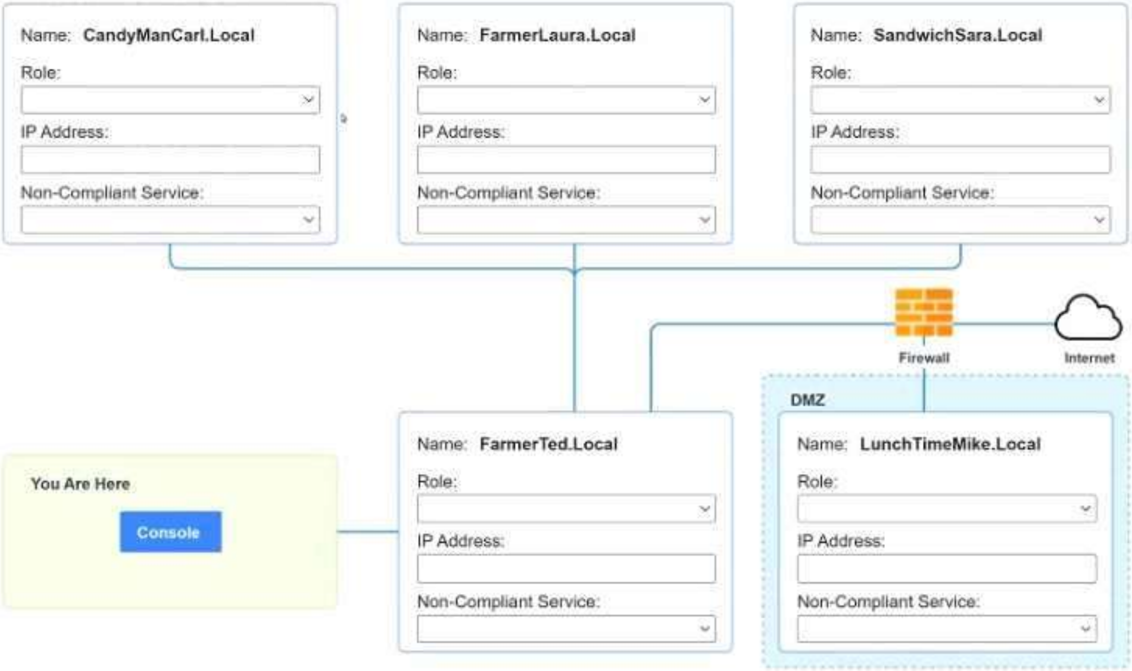
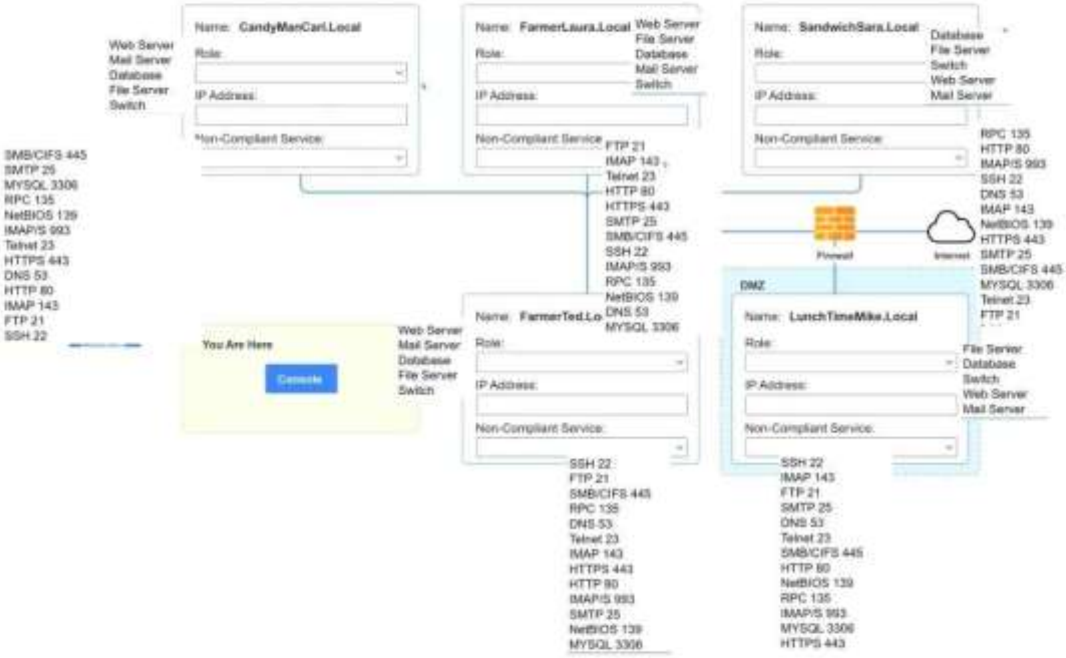
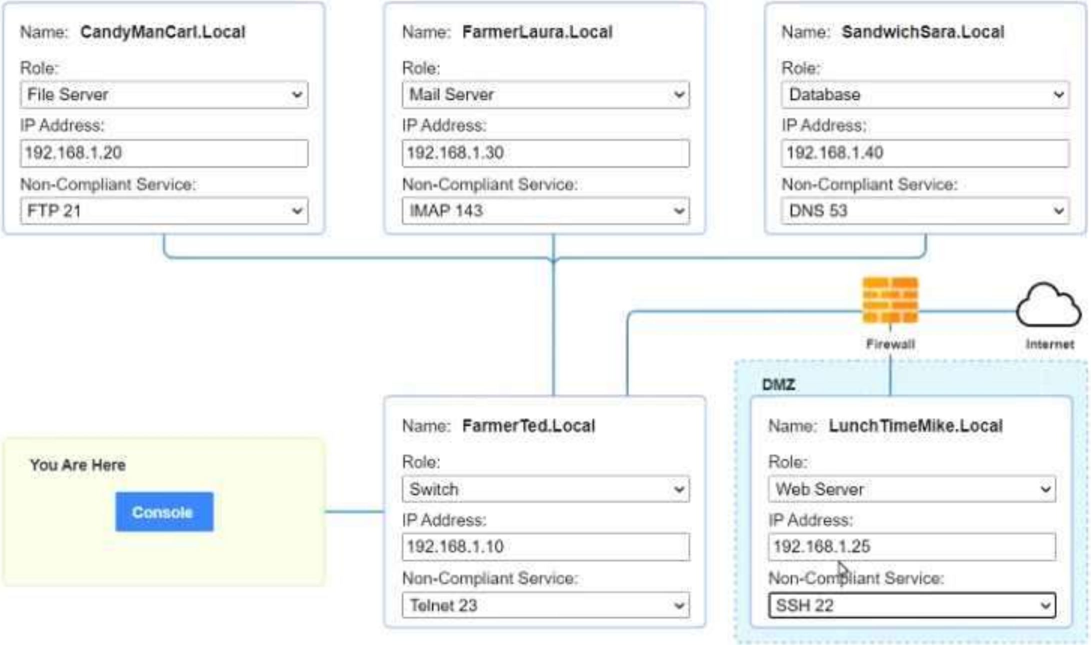
- **Vendor:** CompTIA
- **Exam Code:** CS0-002
- **Exam Name:** CompTIA CSA+ Certification Exam
- **New Updated Questions from** Braindump2go (**Updated in** August/2022)

QUESTION 807
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
If at any time you would like to bring back.





Answer:



Name: CandyManCarl.Local
Role: File Server
IP Address: 192.168.1.20
Non-Compliant Service: FTP 21

Name: FarmerLaura.Local
Role: Mail Server
IP Address: 192.168.1.30
Non-Compliant Service: IMAP 143

Name: SandwichSara.Local
Role: Database
IP Address: 192.168.1.40
Non-Compliant Service: DNS 53

Name: FarmerTed.Local
Role: Switch
IP Address: 192.168.1.10
Non-Compliant Service: Telnet 23

Name: LunchTimeMike.Local
Role: Web Server
IP Address: 192.168.1.25
Non-Compliant Service: SSH 22

QUESTION 808

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. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape

Answer: C

QUESTION 809
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. Web-application vulnerability scan
B. Static analysis
C. Packet inspection
D. Penetration test

Answer: B

QUESTION 810
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. threat hunting.
C. red learning.
D. penetration testing.

Answer: A

QUESTION 811
Which of the following BEST explains the function of a managerial control?

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

Answer: A

QUESTION 812
Which of the following types of controls defines placing an ACL on a file folder?

A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control

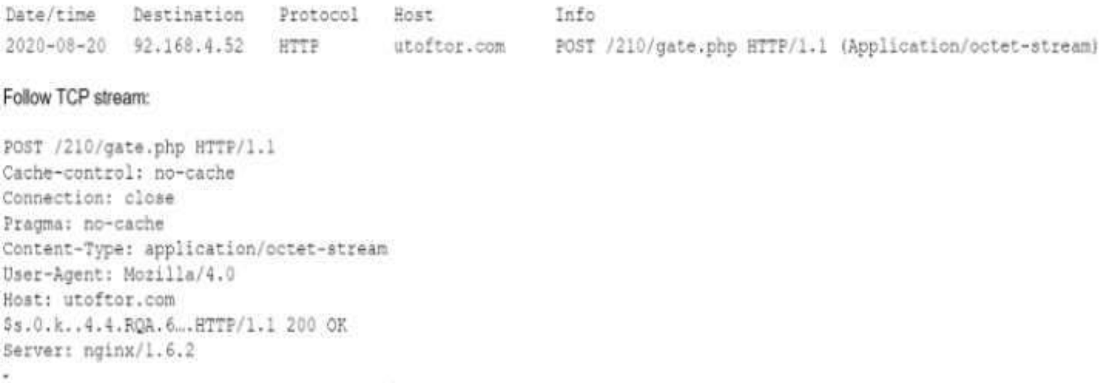
Answer: A

QUESTION 813
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. decode.
C. guess.
D. decrypt.

Answer: A

QUESTION 814
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:



```
Date/time    Destination   Protocol   Host          Info
2020-08-20   92.168.4.52   HTTP       utoftor.com   POST /210/gate.php HTTP/1.1 (Application/octet-stream)
```

Follow TCP stream:

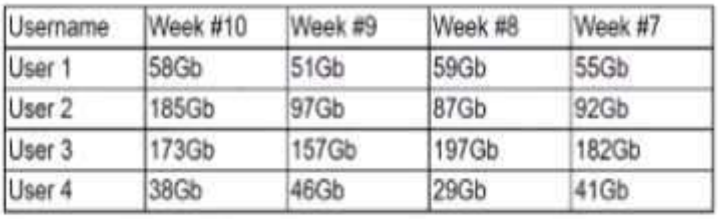
```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6….HTTP/1.1 200 OK
Server: nginx/1.6.2
-
```

Which of the following describes what has occurred?
The host attempted to download an application from utoftor.com.

A. The host downloaded an application from utoftor.com.
B. The host attempted to make a secure connection to utoftor.com.
C. The host rejected the connection from utoftor.com.

Answer:

QUESTION 815
A security analyst is reviewing the following Internet usage trend report:



Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

Which of the following usernames should the security analyst investigate further?

A. User1
B. User 2
C. User 3
D. User 4

Answer: B

QUESTION 816

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. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
B. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
D. Meet with the senior management team to determine if funding is available for recommended solutions.

Answer: C

QUESTION 817
Which of the following, BEST explains the function of TPM?

A. To provide hardware-based security features using unique keys
B. To ensure platform confidentiality by storing security measurements
C. To improve management of the OS installation.
D. To implement encryption algorithms for hard drives

Answer: A

QUESTION 818
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance.
B. Implement blacklisting lor IP addresses from outside the county.
C. Implement strong authentication controls for at contractors.
D. Implement user behavior analytics tor key staff members.

Answer: A

QUESTION 819
A company's application development has been outsourced to a third-party development team.
Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

A. Input validation
B. Security regression testing
C. Application fuzzing
D. User acceptance testing
E. Stress testing

Answer: D

QUESTION 820
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:
- The partners' PCs must not connect directly to the laboratory network.
- The tools the partners need to access while on the laboratory network must be available to all partners
- The partners must be able to run analyses on the laboratory network, which may take hours to complete
Which of the following capabilities will MOST likely meet the security objectives of the request?

A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools tor analysis
C. Deployment of a firewall to allow access to the laboratory network and use of VDI In persistent mode to provide the necessary tools for analysis
D. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

Answer: C

QUESTION 821
Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).

A. To establish a clear chain of command
B. To meet regulatory requirements for timely reporting
C. To limit reputation damage caused by the breach
D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes

Answer: BF

QUESTION 822
Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

A. There is a longer period of time to assess the environment.
B. The testing is outside the contractual scope
C. There is a shorter period of time to assess the environment
D. No status reports are included with the assessment.

Answer: B

QUESTION 823
Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques
B. Understanding how to build correlation rules within a SIEM
C. Understanding security software technologies
D. Understanding assets and categories of assets

Answer: D

QUESTION 824
Which of the following are considered PH by themselves? (Select TWO).

A. Government ID
B. Job title
C. Employment start date
D. Birth certificate
E. Employer address
F. Mother's maiden name

Answer: AD

QUESTION 825
Which of the following BEST describes HSM?

A. A computing device that manages cryptography, decrypts traffic, and maintains library calls
B. A computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions
C. A computing device that manages physical keys, encrypts devices, and creates strong cryptographic functions
D. A computing device that manages algorithms, performs entropy functions, and maintains digital signatures

Answer: B

QUESTION 826
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

A. The whitelist
B. The DNS
C. The blocklist
D. The IDS signature

Answer: D

QUESTION 827
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

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

Answer: B

QUESTION 828
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. SCADA
B. CAN bus
C. Modbus
D. loT

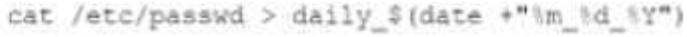
Answer: D

QUESTION 829
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. Header analysis
B. File carving
C. Metadata analysis
D. Data recovery

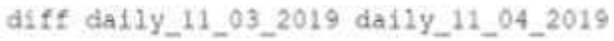
Answer: B

QUESTION 830
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:

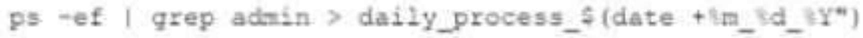


```
cat /etc/passwd > daily_$(date +"%m_%d_%Y")
```

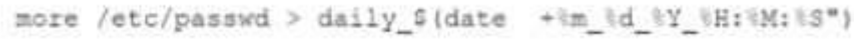
This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?

A. 

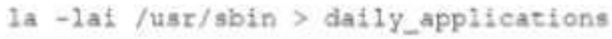
```
diff daily_11_03_2019 daily_11_04_2019
```

B. 

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

C. 

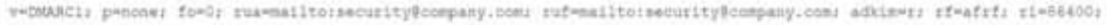
```
more /etc/passwd > daily_$(date  +%m_%d_%Y_%H:%M:%S")
```

D. 

```
la -lai /usr/sbin > daily_applications
```

Answer: B

QUESTION 831
A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:



```
v=DMARC1; p=none; fo=0; rua=mailto:security@company.com; ruf=mailto:security@company.com; adkim=r; rf=afrf; ri=86400;
```

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

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

Answer: C

QUESTION 832
Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.
B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom toots for embedded devices.
C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices
D. Trusted firmware updates provide organizations with secure code signing, distribution, installation. and attestation for embedded devices.

Answer: D

QUESTION 833
A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?

A. Contact the CRM vendor.
B. Prepare an incident summary report.
C. Perform postmortem data correlation.
D. Update the incident response plan.

Answer: C

QUESTION 834
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

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

Answer: D

QUESTION 835
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

Answer: C

QUESTION 836
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department
B. Customers
C. Company leadership
D. The legal team

Answer: D

QUESTION 837
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions

should be taken FIRST to prevent a more serious compromise?

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

Answer: A

QUESTION 838
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

A. On a private VLAN
B. Full disk encrypted
C. Powered off
D. Backed up hourly
E. VPN accessible only
F. Air gapped

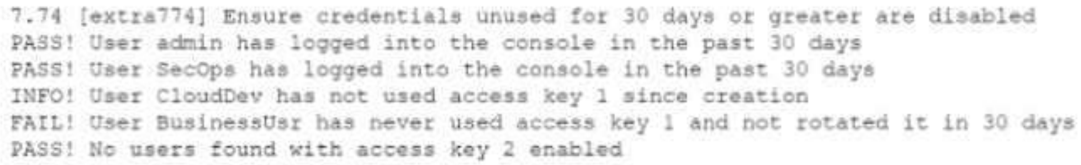
Answer: EF

QUESTION 839
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

A. To identify weaknesses in an organization's security posture
B. To identify likely attack scenarios within an organization
C. To build a business security plan for an organization
D. To build a network segmentation strategy

Answer: B

QUESTION 840
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
```

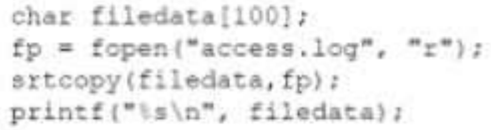
Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1.
C. Delete access key 1.
D. Delete access key 2.

Answer: D

QUESTION 841

An internally developed file-monitoring system identified the following except as causing a program to crash often:



```
char filedata[100];
fp = fopen("access.log", "r");
srtcopy(filedata,fp);
printf("%s\n", filedata);
```

Which of the following should a security analyst recommend to fix the issue?

A. Open the access.log file ri read/write mode.
B. Replace the strcpv function.
C. Perform input samtizaton
D. Increase the size of the file data buffer

Answer: A

QUESTION 842
An organization has the following policy statements:
- All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
- All network activity will be logged and monitored.
- Confidential data will be tagged and tracked
- Confidential data must never be transmitted in an unencrypted form.
- Confidential data must never be stored on an unencrypted mobile device.
Which of the following is the organization enforcing?

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

Answer: B

QUESTION 843
A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

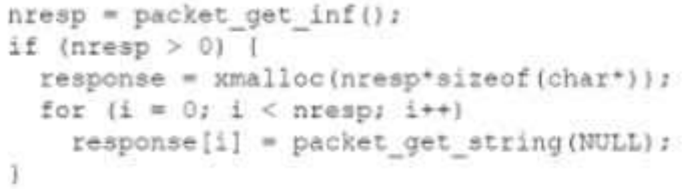
Answer: B

QUESTION 844
A security analyst needs to provide the development learn 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. CASB
B. VPC
C. Federation
D. VPN

Answer: D

QUESTION 845
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;



```
nresp = packet_get_inf();
if (nresp > 0) {
  response = xmalloc(nresp*sizeof(char*));
  for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

A. Convert all integer numbers in strings to handle the memory buffer correctly.
B. Implement float numbers instead of integers to prevent integer overflows.
C. Use built-in functions from libraries to check and handle long numbers properly.
D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

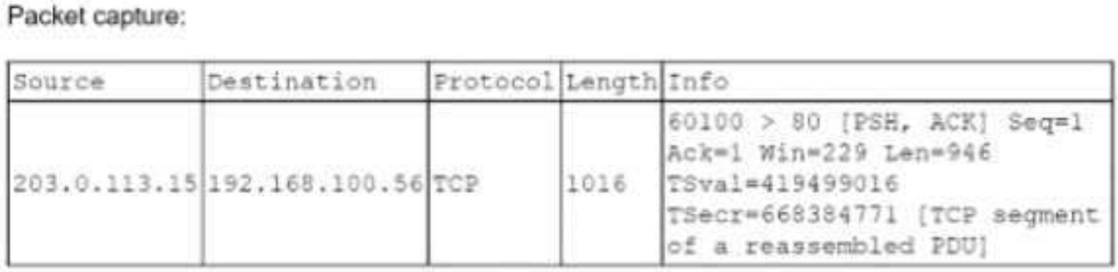
Answer: C

QUESTION 846
A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

A. Implement port security with one MAC address per network port of the switch.
B. Deploy network address protection with DHCP and dynamic VLANs.
C. Configure 802.1X and EAPOL across the network
D. Implement software-defined networking and security groups for isolation

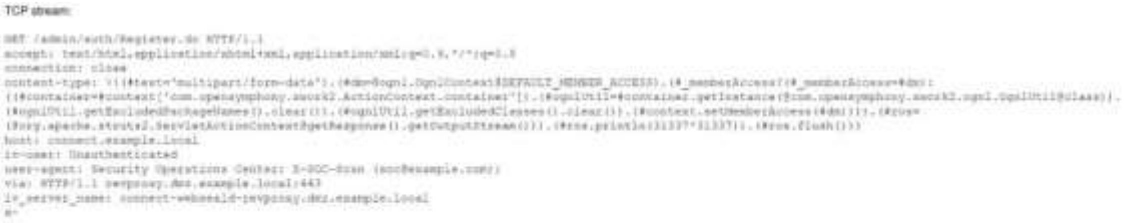
Answer: C

QUESTION 847
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
ir-user: Unauthenticated
user-agent: Security Operations Center: X-SOC-Scan (soc@example.com)
via: HTTP/1.1 revproxy.dmz.example.local:443
ir_server_name: connect-webseald-revproxy.dmz.example.local
a-
```

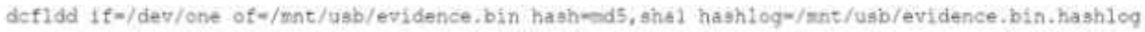
Winch of the following actions should the security analyst lake NEXT?

A. Review the known Apache vulnerabilities to determine if a compromise actually occurred
B. Contact the application owner for connect example local tor additional information
C. Mark the alert as a false positive scan coming from an approved source.

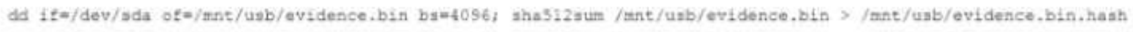
D. Raise a request to the firewall team to block 203.0.113.15.

Answer: D

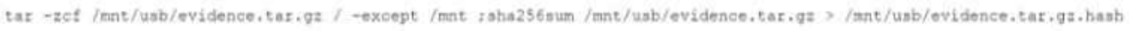
QUESTION 848
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?

A.


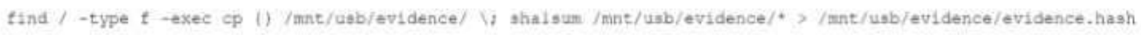
```
dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5,sha1 hashlog=/mnt/usb/evidence.bin.hashlog
```

B.


```
dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
```

C.


```
tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt ;sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
```

D.


```
find / -type f -exec cp {} /mnt/usb/evidence/ \; sha1sum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash
```

Answer: B

QUESTION 849
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. Block the sender In the email gateway.
B. Delete the email from the company's email servers.
C. Ask the sender to stop sending messages.
D. Review the message in a secure environment.

Answer: D

QUESTION 850
Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

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

Answer: B

QUESTION 851
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 business Impact analysis
B. A system assessment
C. Communication of the risk factors
D. A risk identification process

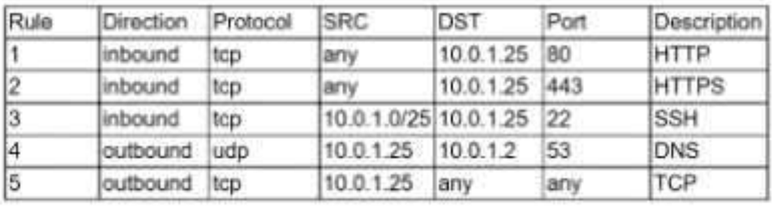
Answer: D

QUESTION 852
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following BST describes the result the security learn hopes to accomplish by adding these sources?

A. Data enrichment
B. Continuous integration
C. Machine learning
D. Workflow orchestration

Answer: A

QUESTION 853
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 1.2. and 3.
B. Remove rules 1.2. 4. and 5.
C. Remove rules 1.2. 3.4. and 5.
D. Remove rules 1.2. and 5.
E. Remove rules 1.4. and 5.
F. Remove rules 4 and 5

Answer: D
\