defined in the newly revised policies
B. Require all employees to attend updated security awareness training and sign an acknowledgement
C. Post the policies on the organization’s intranet and provide copies of any revised policies to all active vendors
D. Distribute revised copies of policies to employees and obtain a signed acknowledgement from them

Answer: B

NEW QUESTION 416
- (Exam Topic 2)
An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization’s network and identify active hosts. An analyst sees the following output from a packet capture:

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

A. flags=RA indicates the testing team is using a Christmas tree attack
B. ttl=64 indicates the testing team is setting the time to live below the firewall’s threshold
C. 0 data bytes indicates the testing team is crafting empty ICMP packets
D. NO FLAGS are set indicates the testing team is using hping

Answer: D

NEW QUESTION 420
- (Exam Topic 2)
The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device
mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

A. Implement an IPS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
B. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
C. Implement an IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
D. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability

Answer: A

NEW QUESTION 425
- (Exam Topic 2)
While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?

A. Block the domain IP at the firewall.
B. Blacklist the new subnet
C. Create an IPS rule.
D. Apply network access control.

Answer: A

NEW QUESTION 426
- (Exam Topic 2)
A company wants to reduce the cost of deploying servers to support increased network growth. The company is currently unable to keep up with the demand, so it wants to outsource the infrastructure to a cloud-based solution.
Which of the following is the GREATEST threat for the company to consider when outsourcing its infrastructure?

A. The cloud service provider is unable to provide sufficient logging and monitoring.
B. The cloud service provider is unable to issue sufficient documentation for configurations.
C. The cloud service provider conducts a system backup each weekend and once a week during peak business times.
D. The cloud service provider has an SLA for system uptime that is lower than 99 9%.

Answer: B

NEW QUESTION 427
- (Exam Topic 2)
A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:

The analyst then compares the following results for port 22: nmap returns "Closed"
hping3 returns "flags=RA"
Which of the following BEST describes the firewall rule?

A. DNAT –-to-destination 1.1.1.1:3000
B. REJECT with –-tcp-reset
C. LOG –-log-tcp-sequence
D. DROP

Answer: B

Explanation:
No doubt does the nmap result mean its being rejected as it returns closed. However, what threw me for a loop was the hping3 response. After further web surfing I found that the "flag=RA" means actually means "flag= RST, ACK" which means that it too was rejected.

NEW QUESTION 429
- (Exam Topic 2)
Which of the following data security controls would work BEST to prevent real Pll from being used in an organization's test cloud environment?

A. Digital rights management
B. Encryption
C. Access control
D. Data loss prevention
E. Data masking

Answer: E

Explanation:
Data masking is a way to create a fake, but a realistic version of your organizational data. The goal is to protect sensitive data, while providing a functional alternative when real data is not needed—for example, in user training, sales demos, or software testing.

NEW QUESTION 430
- (Exam Topic 2)

While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk.
The analyst sees the following on the laptop's screen:

Which of the following is the BEST action for the security analyst to take?

A. Initiate a scan of devices on the network to find password-cracking tools.
B. Disconnect the laptop and ask the users jsmith and progers to log out.
C. Force all users in the domain to change their passwords at the next login.
D. Take the FILE-SHARE-A server offline and scan it for viruses.

Answer: D

NEW QUESTION 433
- (Exam Topic 2)
A company's data is still being exfiltered to business competitors after the implementation of a DLP solution. Which of the following is the most likely reason why the data is still being compromised?

A. Printed reports from the database contain sensitive information
B. DRM must be implemented with the DLP solution
C. Users are not labeling the appropriate data sets
D. DLP solutions are only effective when they are implemented with disk encryption

Answer: B

NEW QUESTION 438
- (Exam Topic 2)
A forensic analyst took an image of a workstation that was involved in an incident To BEST ensure the image is not tampered with me analyst should use:

A. hashing
B. backup tapes
C. a legal hold
D. chain of custody.

Answer: A

NEW QUESTION 443
- (Exam Topic 2)
A bad actor bypasses authentication and reveals all records in a database through an SQL injection. Implementation of which of the following would work BEST to prevent similar attacks in

A. Strict input validation

B. Blacklisting
C. SQL patching
D. Content filtering
E. Output encoding

Answer: A

NEW QUESTION 445
- (Exam Topic 2)
A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts. Which of the following is the FIRST action the analyst should take as part of security operations monitoring?

A. Run scheduled antivirus scans on all employees' machines to look for malicious processes.
B. Reimage the machines of all users within the group in case of a malware infection.
C. Change all the user passwords to ensure the malicious actors cannot use them.
D. Search the event logs for event identifiers that indicate Mimikatz was used.

Answer: D

NEW QUESTION 450
- (Exam Topic 2)
An application server runs slowly and then triggers a high CPU alert. After investigating, a security analyst finds an unauthorized program is running on the server. The analyst reviews the application log below.

Which of the following conclusions is supported by the application log?

A. An attacker was attempting to perform a buffer overflow attack to execute a payload in memory.
B. An attacker was attempting to perform an XSS attack via a vulnerable third-party library.
C. An attacker was attempting to download files via a remote command execution vulnerability
D. An attacker was attempting to perform a DoS attack against the server.

Answer: C

Explanation:
Bin /Bash in this log. looks like reverse shell and definately remote command exacution and downloading something.

NEW QUESTION 452
- (Exam Topic 2)
A company’s Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user’s activity session. Which of the following is the BEST technique to address the CISO’s concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.
C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the file
F. Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
G. Use Wireshark to scan all traffic to and from the director
H. Monitor the files for unauthorized changes.

Answer: AC

NEW QUESTION 457
- (Exam Topic 2)
A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

A. Kill chain
B. Diamond Model of Intrusion Analysis
C. MITRE ATT&CK
D. ITIL

Answer: C

NEW QUESTION 458
- (Exam Topic 2)
Given the Nmap request below:

Which of the following actions will an attacker be able to initiate directly against this host?

A. Password sniffing
B. ARP spoofing
C. A brute-force attack
D. An SQL injection

Answer: C

NEW QUESTION 459
- (Exam Topic 3)
Due to a rise m cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

A. Implement privileged access management
B. Implement a risk management process
C. Implement multifactor authentication
D. Add more security resources to the environment

Answer: C

NEW QUESTION 463
- (Exam Topic 3)
During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Answer: A

NEW QUESTION 465
- (Exam Topic 3)
An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:

This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?
A)

B)

C)

D)

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

Answer: B

NEW QUESTION 468
- (Exam Topic 3)
Which of the following is a difference between SOAR and SCAP?

A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts

Answer: D

NEW QUESTION 472

- (Exam Topic 3)
Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

A. Set up an FTP server that both companies can access and export the required financial data to a folder.
B. Set up a VPN between Company A and Company
C. granting access only lo the ERPs within the connection
D. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
E. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.

Answer: B

NEW QUESTION 473
- (Exam Topic 3)
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.
C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.

Answer: B

NEW QUESTION 477
- (Exam Topic 3)
A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

A. DNSSEC
B. DMARC
C. STP
D. S/IMAP

Answer: B

NEW QUESTION 478
- (Exam Topic 3)
An organization has the following policy statements:
• All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
•AM network activity will be logged and monitored.
• Confidential data will be tagged and tracked
• Confidential data must never be transmitted in an unencrypted form.
• Confidential data must never be stored on an unencrypted mobile device. Which of the following is the organization enforcing?

A. Acceptable use policy
B. Data privacy policy
C. Encryption policy
D. Data management, policy

Answer: B

NEW QUESTION 483
- (Exam Topic 3)
Which of the following BEST explains the function of a managerial control?

A. To help design and implement the security planning, program development, and maintenance of the security life cycle
B. To guide the development of training, education, security awareness programs, and system maintenance
C. To create data classification, risk assessments, security control reviews, and contingency planning
D. To ensure tactical design, selection of technology to protect data, logical access reviews, and theimplementation of audit trails

Answer: C

Explanation:
Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Examples of administrative controls include

periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices

NEW QUESTION 485
- (Exam Topic 3)
A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of Incident in the future?

A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
B. Back up the workstations to facilitate recovery and create a gold Image.
C. Establish a ransomware awareness program and implement secure and verifiable backups.
D. Virtualize all the endpoints with dairy snapshots of the virtual machines.

Answer: A

NEW QUESTION 487
- (Exam Topic 3)
A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

A. Submit a change request to have the system patched
B. Evaluate the risk and criticality to determine it further action is necessary
C. Notify a manager of the breach and initiate emergency procedures.
D. Remove the application from production and Inform the users.

Answer: A

NEW QUESTION 492
- (Exam Topic 3)
An organization has the following policies:
*Services must run on standard ports.
*Unneeded services must be disabled.
The organization has the following servers:
*192.168.10.1 - web server
*192.168.10.2 - database server
A security analyst runs a scan on the servers and sees the following output:

Which of the following actions should the analyst take?

A. Disable HTTPS on 192.168.10.1.
B. Disable IIS on 192.168.10.1.
C. Disable DNS on 192.168.10.2.
D. Disable MSSQL on 192.168.10.2.
E. Disable SSH on both servers.

Answer: C

NEW QUESTION 493
- (Exam Topic 3)
Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?
A. Security regression testing
B. Code review
C. User acceptance testing
D. Stress testing

Answer: C

Explanation:
"User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications." https://www.plutora.com/blog/uat-user-acceptance-testing

NEW QUESTION 498
- (Exam Topic 3)
During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity The analyst also notes there is no other alert in place for this traffic After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

A. Share details of the security incident with the organization's human resources management team
B. Note the security incident so other analysts are aware the traffic is malicious
C. Communicate the security incident to the threat team for further review and analysis
D. Report the security incident to a manager for inclusion in the daily report

Answer: C

NEW QUESTION 503
- (Exam Topic 3)
In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Answer: A

NEW QUESTION 504
- (Exam Topic 3)
An organization is focused on restructuring its data governance programs and an analyst has been Tasked with surveying sensitive data within the organization. Which of the following is the MOST accurate method for the security analyst to complete this assignment?

A. Perform an enterprise-wide discovery scan.
B. Consult with an internal data custodian.
C. Review enterprise-wide asset Inventory.
D. Create a survey and distribute it to data owners.

Answer: D

NEW QUESTION 506
- (Exam Topic 3)
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?

A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist

Answer: D

NEW QUESTION 508
- (Exam Topic 3)
Which of the following is an advantage of SOAR over SIEM?

A. SOAR is much less expensive.
B. SOAR reduces the amount of human intervention required.
C. SOAR can aggregate data from many sources.
D. SOAR uses more robust encryption protocols.

Answer: C

Explanation:
SOAR systems and services tend to add a layer of workflow management. That means that SOAR deployments may actually ingest SIEM alerts and other data and then apply workflows and automation to them. SIEM and SOAR tools can be difficult to distinguish from each other, with one current difference being the broader range of tools that SOAR services integrate with. The same vendors who provide SIEM capabilities also provide SOAR systems in many cases with Splunk, Rapid7, and IBM (QRadar) all included. There are differences, however, as ITSM tools like ServiceNow play in the space as well. As an analyst, you need to know that SOAR services and tools exist and can be leveraged to cover additional elements beyond what traditional SIEM systems have historically handled.

NEW QUESTION 509
- (Exam Topic 3)
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

A. Blacklist the hash in the next-generation antivirus system.
B. Manually delete the file from each of the workstations.
C. Remove administrative rights from all developer workstations.
D. Block the download of the fie via the web proxy

Answer: A

NEW QUESTION 514
- (Exam Topic 3)
A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:

Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?

A. The DMARC record's DKIM alignment tag Is incorrectly configured.
B. The DMARC record's policy tag is incorrectly configured.
C. The DMARC record does not have an SPF alignment tag.
D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.

Answer: C

NEW QUESTION 516
- (Exam Topic 3)
A security is reviewing a vulnerability scan report and notes the following finding:

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

A. Patch or reimage the device to complete the recovery
B. Restart the antiviruses running processes
C. Isolate the host from the network to prevent exposure
D. Confirm the workstation's signatures against the most current signatures.

Answer: D

NEW QUESTION 517
- (Exam Topic 3)
A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?
A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: B

NEW QUESTION 522
- (Exam Topic 3)
A company’s Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

A. Implement a virtual machine alternative.
B. Develop a new secured browser.
C. Configure a personal business VLAN.
D. Install kiosks throughout the building.

Answer: C

NEW QUESTION 524
- (Exam Topic 3)
In response to an audit finding, a company's Chief information Officer (CIO) instructed the security department to Increase the security posture of the vulnerability management program. Currency, the company's vulnerability management program has the following attributes:

Which of the following would BEST Increase the security posture of the vulnerably management program?

A. Expand the ports Being scanned lo Include al ports increase the scan interval to a number the business win accept without causing service interruptio
B. Enable authentication and perform credentialed scans
C. Expand the ports being scanned to Include all port
D. Keep the scan interval at its current level Enable authentication and perform credentialed scans.
E. Expand the ports being scanned to Include at ports increase the scan interval to a number the business will accept without causing service Interruptio
F. Continue unauthenticated scans.
G. Continue scanning the well-known ports increase the scan interval to a number the business will accept without causing service Interruptio
H. Enable authentication and perform credentialed scans.

Answer: A

NEW QUESTION 526
- (Exam Topic 3)
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

A. Fully segregate the affected servers physically in a network segment, apart from the production network.
B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours
C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
D. Collect all the files that have changed and compare them with the previous baseline

Answer: A

NEW QUESTION 530
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

https://www.2passeasy.com/dumps/CS0-003/

Money Back Guarantee

CS0-003 Practice Exam Features:

* CS0-003 Questions and Answers Updated Frequently

* CS0-003 Practice Questions Verified by Expert Senior Certified Staff

* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year