Exam Questions SY0-601

CompTIA Security+ Exam

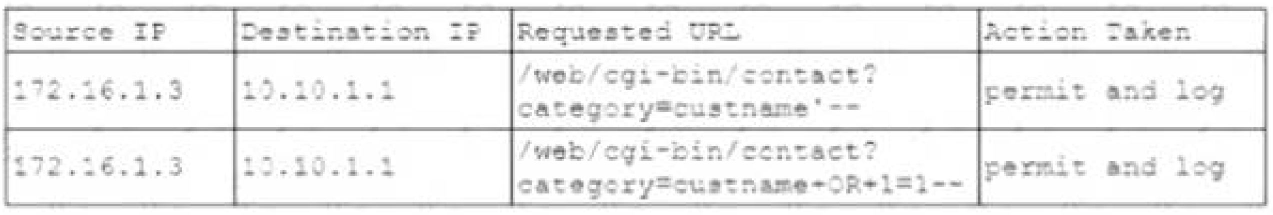
https://www.2passeasy.com/dumps/SY0-601/

NEW QUESTION 1
- (Exam Topic 1)
A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?

A. SSO
B. IDS
C. MFA
D. TPM

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:



Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

A. XSS attack
B. SQLi attack
C. Replay attack
D. XSRF attack

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
Which of the following would detect intrusions at the perimeter of an airport?

A. Signage
B. Fencing
C. Motion sensors
D. Lighting
E. Bollards

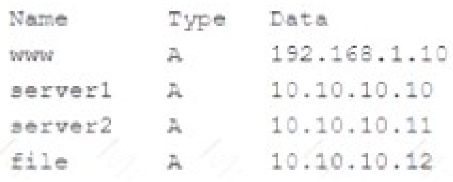
Answer: C

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:



```
Name      Type   Data
www       A      192.168.1.10
server1   A      10.10.10.10
server2   A      10.10.10.11
file      A      10.10.10.12
```

Which of the following attacks has taken place?

A. Domain reputation
B. Domain hijacking
C. Disassociation
D. DNS poisoning

Answer: D

NEW QUESTION 6
- (Exam Topic 1)
An amusement park is implementing a btomelnc system that validates customers' fingerpnnts to ensure they are not sharing tickets The park's owner values customers above all and would prefer customers' convenience over security For this reason which of the following features should the security team prioritize FIRST?

A. Low FAR
B. Low efficacy
C. Low FRR
D. Low CER

Answer: C

Explanation:
FAR (False Acceptance Rate) FRR (False Rejection Rate)
CER (Crossover Error Rate) AKA ERR (Equal Error Rate)
since he is willing to sacrifice Security for Customer Service, Best way to understand this is. FAR has to go up in order for FRR to go down.
typical business practice is in the middle of both which would be near the CER.

NEW QUESTION 7
- (Exam Topic 1)
An organization is building backup server rooms in geographically diverse locations The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room Which of the following should the systems engineer consider?

A. Purchasing hardware from different vendors
B. Migrating workloads to public cloud infrastructure
C. Implementing a robust patch management solution
D. Designing new detective security controls

Answer: A

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
An employee received a word processing file that was delivered as an email attachment The subject line and email content enticed the employee to open the attachment. Which of the following attack vectors BEST matches this malware?

A. Embedded Python code
B. Macro-enabled file
C. Bash scripting
D. Credential-harvesting website

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:

A. employees of other companies and the press
B. all members of the department that created the documents
C. only the company's employees and those listed in the document
D. only the individuate listed in the documents

Answer: A

NEW QUESTION 10
- (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 14
- (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 17
- (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 19
- (Exam Topic 1)
A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data toss?

A. Logic bomb
B. Ransomware
C. Fileless virus
D. Remote access Trojans
E. Rootkit

Answer: A

NEW QUESTION 23
- (Exam Topic 1)
An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps Which of the following control types has the organization implemented?

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

Answer: C

Explanation:
the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. Compensating means to substitute one control with another (not happened here), Corrective means the attack has already happened (no mentioning), and detective is incorrect because the detective control detects ATTACKS, not vulnerabilities.

NEW QUESTION 27
- (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 32
- (Exam Topic 1)
Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?

A. The business continuity plan
B. The retention policy

C. The disaster recovery plan
D. The incident response plan

Answer: A

Explanation:
BCP is to empower an organization to keep crucial functions running during downtime. This, in turn, helps the organization respond quickly to an interruption, while creating resilient operational protocols.

NEW QUESTION 34
- (Exam Topic 1)
An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

A. Application allow list
B. SWG
C. Host-based firewall
D. VPN

Answer: B

NEW QUESTION 38
- (Exam Topic 1)
After reluming from a conference, a user's laptop has been operating slower than normal and overheating and the fans have been running constantly Dunng the diagnosis process, an unknown piece of hardware is found connected to the laptop's motherboard Which of the following attack vectors was exploited to install the hardware?

A. Removable media
B. Spear phishing
C. Supply chain
D. Direct access

Answer: D

NEW QUESTION 39
- (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 44
- (Exam Topic 1)
Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

A. EOL
B. SLA
C. MOU
D. EOSL

Answer: B

NEW QUESTION 45
- (Exam Topic 1)
An organization maintains several environments in which patches are developed and tested before deployed to an operation status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?

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

Answer: D

Explanation:
The staging environment is an optional environment, but it is commonly used when an organization has multiple production environments. After passing testing, the system moves into staging, from where it can be deployed to the different production systems.

NEW QUESTION 46
- (Exam Topic 1)
As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

A. User behavior analysis
B. Packet captures
C. Configuration reviews
D. Log analysis

Answer: D

Explanation:
A vulnerability scanner is essentially doing that. It scans every part of your network configuration that it can, and determines if known vulnerabilities are known at any point of that.

NEW QUESTION 47
- (Exam Topic 1)
Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

A. Common Weakness Enumeration
B. OSINT
C. Dark web
D. Vulnerability databases

Answer: C

NEW QUESTION 49
- (Exam Topic 1)
A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field. Which of the following concepts does this message describe?

A. Password complexity
B. Password reuse
C. Password history
D. Password age

Answer: A

NEW QUESTION 51
- (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 52
- (Exam Topic 1)
Which of the following describes the exploitation of an interactive process to gain access to restncted areas?

A. Persistence
B. Buffer overflow
C. Privilege escalation
D. Pharming

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%2

NEW QUESTION 55
- (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 60
- (Exam Topic 1)
Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU
B. ISA
C. SLA
D. NDA

Answer: A

Explanation:
A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.
https://csrc.nist.gov/glossary/term/interconnection_security_agreement

NEW QUESTION 65
- (Exam Topic 1)
A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department Which of the following account types Is MOST appropriate for this purpose?

A. Service
B. Shared
C. eneric
D. Admin

Answer: A

NEW QUESTION 67
- (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 69
- (Exam Topic 1)
Which of the following will increase cryptographic security?

A. High data entropy
B. Algorithms that require less computing power
C. Longer key longevity
D. Hashing

Answer: C

NEW QUESTION 71
- (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 75

- (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

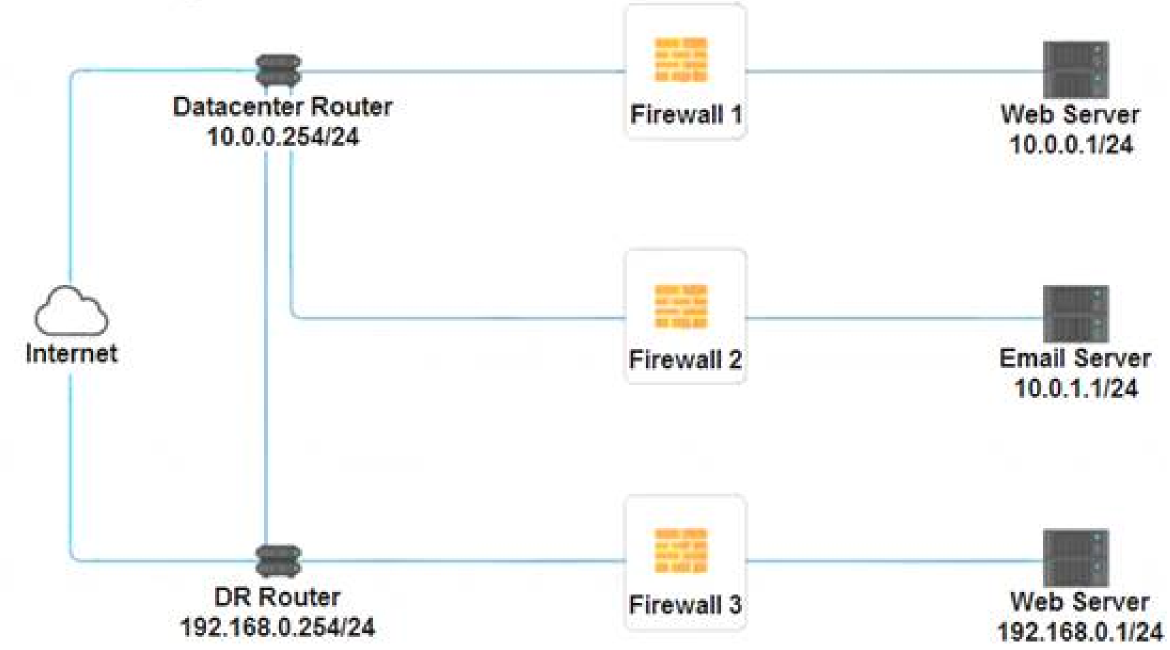
Click on each firewall to do the following:

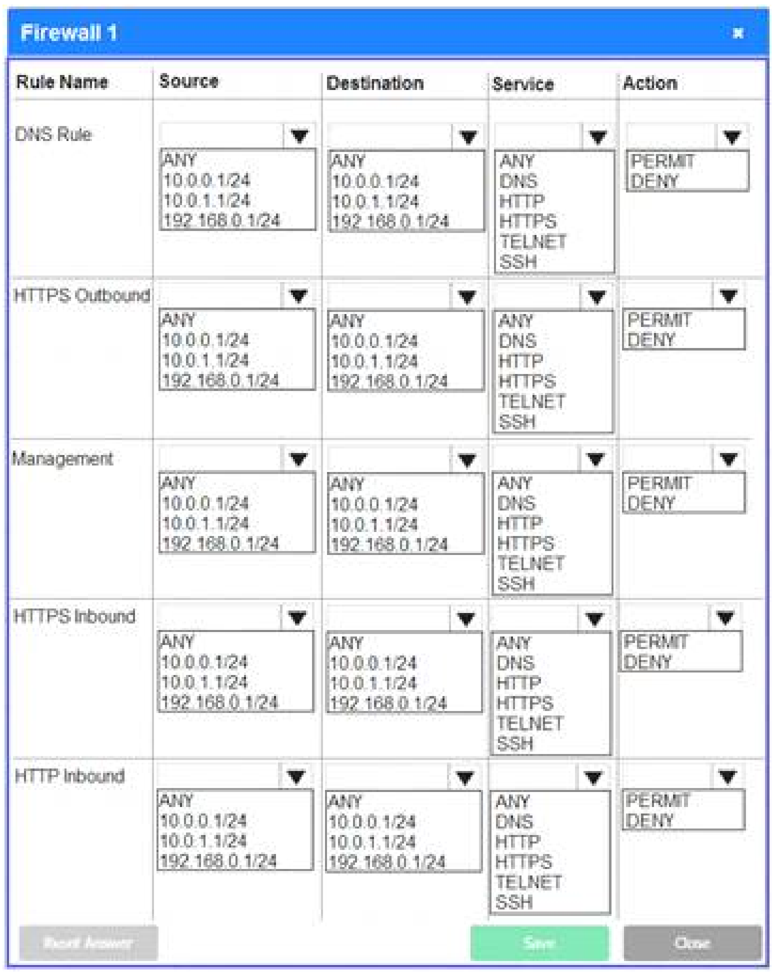
- Deny cleartext web traffic.
- Ensure secure management protocols are used. Please Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

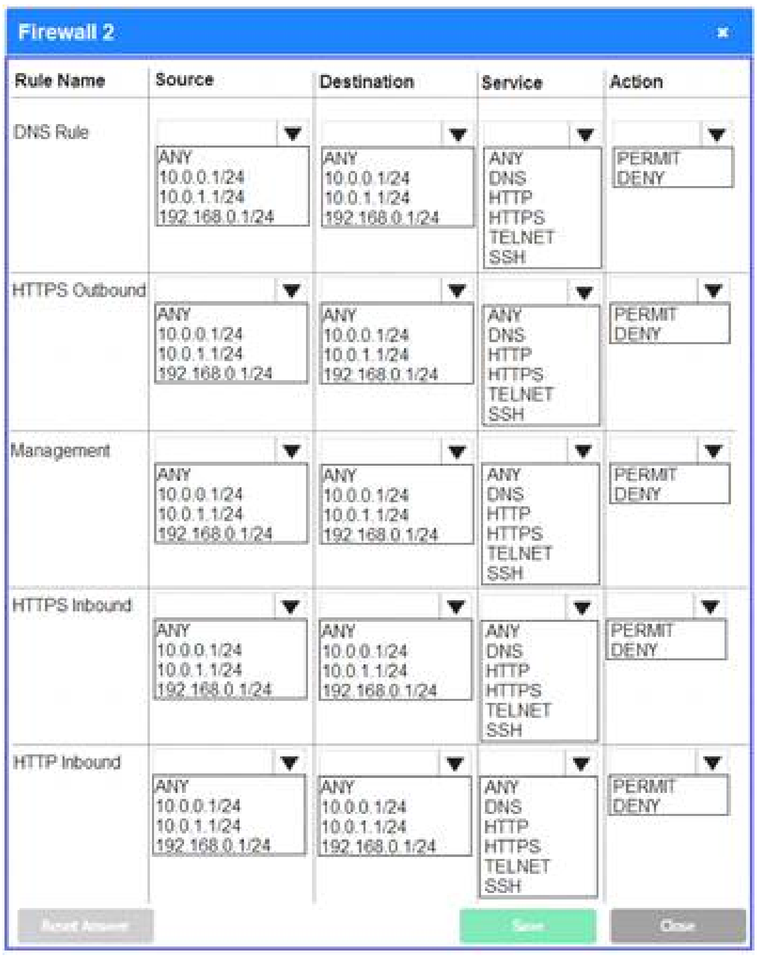
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram



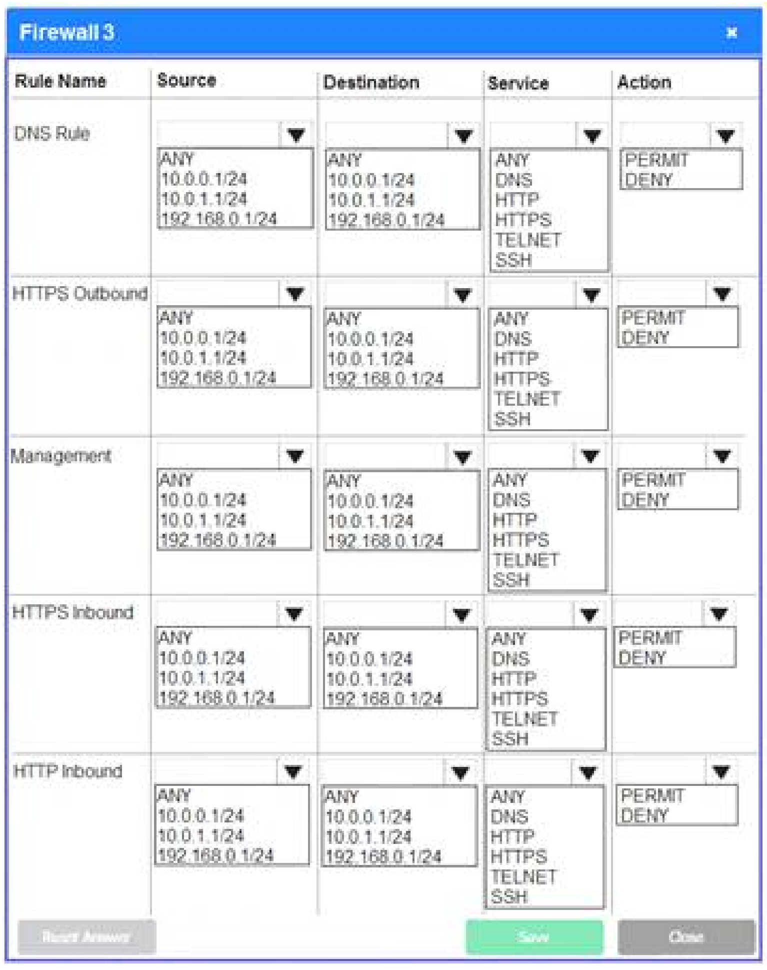


Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS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



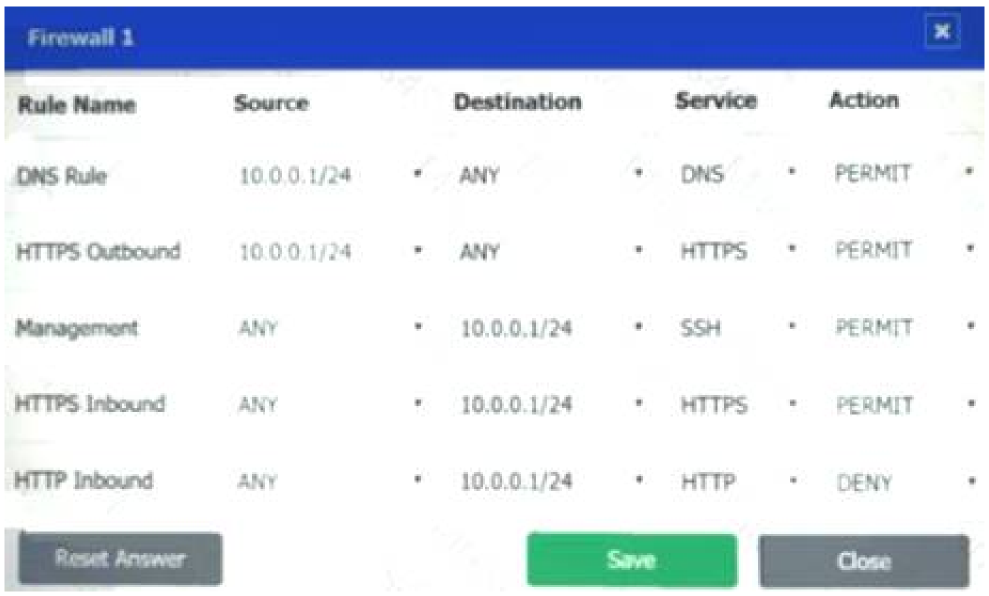
Firewall 3

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

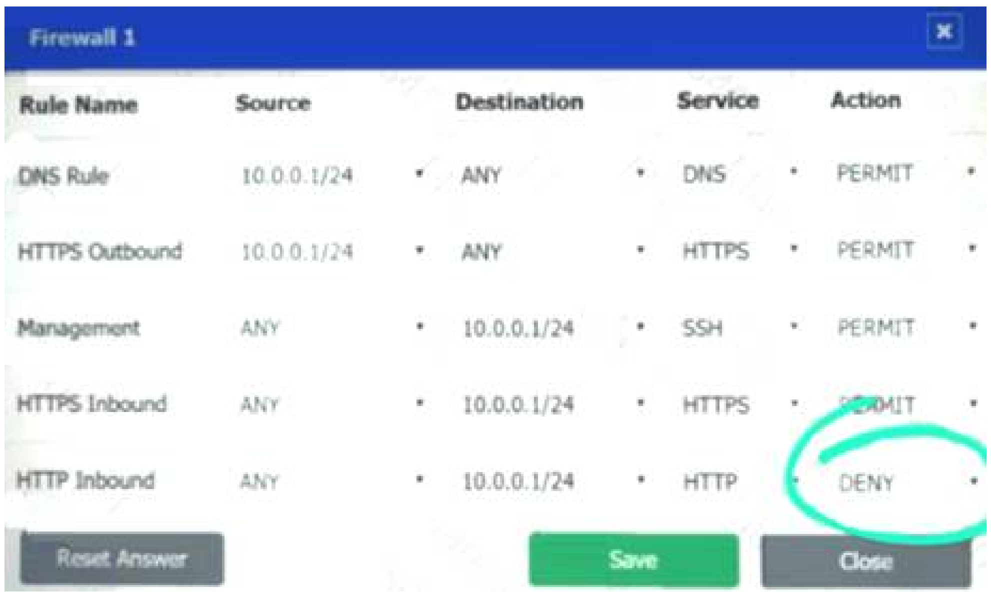
Answer: A

Explanation:
Firewall 1:



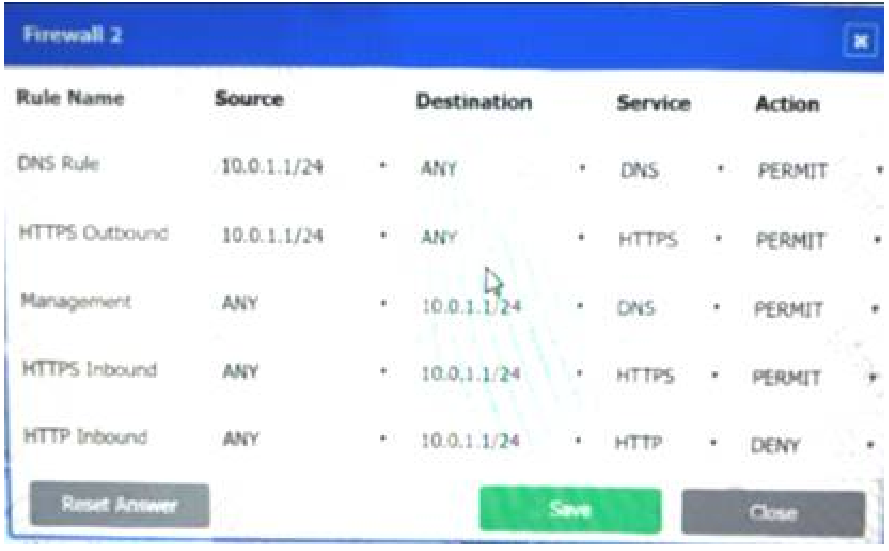
Firewall 1

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

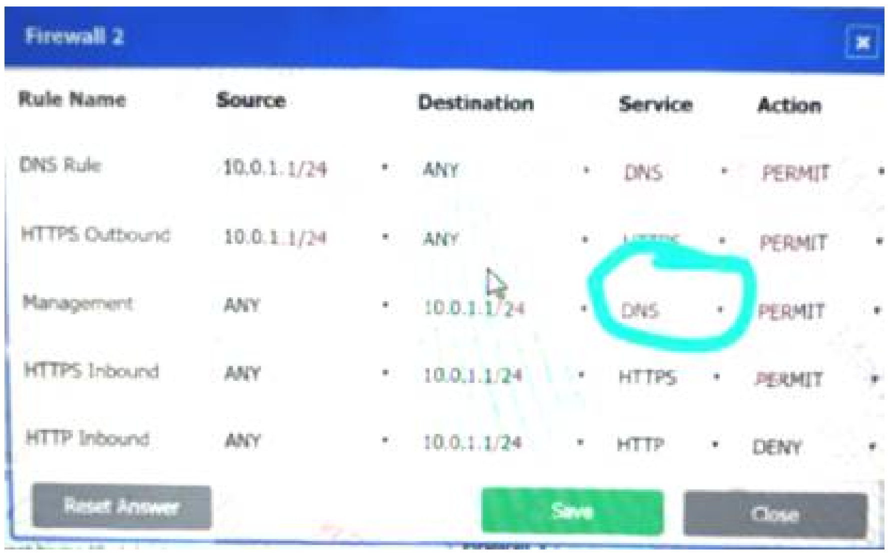


Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

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

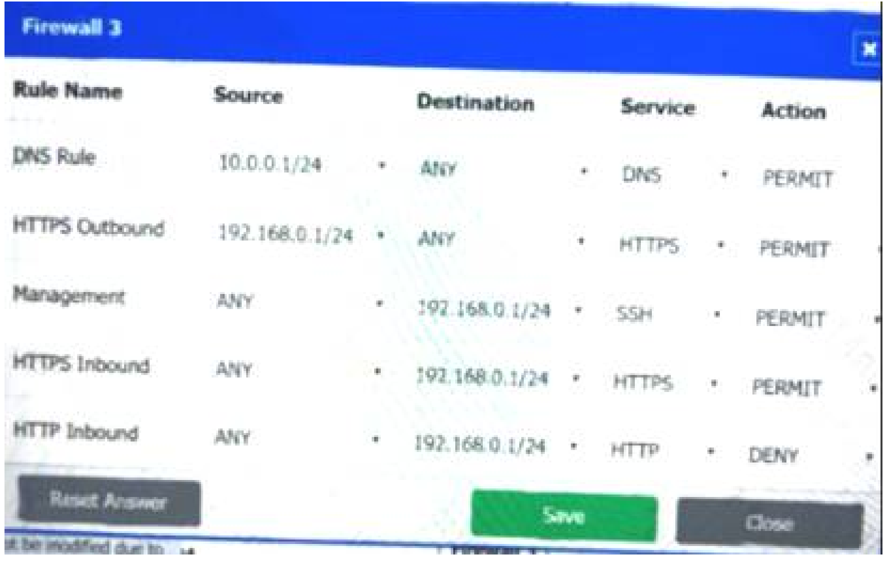


Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

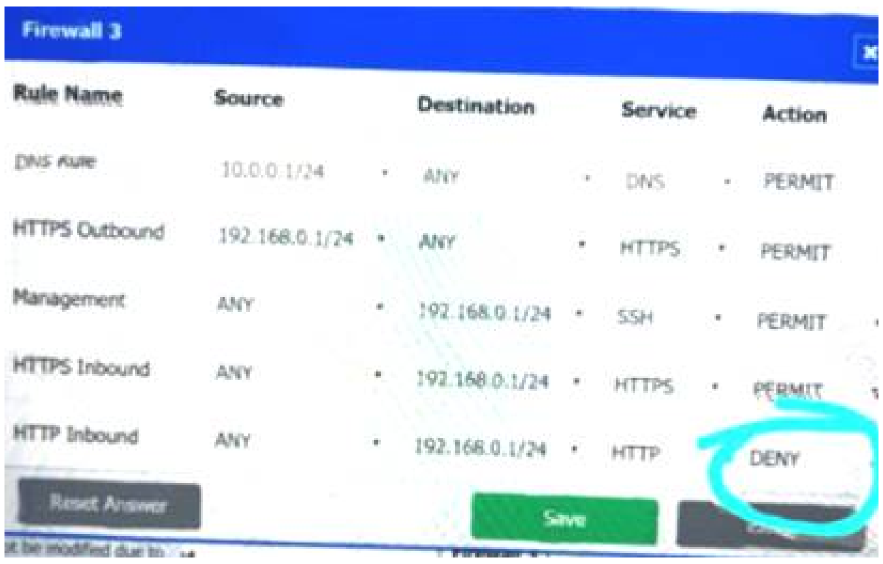


Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

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



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 77
- (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 80
- (Exam Topic 1)
A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?

A. HTTP security header
B. DNSSEC implementation
C. SRTP
D. S/MIME

Answer: C

NEW QUESTION 82
- (Exam Topic 1)
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement?

A. Proxy server
B. WAF
C. Load balancer
D. VPN

Answer: B

NEW QUESTION 85
- (Exam Topic 1)
A cloud service provider has created an environment where customers can connect existing local networks to the cloud for additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?

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

Answer: C

Explanation:
Hybrid cloud refers to a mixed computing, storage, and services environment made up of on-premises infrastructure, private cloud services, and a public cloud—such as Amazon Web Services (AWS) or Microsoft Azure—with orchestration among the various platforms

NEW QUESTION 86
- (Exam Topic 1)
A Chief Information Security Officer has defined resiliency requirements for a new data center architecture The requirements are as follows
• Critical fileshares will remain accessible during and after a natural disaster
• Frve percent of hard disks can fail at any given time without impacting the data.
• Systems will be forced to shut down gracefully when battery levels are below 20% Which of the following are required to BEST meet these objectives? (Select THREE)

A. Fiber switching

B. laC
C. NAS
D. RAID
E. UPS
F. Redundant power supplies
G. Geographic dispersal
H. Snapshots
I. Load balancing

Answer: DEG

NEW QUESTION 90
- (Exam Topic 1)
A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers Which of the following is the BEST remediation strategy?

A. Update the base container image and redeploy the environment
B. Include the containers in the regular patching schedule for servers
C. Patch each running container individually and test the application
D. Update the host in which the containers are running

Answer: C

NEW QUESTION 92
- (Exam Topic 1)
A security analyst receives an alert from trie company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192 168.3426. Which of the following describes this type of alert?

A. True positive
B. True negative
C. False positive
D. False negative

Answer: C

NEW QUESTION 97
- (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 101
- (Exam Topic 2)
A security analyst is tasked with defining the “something you are“ factor of the company’s MFA settings. Which of the following is BEST to use to complete the configuration?

A. Gait analysis
B. Vein
C. Soft token
D. HMAC-based, one-time password

Answer: A

NEW QUESTION 105
- (Exam Topic 2)
An organization is planning to roll out a new mobile device policy and issue each employee a new laptop, These laptops would access the users' corporate operating system remotely and allow them to use the laptops for purposes outside of their job roles. Which of the following deployment models is being utilized?

A. MDM and application management
B. BYOO and containers
C. COPE and VDI
D. CYOD and VMs

Answer: C

NEW QUESTION 107
- (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 111
- (Exam Topic 2)
Which of the following typically uses a combination of human and artificial intelligence to analyze event data and take action without intervention?

A. TTP
B. OSINT
C. SOAR
D. SIEM

Answer: C

NEW QUESTION 116
- (Exam Topic 2)
A user reports falling for a phishing email to an analyst. Which of the following system logs would the analyst check FIRST?

A. DNS
B. Message gateway
C. Network
D. Authentication

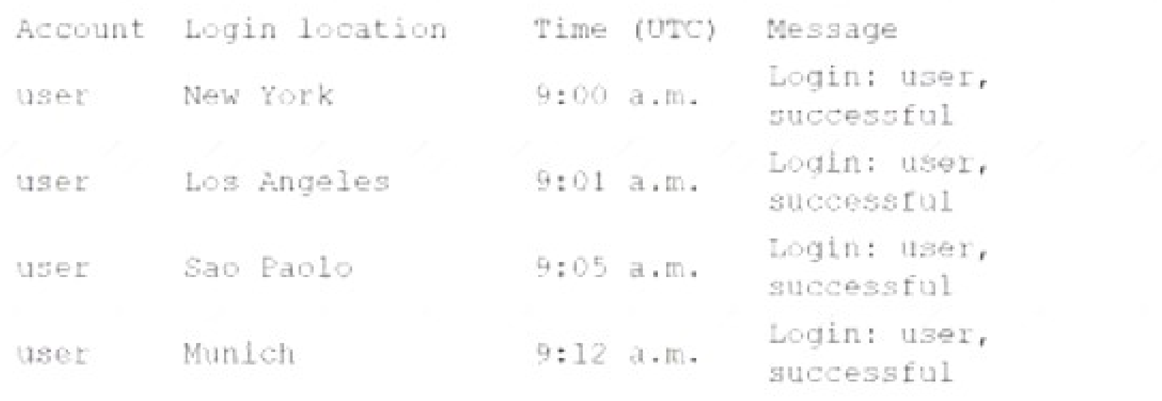
Answer: B

NEW QUESTION 118
- (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 122
- (Exam Topic 2)
During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:



Account	Login location	Time (UTC)	Message
user	New York	9:00 a.m.	Login: user, successful
user	Los Angeles	9:01 a.m.	Login: user, successful
user	Sao Paolo	9:05 a.m.	Login: user, successful
user	Munich	9:12 a.m.	Login: user, successful

Which Of the following account policies would BEST prevent attackers from logging in as user?

A. Impossible travel time
B. Geofencing
C. Time-based logins
D. Geolocation

Answer: A

NEW QUESTION 124
- (Exam Topic 2)
Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only.
In order to proceed past that banner. users must click the OK button. Which of the following is this an example of?

A. AUP
B. NDA
C. SLA

D. MOU

Answer: A

NEW QUESTION 129
- (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 134
- (Exam Topic 2)
A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?

A. Reverse proxy
B. NIC teaming
C. Load balancer
D. Forward proxy

Answer: B

NEW QUESTION 135
- (Exam Topic 2)
A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

A. The order of volatility
B. A CRC32 checksum
C. The provenance of the artifacts
D. The vendor's name
E. The date time
F. A warning banner

Answer: AE

NEW QUESTION 137
- (Exam Topic 2)
Which of the following controls is used to make an organization initially aware of a data compromise?

A. Protective
B. Preventative
C. Corrective
D. Detective

Answer: D

Explanation:
https://purplesec.us/security-controls/

NEW QUESTION 139
- (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 140
- (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 144
- (Exam Topic 2)
A company's security team received notice of a critical vulnerability affecting a high-profile device within the web infrastructure. The vendor patch was just made available online but has not yet been regression tested in development environments. In the interim, firewall rules were implemented to reduce the access to the interface affected by the vulnerability. Which of the following controls does this scenario describe?

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

Answer: B

NEW QUESTION 149
- (Exam Topic 2)
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: B

NEW QUESTION 154
- (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 155
- (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 156
- (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 160
- (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 164
- (Exam Topic 2)
During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?

A. dd
B. memdump
C. tcpdump
D. head

Answer: A

NEW QUESTION 166
- (Exam Topic 2)
A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?

A. Time-based logins
B. Geofencing
C. Network location
D. Password history

Answer: A

NEW QUESTION 167
- (Exam Topic 2)
A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security team has been instructed to resolve the problem as quickly as possible causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?

A. Update the host firewalls to block outbound SMB.
B. Place the machines with the unapproved software in containment.
C. Place the unauthorized application in a blocklist.
D. Implement a content filter to block the unauthorized software communication.

Answer: B

NEW QUESTION 172
- (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 175
- (Exam Topic 2)
A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?

A. Race-condition
B. Pass-the-hash
C. Buffer overflow
D. XSS

Answer: C

NEW QUESTION 176
- (Exam Topic 3)
A root cause analysis reveals that a web application outage was caused by one of the company’s developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

Answer: C

Explanation:
Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

NEW QUESTION 177
- (Exam Topic 3)
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Answer: B

NEW QUESTION 178
- (Exam Topic 3)
A news article states that a popular web browser deployed on all corporate PCs is vulnerable to a zero-day attack. Which of the following MOST concerns the Chief Information Security Officer about the information in the news article?

A. Insider threats have compromised this network.
B. Web browsing is not functional for the entire network.
C. Antivirus signatures are required to be updated immediately.
D. No patches are available for the web browser.

Answer: D

NEW QUESTION 183
- (Exam Topic 3)
An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 184
- (Exam Topic 3)
A security monitoring company offers a service that alerts its customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?

A. STIX
B. The dark web
C. TAXI
D. Social media
E. PCI

Answer: B

NEW QUESTION 185
- (Exam Topic 3)
Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

A. SIEM
B. CASB
C. UTM
D. DLP

Answer: B

Explanation:
Microsoft has a straightforward definition and it includes DLP. "is a security policy enforcement point positioned between enterprise users and cloud service providers"
https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb
A cloud access security broker (CASB) works by securing data flowing to and from in-house IT architectures and cloud vendor environments using an organization's security policies. CASBs protect enterprise systems against cyberattacks through malware prevention and provide data security through encryption, making data streams unreadable to outside parties. CASBs were created with one thing in mind: protecting proprietary data stored in external, third-party media. CASBs deliver capabilities not generally available in traditional controls such as secure web gateways (SWGs) and enterprise firewalls. CASBs provide policy and governance concurrently across multiple cloud services and provide granular visibility into and control over user activities. https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker

NEW QUESTION 189
- (Exam Topic 3)
A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security
assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head
B. Tcpdump
C. grep
D. rail
E. curl
F. openssi
G. dd

Answer: AC

Explanation:
A - "analyst needs to review the first transactions quickly"
C - "search the entire series of requests for a particular string"

NEW QUESTION 193
- (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 197
- (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 200
- (Exam Topic 3)
A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 204
- (Exam Topic 3)
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Answer: C

NEW QUESTION 205
- (Exam Topic 3)
A network engineer at a company with a web server is building a new web environment with the following requirements:
* Only one web server at a time can service requests.
* If the primary web server fails, a failover needs to occur to ensure the secondary web server becomes the primary.
Which of the following load-balancing options BEST fits the requirements?

A. Cookie-based
B. Active-passive
C. Persistence
D. Round robin

Answer: A

NEW QUESTION 206
- (Exam Topic 3)
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

A. A captive portal
B. PSK
C. 802.1X
D. WPS

Answer: C

NEW QUESTION 211
- (Exam Topic 3)
A security engi is cor that the gy tor on endpoints ts too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key Mes and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?

A. NIDS
B. HIPS
C. AV
D. NGFW

Answer: A

NEW QUESTION 214
- (Exam Topic 3)
An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization’s needs for a third factor?

A. Date of birth
B. Fingerprints
C. PIN
D. TPM

Answer: B

NEW QUESTION 218
- (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 220
- (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 221
- (Exam Topic 3)
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

Answer: A

NEW QUESTION 224
- (Exam Topic 3)

A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to implement a high availability pair to:

A. ned that business may be negatecrease the mean time between failures.
B. remove the single point of failure.
C. cut down the mean time to repair,
D. reduce the recovery time objective.

Answer: B

NEW QUESTION 229
- (Exam Topic 3)
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols

Answer: AC

NEW QUESTION 234
- (Exam Topic 3)
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Answer: B

NEW QUESTION 238
- (Exam Topic 3)
A security engineer needs to Implement the following requirements:
• All Layer 2 switches should leverage Active Directory tor authentication.
• All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
• All Layer 2 switches are not the same and are manufactured by several vendors.
Which of the following actions should the engineer take to meet these requirements? (Select TWO). Implement RADIUS.

A. Configure AAA on the switch with local login as secondary
B. Configure port security on the switch with the secondary login method.
C. Implement TACACS+
D. Enable the local firewall on the Active Directory server.
E. Implement a DHCP server

Answer: AB

NEW QUESTION 239
- (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 243
- (Exam Topic 3)
Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

Answer: A

NEW QUESTION 247
- (Exam Topic 3)
To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

Answer: C

NEW QUESTION 252
- (Exam Topic 3)
A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

Answer: D

NEW QUESTION 255
- (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 258
- (Exam Topic 3)
A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Answer: B

Explanation:
"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker."
For purposes of knowing, https://security.opentext.com/tableau/hardware/details/t8u write blockers like this are the most popular hardware blockers

NEW QUESTION 261
- (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 266
- (Exam Topic 3)
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

A. The S/MME plug-in is not enabled.
B. The SLL certificate has expired.
C. Secure IMAP was not implemented
D. POP3S is not supported

Answer: A

NEW QUESTION 271
- (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 273
- (Exam Topic 3)
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

Answer: A

Explanation:
An attack in which an attacker targets specific groups or organizations, discovers which websites they frequent, and injects malicious code into those sites.

NEW QUESTION 274
- (Exam Topic 3)
Which of the following would satisfy three-factor authentication?

A. Password, retina scanner, and NFC card
B. Password, fingerprint scanner, and retina scanner
C. Password, hard token, and NFC card
D. Fingerpnint scanner, hard token, and retina scanner

Answer: C

NEW QUESTION 276
- (Exam Topic 3)
An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering it the organization may need to scale down just as quickly as it scaled up. The ClO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the ClO's concerns?

A. Disallow new hires from using mobile devices for six months
B. Select four devices for the sales department to use in a CYOD model
C. Implement BYOD for the sates department while leveraging the MDM
D. Deploy mobile devices using the COPE methodology

Answer: C

NEW QUESTION 281
- (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 284

- (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 285
- (Exam Topic 3)
Which of the fofowing should an organization conskier implementing in the event executives need to speak to the media after a publicized data breach?

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

Answer: C

NEW QUESTION 290
- (Exam Topic 3)
A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

A. RA1D 0
B. RAID1
C. RAID 5
D. RAID 10

Answer: A

Explanation:
https://techgenix.com/raid-10-vs-raid-5/

NEW QUESTION 292
- (Exam Topic 3)
A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth
B. SSO
C. SAML
D. PAP

Answer: C

NEW QUESTION 293
- (Exam Topic 3)
A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?

A. netstat
B. net share
C. netcat
D. nbtstat
E. net session

Answer: A

NEW QUESTION 297
- (Exam Topic 3)
A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

A. DNS sinkholding
B. DLP rules on the terminal
C. An IP blacklist
D. Application whitelisting

Answer: D

NEW QUESTION 298
- (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 300
- (Exam Topic 3)
A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

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

Answer: C

NEW QUESTION 304
- (Exam Topic 3)
A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

A. # iptables -t mangle -X
B. # iptables –F
C. # iptables -Z
D. # iptables -P INPUT -j DROP

Answer: D

NEW QUESTION 307
- (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 312
- (Exam Topic 3)
A RAT that was used to compromise an organization’s banking credentials was found on a user’s computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary

Answer: C

NEW QUESTION 313
- (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 317
- (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 321
- (Exam Topic 3)
When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

Answer: C

NEW QUESTION 323
- (Exam Topic 3)
Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer
B. The data processor
C. The data owner
D. The data controller

Answer: C

NEW QUESTION 327
- (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 329
- (Exam Topic 3)
A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?

A. Port
B. Intrusive
C. Host discovery
D. Credentialed

Answer: D

NEW QUESTION 333
- (Exam Topic 3)
A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME
B. DLP
C. IMAP
D. HIDS

Answer: B

Explanation:
Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

NEW QUESTION 335
- (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 338
- (Exam Topic 3)
When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

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

Answer: D

Explanation:
Risk Transference refers to the shifting of the burden of loss for a risk to another party through legislation, contract, insurance or other means. https://www.bcmpedia.org/wiki/Risk_Transference

NEW QUESTION 342
- (Exam Topic 3)
Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification
B. Accountability
C. Legal hald
D. Chain of custody

Answer: C

NEW QUESTION 345
- (Exam Topic 3)
A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

A. Verification
B. Validation
C. Normalization
D. Staging

Answer: A

NEW QUESTION 349
- (Exam Topic 3)
Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.
B. Implement an IDS/IPS
C. Implement a heuristic behavior-detection solution.
D. Implement CASB to protect the network shares.

Answer: C

Explanation:
Heuristic analysis is also one of the few methods capable of combating polymorphic viruses — the term for malicious code that constantly changes and adapts. Heuristic analysis is incorporated into advanced security solutions offered by companies like Kaspersky Labs to detect new threats before they cause harm, without the need for a specific signature. https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis

NEW QUESTION 351
- (Exam Topic 3)
A security analyst Is hardening a Linux workstation and must ensure It has public keys forwarded to remote systems for secure login Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

A. Forward the keys using ssh-copy-id.
B. Forward the keys using scp.
C. Forward the keys using ash -i.
D. Forward the keys using openssl -s.
E. Forward the keys using ssh-keyger.

Answer: AD

NEW QUESTION 354

- (Exam Topic 3)
Which of the following corporate policies is used to help prevent employee fraud and to detect system log modifications or other malicious activity based on tenure?

A. Background checks
B. Mandatory vacation
C. Social media analysis
D. Separation of duties

Answer: B

NEW QUESTION 355
- (Exam Topic 3)
Which of the following control sets should a well-written BCP include? (Select THREE)

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

Answer: ADG

NEW QUESTION 357
- (Exam Topic 3)
ecent changes toa company's BYOD policy require all personal mobile devices to use a two-factor authentication method that Is not something you know or have.
Which of the following will meet this requirement?

A. Facial recognition
B. Six-digit PIN
C. PKI certificate
D. Smart card

Answer: C

NEW QUESTION 358
- (Exam Topic 3)
Which of the following describes the ability of code to target a hypervisor from inside

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Answer: B

Explanation:
Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%

NEW QUESTION 361
- (Exam Topic 3)
Which of the following would be used to find the MOST common web-application vulnerabilities?

A. OWASP
B. MITRE ATT&CK
C. Cyber Kill Chain
D. SDLC

Answer: A

NEW QUESTION 364
- (Exam Topic 3)
Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

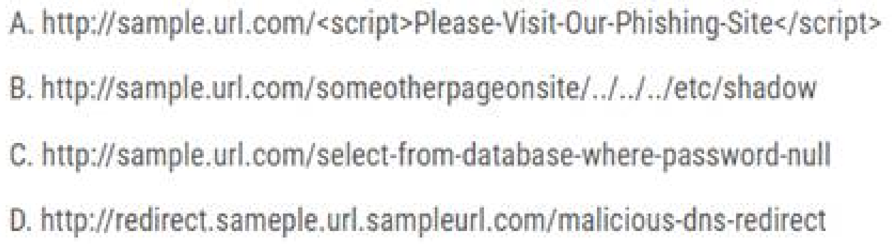
Answer: B

NEW QUESTION 368
- (Exam Topic 3)
A penetration tester gains access to a network by exploiting a vulnerability on a public-facing web server. Which of the following techniques will the tester most likely perform NEXT?

A. Gather more Information about the target through passive reconnaissance.
B. Establish rules of engagement before proceeding.
C. Create a user account to maintain persistence.
D. Move laterally throughout the network to search for sensitive information.

Answer: C

NEW QUESTION 373
- (Exam Topic 3)
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?



A. http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>

B. http://sample.url.com/someotherpageonsite/../../../etc/shadow

C. http://sample.url.com/select-from-database-where-password-null

D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect

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

Answer: B

NEW QUESTION 376
- (Exam Topic 3)
Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee’s workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

A. A worm that has propagated itself across the intranet, which was initiated by presentation media
B. A fileless virus that is contained on a vCard that is attempting to execute an attack
C. A Trojan that has passed through and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Answer: A

NEW QUESTION 380
- (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 381
- (Exam Topic 3)
uring an investigation, a security manager receives notification from local authorities that company proprietary data was found on a former employee's home computer. The former employee's
corporate workstation has since been repurposed, and the data on the hard drive has been overwritten. Which of the following would BEST provide the security manager with enough details to
determine when the data was removed from the company network?

A. Properly configured hosts with security logging
B. Properly configured endpoint security tool with alerting
C. Properly configured SIEM with retention policies
D. Properly configured USB blocker with encryption

Answer: C

NEW QUESTION 382
- (Exam Topic 3)
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

Answer: DE

NEW QUESTION 385
- (Exam Topic 3)
An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack
B. A watering-hole attack
C. Typo squatting
D. A phishing attack

Answer: B

NEW QUESTION 390
- (Exam Topic 3)
A security analyst Is investigating a malware incident at a company. The malware is accessing a command-and-control website at www.comptia.com. All outbound Intemet traffic is logged to a syslog server and stored in / logfiles/messages. Which of the following commands would be BEST for the analyst to use on the syslog server to search for recent traffic to the command-and-control website?

A. head -500 www.comptia.com | grep /logfiles/messages
B. cat /logfiles/messages | tail -500 wew.comptia.com
C. tail -500 /legfiles/messages | grep www.comptia.com
D. grep -500 /logfiles/messages | cat www.comptia.com

Answer: B

NEW QUESTION 395
- (Exam Topic 3)
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO’s concern? (Select TWO).

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

Answer: AE

NEW QUESTION 398
- (Exam Topic 3)
A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST these requirement?

A. RA
B. OCSP
C. CRL
D. CSR

Answer: C

NEW QUESTION 403
- (Exam Topic 3)
An engineer is configuring AAA authentication on a Cisco MDS 9000 Series Switch. The LDAP server is located under the IP 10.10.2.2. The data sent to the LDAP server should be encrypted. Which command should be used to meet these requirements?

A. Idap-server 10.10.2.2 key SSL_KEY
B. Idap-server host 10.10.2.2 key SSL_KEY
C. Idap-server 10.10.2.2 port 443
D. Idap-server host 10.10.2.2 enable-ssl

Answer: D

NEW QUESTION 404
- (Exam Topic 3)
An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

A. Document the collection and require a sign-off when possession changes.
B. Lock the device in a safe or other secure location to prevent theft or alteration.
C. Place the device in a Faraday cage to prevent corruption of the data.
D. Record the collection in a blockchain-protected public ledger

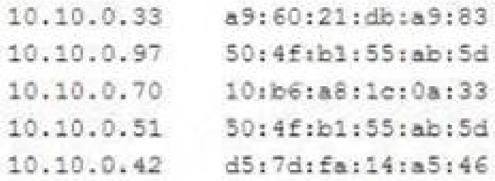
Answer: A

NEW QUESTION 409
- (Exam Topic 3)
The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Answer: A

NEW QUESTION 412
- (Exam Topic 3)
A penetration tester successfully gained access ta a company's network, The investigating analyst detarmines malicious traffic connacted through the WAP despite filtering rules being in place, Logging in to the connected switch, the analyst sees the folowing in the ARP table:



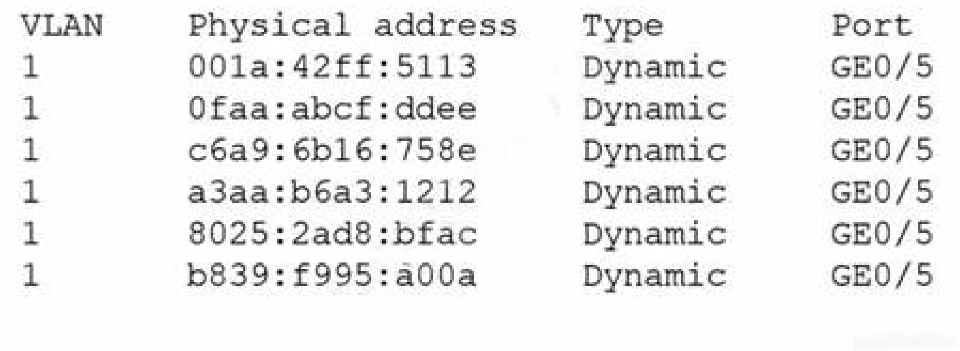
```
10.10.0.33    a9:60:21:db:a9:83
10.10.0.97    50:4f:b1:55:ab:5d
10.10.0.70    10:b6:a8:1c:0a:33
10.10.0.51    50:4f:b1:55:ab:5d
10.10.0.42    d5:7d:fa:14:a5:46
```

Which of the following cid the penetration tester MOST liely use?

A. ARP poisoning
B. MAG eioning
C. Man in the middle
D. Evil twin

Answer: B

NEW QUESTION 414
- (Exam Topic 3)
A security administrator checks the table of a network switch, which shows the following output:



```
VLAN   Physical address   Type      Port
1      001a:42ff:5113     Dynamic   GE0/5
1      0faa:abcf:ddee     Dynamic   GE0/5
1      c6a9:6b16:758e     Dynamic   GE0/5
1      a3aa:b6a3:1212     Dynamic   GE0/5
1      8025:2ad8:bfac     Dynamic   GE0/5
1      b839:f995:a00a     Dynamic   GE0/5
```

Which of the following is happening to this switch?

A. MAC Flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

Answer: A

NEW QUESTION 419
- (Exam Topic 3)
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement
B. Least privilege
C. An acceptable use policy
D. Ofboarding

Answer: D

NEW QUESTION 422
- (Exam Topic 3)
An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Type squatting
C. Impersonation
D. Watering-hole attack

Answer: D

NEW QUESTION 426
- (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 427
- (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 432
- (Exam Topic 3)
In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

Answer: D

NEW QUESTION 433
- (Exam Topic 3)
Which of the following stores data directly on devices with limited processing and storage capacity?

A. Thin client
B. Containers
C. Edge
D. Hybrid cloud

Answer: A

NEW QUESTION 437
- (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 442
- (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 447
- (Exam Topic 3)
Which of the following policies establishes rules to measure third-party work tasks and ensure deliverables are provided within a specific time line?

A. SLA
B. MOU
C. AUP
D. NDA

Answer: A

NEW QUESTION 449
- (Exam Topic 3)
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting

Answer: B

NEW QUESTION 451
- (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 454
- (Exam Topic 3)
An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise.
Which of the following will accomplish this goal?

A. Antivirus
B. IPS.
C. FTP
D. FIM

Answer: D

NEW QUESTION 459
- (Exam Topic 3)
Which of the following describes the BEST approach for deploying application patches?

A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
C. Test the patches m a test environment apply them to the production systems and then apply them to a staging environment
D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Answer: A

Explanation:
https://oroinc.com/b2b-ecommerce/blog/testing-and-staging-environments-in-ecommerce-implementation/

NEW QUESTION 460
- (Exam Topic 3)
A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time In the event of a failure, which being maindful of the limited available storage space?

A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
C. Implement nightly full backups every Sunday at 8:00 p.m
D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

Answer: B

NEW QUESTION 462

- (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 464
- (Exam Topic 3)
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

Answer: A

NEW QUESTION 469
- (Exam Topic 3)
A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

A. Checksums
B. Watermarks
C. Oder of volatility
D. A log analysis
E. A right-to-audit clause

Answer: D

Explanation:
https://www.sumologic.com/glossary/log-analysis/
“While companies can operate private clouds, forensics in a public cloud are complicated by the right to audit permitted to you by your service level agreement (SLA) with the cloud provider.”

NEW QUESTION 474
- (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 476
- (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: C

NEW QUESTION 480
- (Exam Topic 3)
A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization’s network. Which of the following will the analyst MOST likely use to accomplish the objective?

A. A table exercise
B. NST CSF
C. MTRE ATT$CK
D. OWASP

Answer: A

NEW QUESTION 482
- (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 487
- (Exam Topic 3)
Which of the following refers to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Answer: A

NEW QUESTION 492
- (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 493
- (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 494
- (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 499
- (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 501
- (Exam Topic 4)
A systoms administrator needs to instal the seme X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. Asself-signed certificate

C. Cerificate chaining
D. An extended validation certificate

Answer: B

NEW QUESTION 504
- (Exam Topic 4)
A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

A. Fileless malware
B. A downgrade attack
C. A supply-chain attack
D. A logic bomb
E. Misconfigured BIOS

Answer: C

NEW QUESTION 507
- (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 508
- (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 510
- (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 515
- (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 520
- (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 523
- (Exam Topic 4)
The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The
system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?

A. Baseline modification
B. A fileless virus
C. Tainted training data
D. Cryptographic manipulation

Answer: C

NEW QUESTION 525
- (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 530
- (Exam Topic 4)
The website http://companywebsite.com requires users to provide personal information, including security question responses, for registration. Which of the following would MOST likely cause a data breach?

A. Lack of input validation
B. Open permissions
C. Unsecure protocol
D. Missing patches

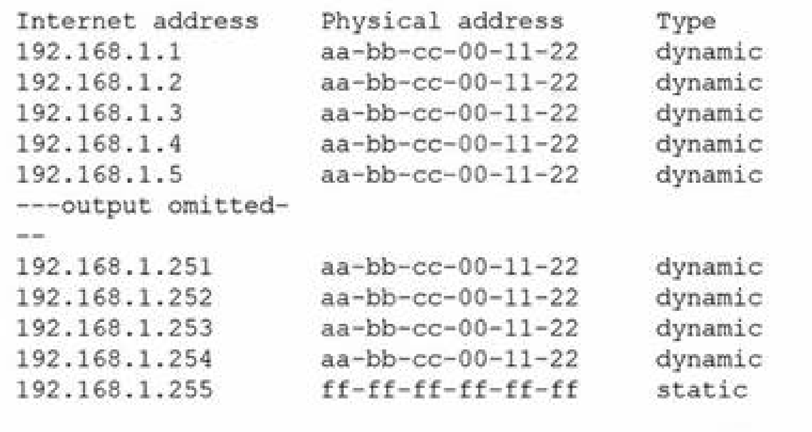
Answer: C

NEW QUESTION 531
- (Exam Topic 4)
When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols

Answer: D

NEW QUESTION 532
- (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 533
- (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 535
- (Exam Topic 4)
A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.
Which of the following tools can the analyst use to verify the permissions?

A. ssh
B. chmod
C. 1s
D. setuid
E. nessus
F. ne

Answer: B

NEW QUESTION 540
- (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. Recowery
C. identiticalion
D. Preparation

Answer: C

NEW QUESTION 542
- (Exam Topic 4)
Asecurity analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the
organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS. Which of the following is the MOST likely attack type?

A. Request forgery
B. Session replay
C. DLL injection
D. Shimming

Answer: A

NEW QUESTION 547
- (Exam Topic 4)
A company Is concerned about ts securkty afler a red-tearn exercise. The report shows the team was able to reach the critical servers due to Ihe SMB being exposed fo the Internet and running NTLMV1, Which of the following BEST explains the findings?

A. Default settings on the servers
B. Unsecuted administrator accounts
C. Open ports and services
D. Weak Gata encryption

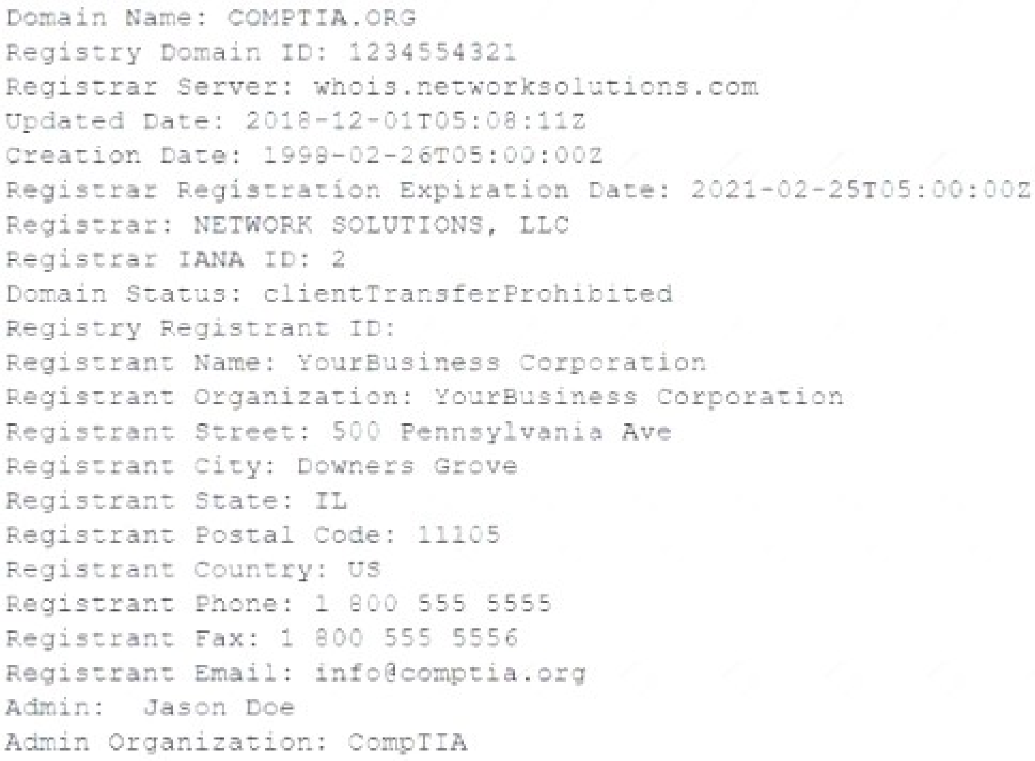
Answer: C

NEW QUESTION 549
- (Exam Topic 4)
A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations. Which of the following would address the CSO's concerns?

A. SPF
B. DMARC
C. SSL
D. DKIM
E. TLS

Answer: E

NEW QUESTION 551
- (Exam Topic 4)
Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:



```
Domain Name: COMPTIA.ORG
Registry Domain ID: 1234554321
Registrar Server: whois.networksolutions.com
Updated Date: 2018-12-01T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC
Registrar IANA ID: 2
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: YourBusiness Corporation
Registrant Organization: YourBusiness Corporation
Registrant Street: 500 Pennsylvania Ave
Registrant City: Downers Grove
Registrant State: IL
Registrant Postal Code: 11105
Registrant Country: US
Registrant Phone: 1 800 555 5555
Registrant Fax: 1 800 555 5556
Registrant Email: info@comptia.org
Admin:  Jason Doe
Admin Organization: CompTIA
```

Which of the following can be determined about the organization's public presence and security posture? (Select TWO).

A. Joe used Whois to produce this output.
B. Joe used cURL to produce this output.
C. Joe used Wireshark to produce this output.
D. The organization has adequate information available in public registration.
E. The organization has too much information available in public registration.
F. The organization has too little information available in public registration.

Answer: AD

NEW QUESTION 552
- (Exam Topic 4)
An analyst is trying to identify insecure services thal are running on the intemal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)

A. SFT
B. FIPS
C. SNMPv2, SNMPv3
D. HTTP, HTTPS D TFTP, FTP
E. SNMPyt, SNMPy2
F. Tenet, SSH
G. TLS, SSL
H. POP, IMAP
I. Login, nogin

Answer: AEG

NEW QUESTION 555
- (Exam Topic 4)
An attacker is attempting to harvest user credentials on a client's wedsite, A security analyst notices multiple attempts of rencom usemames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:
The username you entered does not exist.
Which of the following should the analyst recommend be enabled?

A. Input validation
B. Obfuscation
C. Error handling
D. Username lockout

Answer: B

NEW QUESTION 559
- (Exam Topic 4)
Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers?
accounts. Which of the following should be implemented to prevent similar situations in the future?

A. Ensure input validation is in place to prevent the use of invalid characters and values.
B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.
C. Configure the web application firewall to look for and block session replay attacks.
D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

Answer: A

NEW QUESTION 561
- (Exam Topic 4)
A SECURITY ANALYST NEEDS TO FIND REAL-TIME DATA ON THE LATEST MALWARE AND loCs WHICH OF THE FOLLOWING BEST DESCRIBE THE SOLUTION THE ANALYST SHOULD PERSUE?

A. ADVISORIES AND BULLETINS
B. THREAT FEEDS
C. SECURITY NEWS ARTICLES
D. PEER-REVIEWED CONTENT

Answer: B

NEW QUESTION 565
- (Exam Topic 4)
DURING A SECURITY ASSESSMENT. A SECURITY ANALYST FINDS A FILE WITH OVERLY PERMISSIVE PERMISSION. WICH OF THE FOLLOWING TOOL WILL ALLOW THE ANALYST TO REDUCE THR PERMISSONFOR THE EXIXTING USER AND GROUPS AND REMOVE THE SET-USER-ID BIT FROM THE FILE?

A. 1a
B. Chflaga
C. Chmod
D. Leof
E. aeuid

Answer: C

NEW QUESTION 568
- (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 573
- (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 578
- (Exam Topic 4)
A security administrator needs to inspect in-transit files on the enterprise network to search for Pll, credit card data, and classification words. Which of the following would be the BEST to use?

A. IDS solution
B. EDR solution
C. HIPS software solution
D. Network DLP solution

Answer: D

NEW QUESTION 580
- (Exam Topic 4)
A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform e@ vulnerability scan to identify the weak spots.
B. Use a packet analyzer to investigate the NetFlow traffic
C. Check the SIEM to review the correlated logs.
D. Require access to the routers to view current sessions,

Answer: C

NEW QUESTION 585
- (Exam Topic 4)
A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

A. WEP
B. MSCHAP
C. wes
D. SAE

Answer: D

NEW QUESTION 586
- (Exam Topic 4)
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?

A. Always On
B. Remote access
C. Site-to-site
D. Full tunnel

Answer: C

NEW QUESTION 587
- (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 592
- (Exam Topic 5)
A company recenty experienced an attack during which its main website was Girected to the attacker's web server, allowing the attacker to harvest credentials trom unsuspecting customers, Which of the following should the company implement lo prevent this type of attack from occurring In the future?

A. PSec
B. SSL/TLS
C. ONSSEC
D. SMIME

Answer: B

NEW QUESTION 597
- (Exam Topic 5)
Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

A. Block cipher
B. Hashing
C. Private key
D. Perfect forward secrecy
E. Salting
F. Symmetric keys

Answer: BC

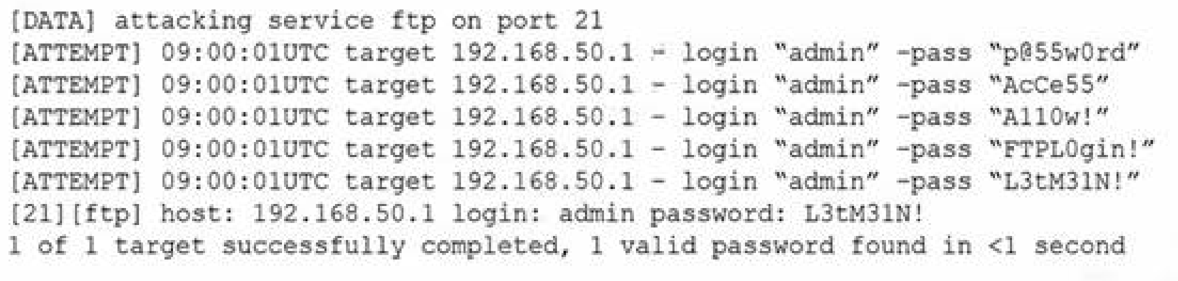
NEW QUESTION 601
- (Exam Topic 5)
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

Answer: B

NEW QUESTION 604
- (Exam Topic 5)

The following are the logs of a successful attack.



```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity
D. Account lockout

Answer: D

NEW QUESTION 605
- (Exam Topic 5)
A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?

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

Answer: B

NEW QUESTION 609
- (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 611
- (Exam Topic 5)
A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor
B. Service requestor
C. Identity provider
D. Service provider
E. Tokenized resource
F. Notarized referral

Answer: BC

NEW QUESTION 614
- (Exam Topic 5)
An enterpnse has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

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

Answer: A

NEW QUESTION 619
- (Exam Topic 5)
Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?

A. Production
B. Test
C. Staging

D. Development

Answer: B

NEW QUESTION 622
- (Exam Topic 5)
Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm
B. The encryption algorithm's longevity
C. A method of introducing entropy into key calculations
D. The computational overhead of calculating the encryption key

Answer: B

NEW QUESTION 626
- (Exam Topic 5)
Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

A. ISO 27701
B. The Center for Internet Security
C. SSAE SOC 2
D. NIST Risk Management Framework

Answer: B

NEW QUESTION 629
- (Exam Topic 5)
The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?

A. CASB
B. VPN concentrator
C. MFA
D. VPC endpoint

Answer: A

NEW QUESTION 633
- (Exam Topic 5)
A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?

A. NIC Teaming
B. Port mirroring
C. Defense in depth
D. High availability
E. Geographic dispersal

Answer: C

NEW QUESTION 637
- (Exam Topic 5)
The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team
B. The vulnerability management team
C. The CIRT
D. The read team

Answer: C

NEW QUESTION 640
- (Exam Topic 5)
A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

Answer: B

NEW QUESTION 641
- (Exam Topic 5)
The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

A. Requiring all new, on-site visitors to configure their devices to use WPS
B. Implementing a new SSID for every event hosted by the college that has visitors
C. Creating a unique PSK for every visitor when they arrive at the reception area
D. Deploying a captive portal to capture visitors' MAC addresses and names

Answer: D

NEW QUESTION 642
- (Exam Topic 5)
A company ts required to continue using legacy softveare to support a critical serwce. Whech of the folowing BEST explans a reek of this prachce?

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

Answer: B

NEW QUESTION 643
- (Exam Topic 5)
As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII
B. TLP
C. TTP
D. STIX

Answer: C

NEW QUESTION 647
- (Exam Topic 5)
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD

Answer: AD

NEW QUESTION 651
- (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 653
- (Exam Topic 5)
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.
C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution

Answer: BC

NEW QUESTION 655

- (Exam Topic 5)
it a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?

A. Pertect forward secrecy
B. Eiliptic-curve cryptography
C. Key stretching
D. Homomorphic encryption

Answer: B

NEW QUESTION 658
- (Exam Topic 5)
An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

A. SIEM
B. SOAR
C. EDR
D. CASB

Answer: B

NEW QUESTION 663
- (Exam Topic 5)
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alert

Answer: A

NEW QUESTION 667
- (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 certificate key
B. DNS hijackeng to reroute tratic
C. Brute force 1 tho access point
D. A SSL/TLS downgrade

Answer: D

NEW QUESTION 669
- (Exam Topic 5)
A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

A. inability to authenticate
B. Implied trust
C. Lack of computing power
D. Unavailable patch

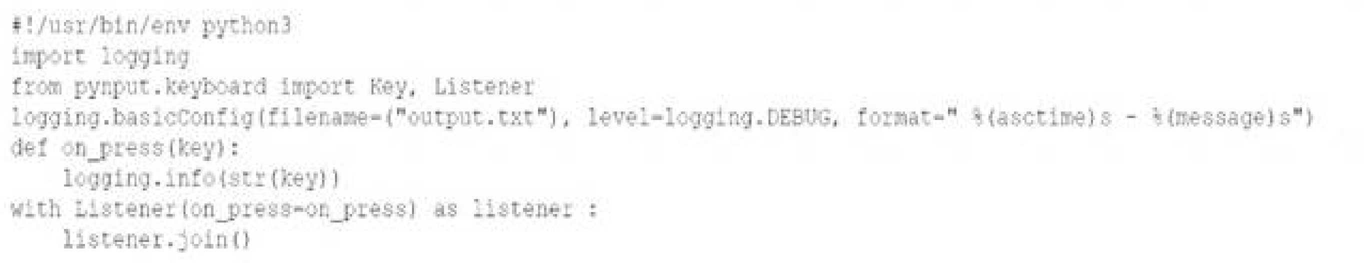
Answer: D

NEW QUESTION 671
- (Exam Topic 5)
A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

A. openssl
B. hping
C. netcat
D. tcpdump

Answer: A

NEW QUESTION 676
- (Exam Topic 6)
Given the following snippet of Python code:
Which of the following types of malware MOST likely contains this snippet?



```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename=("output.txt"), level=logging.DEBUG, format=" %(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener :
    listener.join()
```

A. Logic bomb
B. Keylogger
C. Backdoor
D. Ransomware

Answer: B

NEW QUESTION 677
- (Exam Topic 6)
A security administrator Is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

A. IPSec
B. SFTP
C. SRTP
D. LDAPS
E. S/MIME
F. SSL VPN

Answer: AF

Explanation:
IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.
SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

NEW QUESTION 679
- (Exam Topic 6)
An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for the high number of findings?

A. The vulnerability scanner was not properly configured and generated a high number of false positives
B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.
D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

Answer: A

Explanation:
The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/

NEW QUESTION 684
- (Exam Topic 6)
A new security engineer has started hardening systems. One o(the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability lo 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 ssh
D. conf.
E. Network services are no longer running on the NAS

Answer: B

Explanation:
SSH is used to securely transfer files to the remote server and is required for SCP to work. Disabling SSH will prevent users from being able to use SCP to transfer files to the server. To enable SSH, the security engineer should modify the SSH configuration file (sshd.conf) and make sure that SSH is enabled. For more information on hardening systems and the security techniques that can be used, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 687
- (Exam Topic 6)

Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

A. Privileged access management
B. SSO
C. RADIUS
D. Attribute-based access control

Answer: A

NEW QUESTION 688
- (Exam Topic 6)
An attacker replaces a digitally signed document with another version that goes unnoticed Upon reviewing the document's contents the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue. Which of the following attacks was used?

A. Cryptomalware
B. Hash substitution
C. Collision
D. Phishing

Answer: B

Explanation:
This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

NEW QUESTION 693
- (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 696
- (Exam Topic 6)
A company would like to set up a secure way to transfer data between users via their mobile phones The company's top pnonty is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

A. Cellular
B. NFC
C. Wi-Fi
D. Bluetooth

Answer: B

Explanation:
NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

NEW QUESTION 700
......