CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
- (Exam Topic 1)
A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

A. laaS
B. PasS
C. MaaS
D. SaaS

Answer: D

NEW QUESTION 2
- (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 3
- (Exam Topic 1)
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

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

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

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

Answer: D

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

NEW QUESTION 5
- (Exam Topic 1)
Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is a benefit of including a risk management framework into an organization's security approach?

A. It defines expected service levels from participating supply chain partners to ensure system outages are remediated in a timely manner
B. It identifies specific vendor products that have been tested and approved for use in a secure environment.
C. It provides legal assurances and remedies in the event a data breach occurs
D. It incorporates control, development, policy, and management activities into IT operations.

Answer: D

NEW QUESTION 7

- (Exam Topic 1)
Business partners are working on a secunty mechanism lo validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign encrypt, and decrypt transaction files. Which of the following is the BEST solution to adopt?

A. PKI
B. Blockchain
C. SAML
D. OAuth

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
During an incident response, an analyst applied rules to all inbound traffic on the border firewall and implemented ACLs on each critical server Following an investigation, the company realizes it is still vulnerable because outbound traffic is not restricted and the adversary is able lo maintain a presence in the network. In which of the following stages of the Cyber Kill Chain is the adversary currently operating?

A. Reconnaissance
B. Command and control
C. Actions on objective
D. Exploitation

Answer: B

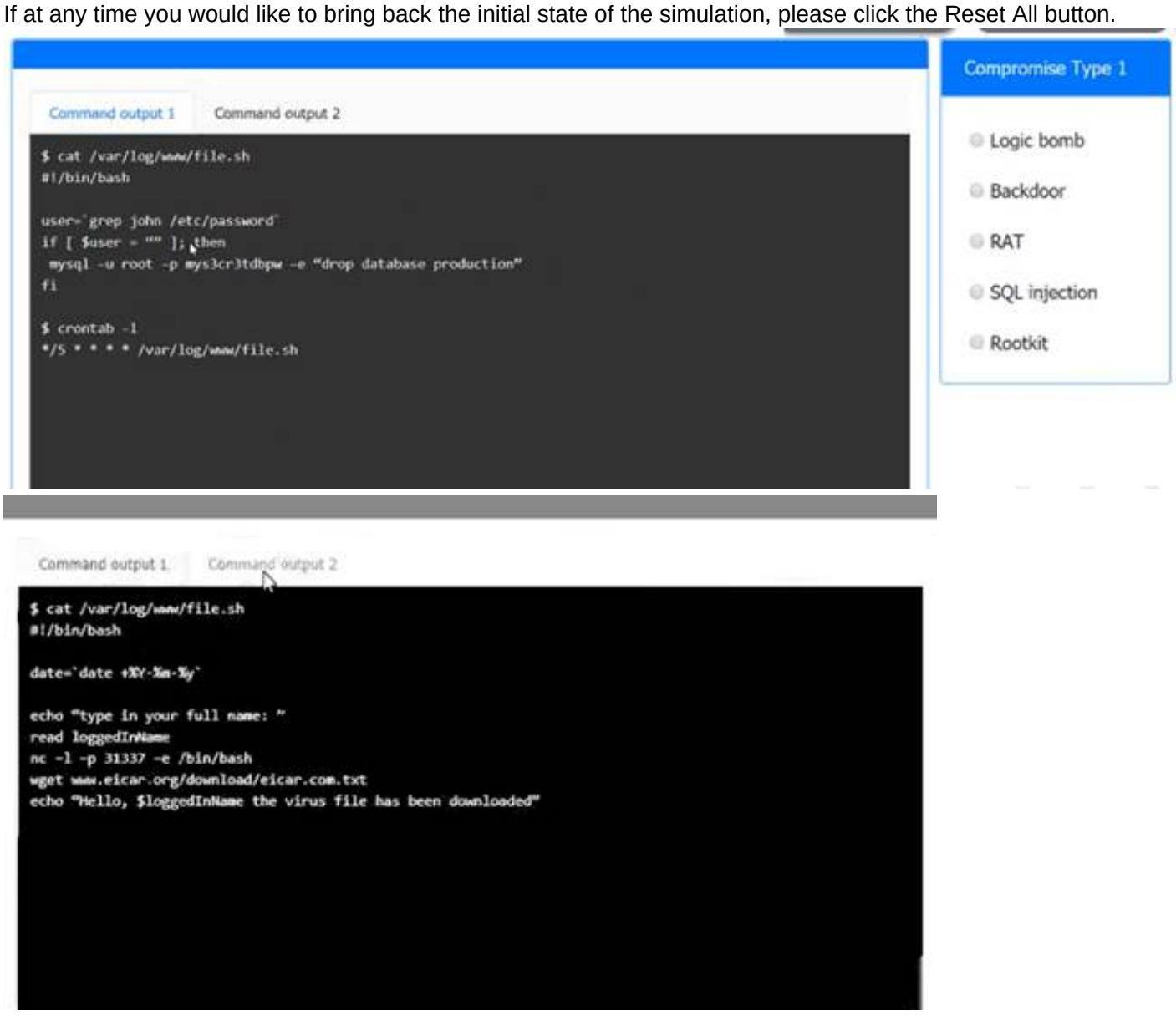
NEW QUESTION 9
- (Exam Topic 1)
Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

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

Answer: A

Explanation:
CVSS is maintained by the Forum of Incident Response and Security Teams (first.org/cvss). CVSS metrics generate a score from 0 to 10 based on characteristics of the vulnerability, such as whether it can be triggered remotely or needs local access, whether user intervention is required, and so on

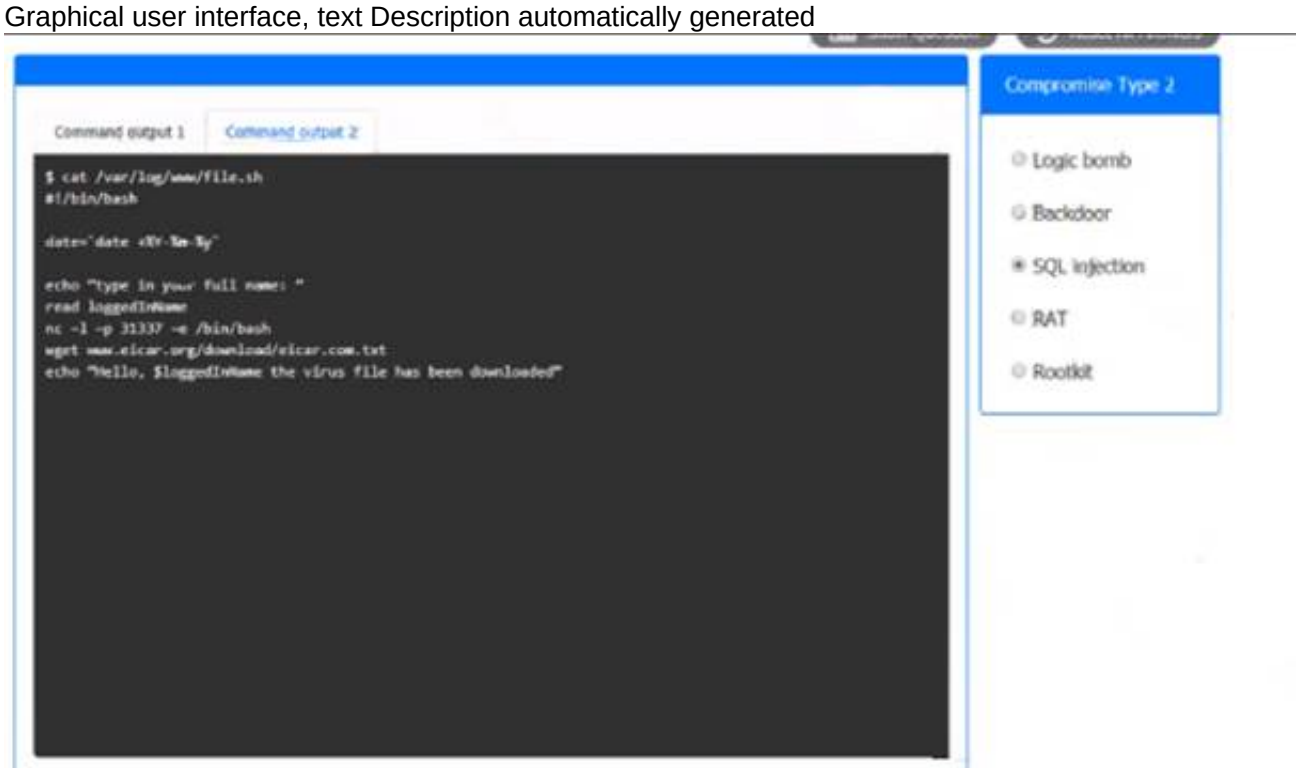
NEW QUESTION 10
- (Exam Topic 1)
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

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



NEW QUESTION 10
- (Exam Topic 1)
Security analysts are conducting an investigation of an attack that occurred inside the organization's network. An attacker was able to connect network traffic between workstation throughout the network. The analysts review the following logs:

VLAN	Address
1	0007.1e5d.3213
1	002a.7d.44.8801
1	0011.aab4.344d

The layer 2 address table has hundred of entries similar to the ones above. Which of the following attacks has MOST likely occurred?

A. SQL injection
B. DNS spoofing
C. MAC flooding
D. ARP poisoning

Answer: D

NEW QUESTION 11
- (Exam Topic 1)
A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Answer: A

NEW QUESTION 13
- (Exam Topic 1)
A security administrator is analyzing the corporate wireless network The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports Which of the following attacks in happening on the corporate network?

A. Man in the middle
B. Evil twin
C. Jamming
D. Rogue access point
E. Disassociation

Answer: B

NEW QUESTION 16
- (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 17
- (Exam Topic 1)
A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement Which of the following tools if available on the server, will provide the MOST useful information for the next assessment step?

A. Autopsy
B. Cuckoo
C. Memdump
D. Nmap

Answer: D

Explanation:
Nmap is basically mapping a network. The purpose of lateral pivoting is to gain a new perspective, or new information that will allow you to either privilege escalate, or to achieve the goal of the attack. If the compromised server the pen tester is exploiting has nmap enabled, the pen tester will be able to get an in-depth inside view of the internal network structure.

NEW QUESTION 19
- (Exam Topic 1)
Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

A. Shut down the VDI and copy off the event logs.
B. Take a memory snapshot of the running system.
C. Use NetFlow to identify command-and-control IPs.
D. Run a full on-demand scan of the root volume.

Answer: B

NEW QUESTION 23
- (Exam Topic 1)
Which of the following are common VoIP-associated vulnerabilities? (Select TWO).

A. SPIM
B. vishing
C. Hopping
D. Phishing
E. Credential harvesting
F. Tailgating

Answer: AB

NEW QUESTION 26
- (Exam Topic 1)
A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations Every day each location expenences very bnef outages that last for a few seconds However dunng the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an jndustnal smelter. Which of the following is the BEST solution to reduce the risk of data loss?

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

Answer: B

NEW QUESTION 28
- (Exam Topic 1)
Which of the following is assured when a user signs an email using a private key?

A. Non-repudiation

B. Confidentiality
C. Availably
D. Authentication

Answer: A

Explanation:
Non Repudiation is your virtual John Hancock. It's a way of virtually stamping any data or document with "I am who I say I am". Only way to break this would be if the private key owners' private key became compromised. Which at that point you got bigger problems than Non Repudiation.

NEW QUESTION 29
- (Exam Topic 1)
An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

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

Answer: A

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

NEW QUESTION 34
- (Exam Topic 1)
Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

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

Answer: A

NEW QUESTION 39
- (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 41
- (Exam Topic 1)
The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?

A. Preventing any current employees' siblings from working at the bank to prevent nepotism
B. Hiring an employee who has been convicted of theft to adhere to industry compliance
C. Filtenng applicants who have added false information to resumes so they appear better qualified
D. Ensuring no new hires have worked at other banks that may be trying to steal customer information

Answer: B

NEW QUESTION 43
- (Exam Topic 1)
An organization has hired a ted team to simulate attacks on its security posture Which of the following will the blue team do after detecting an loC?

A. Reimage the impacted workstations
B. Activate runbooks for incident response
C. Conduct forensics on the compromised system
D. Conduct passive reconnaissance to gather information

Answer: B

NEW QUESTION 46
- (Exam Topic 1)
Which of the following statements BEST describes zero-day exploits'?

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

Answer: C

NEW QUESTION 47
- (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 52
- (Exam Topic 1)
After a recent security incident, a security analyst discovered that unnecessary ports were open on a firewall policy for a web server. Which of the following firewall policies would be MOST secure for a web server?
A)

[Source	Destination	Port	Action]
Any	Any	TCP 53	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

B)

[Source	Destination	Port	Action]
Any	Any	TCP 53	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

C)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Deny
Any	Any	TCP 443	Allow
Any	Any	Any	Allow

D)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Deny

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

Answer: D

NEW QUESTION 54
- (Exam Topic 1)
A company is receiving emails with links to phishing sites that look very similar to the company's own website address and content. Which of the following is the BEST way for the company to mitigate this attack?

A. Create a honeynet to trap attackers who access the VPN with credentials obtained by phishing.
B. Generate a list of domains similar to the company's own and implement a DNS sinkhole for each.
C. Disable POP and IMAP on all Internet-facing email servers and implement SMTPS.
D. Use an automated tool to flood the phishing websites with fake usernames and passwords.

Answer: B

NEW QUESTION 58
- (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 60
- (Exam Topic 1)
Which of the following would be indicative of a hidden audio file found inside of a piece of source code?

A. Steganography
B. Homomotphic encryption
C. Cipher surte
D. Blockchain

Answer: A

Explanation:
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

NEW QUESTION 63
- (Exam Topic 1)
A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

A. DNS poisoning
B. MAC flooding
C. DDoS attack
D. ARP poisoning

Answer: C

NEW QUESTION 65
- (Exam Topic 1)
Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

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

Answer: C

Explanation:
Corrective controls are implemented after detective controls to rectify the problem and (ideally) prevent it from happening again.

NEW QUESTION 70
- (Exam Topic 1)
A company needs to validate its updated incident response plan using a real-world scenario that will test decision points and relevant incident response actions without interrupting daily operations. Which of the following would BEST meet the company's requirements?

A. Red-team exercise
B. Capture-the-flag exercise
C. Tabletop exercise
D. Phishing exercise

Answer: C

NEW QUESTION 75
- (Exam Topic 1)
A company is implementing a DLP solution on the file server. The file server has Pll. financial information, and health information stored on it Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data Which of the following should the company do to help accomplish this goal?

A. Classify the data
B. Mask the data
C. Assign an application owner
D. Perform a risk analysis

Answer: A

NEW QUESTION 76
- (Exam Topic 1)
A junior security analyst iss conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple logtn entnes with the following text:

```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time

suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py

suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh

suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```

Which of Ihe following is the MOST likely attack conducted on the environment?

A. Malicious script
B. Privilege escalation
C. Doman hijacking
D. DNS poisoning

Answer: A

NEW QUESTION 79
- (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 83
- (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 87
- (Exam Topic 1)
The board of doctors at a company contracted with an insurance firm to limit the organization’s liability. Which of the following risk management practices does the BEST describe?

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

Answer: A

NEW QUESTION 91
- (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 92
- (Exam Topic 1)
An organization has developed an application that needs a patch to fix a critical vulnerability In which of the following environments should the patch be deployed

LAST?

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

Answer: A

NEW QUESTION 96
- (Exam Topic 1)
After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

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

Answer: A

NEW QUESTION 100
- (Exam Topic 1)
Which of the following terms describes a broad range of information that is sensitive to a specific organization?

A. Public
B. Top secret
C. Proprietary
D. Open-source

Answer: C

NEW QUESTION 103
- (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 104
- (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 105
- (Exam Topic 1) A
user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?

A. On-path
B. Domain hijacking
C. DNS poisoning
D. Evil twin

Answer: C

NEW QUESTION 107
- (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 112
- (Exam Topic 1)
A security analyst has been asked by the Chief Information Security Officer to
• develop a secure method of providing centralized management of infrastructure
• reduce the need to constantly replace aging end user machines
• provide a consistent user desktop expenence
Which of the following BEST meets these requirements?

A. BYOD
B. Mobile device management
C. VDI
D. Containers ation

Answer: C

NEW QUESTION 113
- (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 116
- (Exam Topic 1)
A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website The malicious actor posted an entry in an attempt to trick users into cltckmg the following:

```
https://www.c0mptia.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was MOST likely observed?

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

Answer: B

NEW QUESTION 120
- (Exam Topic 1)
An organization would like to give remote workers the ability to use applications hosted inside the corporate network Users will be allowed to use their personal computers or they will be provided organization assets Either way no data or applications will be installed locally on any user systems Which of the following mobile solutions would accomplish these goals?

A. VDI
B. MDM
C. COPE
D. UTM

Answer: A

Explanation:
MDM would require something to be installed. VDI, virtual desktop infrastructure, would allow employees to use run apps on the company network without installing locally.

NEW QUESTION 125
- (Exam Topic 1)
A recent security breach exploited software vulnerabilities in the firewall and within the network management solution. Which of the following will MOST likely be used to identify when the breach occurred through each device?

A. SIEM correlation dashboards
B. Firewall syslog event logs
C. Network management solution login audit logs
D. Bandwidth monitors and interface sensors

Answer: A

NEW QUESTION 128
- (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 132
- (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 134
- (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 138
- (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 141
- (Exam Topic 1)
A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation which improves conditions, but performance degrades again after a few days. The administrator runs an anarysis tool and sees the following output:

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

The administrator terminates the timeAttend.exe observes system performance over the next few days, and notices that the system performance does not degrade Which of the following issues is MOST likely occurring?

A. DLL injection
B. API attack
C. Buffer oveiflow
D. Memory leak

Answer: C

NEW QUESTION 145
- (Exam Topic 1)
An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

A. FRR
B. Difficulty of use
C. Cost
D. FAR
E. CER

Answer: A

NEW QUESTION 148
- (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 151
- (Exam Topic 1)
Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?

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

Answer: A

NEW QUESTION 153
- (Exam Topic 1)
An organization has activated an incident response plan due to a malware outbreak on its network The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code Which of the following actions would be BEST to prevent reinfection from the initial infection vector?

A. Prevent connections over TFTP from the internal network
B. Create a firewall rule that blocks port 22 from the internet to the server
C. Disable file shanng over port 445 to the server
D. Block port 3389 inbound from untrusted networks

Answer: A

NEW QUESTION 154
- (Exam Topic 1)
A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

A. SQL injection and improper input-handling attempts
B. Cross-site scripting and resource exhaustion attempts
C. Command injection and directory traversal attempts
D. Error handling and privilege escalation attempts

Answer: C

NEW QUESTION 158
- (Exam Topic 1)
A security analyst wants to fingerpnnt a web server Which of the following tools will the security analyst MOST likely use to accomplish this task?

A. nmap -p1-65S35 192.168.0.10
B. dig 192.168.0.10

C. cur1 --htad http://192.168.0.10
D. ping 192.168.0.10

Answer: C

Explanation:
HTTP/1.1 301 Moved Permanently Server: cloudflare
Date: Thu, 01 Sep 2022 22:36:50 GMT
Content-Type: text/html Content-Length: 167 Connection: keep-alive Location: https://1.1.1.1/
CF-RAY: 74417cb04d6b9a50-MFE

NEW QUESTION 160
- (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 164
- (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 167
- (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 169
- (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 172
- (Exam Topic 2)
An attacker browses a company’s online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?

A. Hoax
B. Reconnaissance
C. Impersonation
D. pretexting

Answer: A

NEW QUESTION 177
- (Exam Topic 2)
A security analyst is reviewing application logs to determine the source of a breach and locates the following log:

```
https://www.comptia.com/login.php?id='%20or%20'1'1='1
```

Which Of the following has been observed?

A. DLL Injection
B. API attack
C. SQLI
D. XSS

Answer: C

NEW QUESTION 180
- (Exam Topic 2)
A company recently experienced an inside attack using a corporate machine that resulted in data compromise. Analysis indicated an unauthorized change to the software circumvented technological protection measures, The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?

A. HIPS
B. Flm
C. TPM
D. DLP

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation

NEW QUESTION 183
- (Exam Topic 2)
A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?

A. internet
B. Screened Subnet
C. VLAN segmentation
D. Zero Trust

Answer: C

NEW QUESTION 186
- (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 190
- (Exam Topic 2)
Which of the following should an organization consider implementing In the event executives need to speak to the media after a publicized data breach?

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

Answer: D

NEW QUESTION 191
- (Exam Topic 2)
Which of the following can be used by a monitoring tool to compare values and detect password leaks without providing the actual credentials?

A. Hashing
B. Tokenization
C. Masking
D. Encryption

Answer: A

Explanation:
https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/

NEW QUESTION 196
- (Exam Topic 2)
In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?

A. Authority
B. Intimidation
C. Consensus
D. Scarcity

Answer: B

NEW QUESTION 201
- (Exam Topic 2)
An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

```
Session              : hashcat
Status               : cracked
Hash.Type            : MD5
Hash.Target          : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started         : Fri Mar 10 10:18:45 2020
Recovered            : 1/1 (100%) Digests
Progress             : 28756845 / 450365879 (6.38%) hashes
Time.Stopped         : Fri Mar 10 10:20:12 2020
Password found       : Th3B3stP@55w0rd!
```

Which of the following BEST describes the type of password attack the attacker is performing?

A. Dictionary
B. Pass-the-hash
C. Brute-force
D. Password spraying

Answer: A

NEW QUESTION 203
- (Exam Topic 2)
Which of the following explains why RTO is included in a BIA?

A. It identifies the amount of allowable downtime for an application or system,
B. It prioritizes risks so the organization can allocate resources appropriately,
C. It monetizes the loss of an asset and determines a break-even point for risk mitigation.
D. It informs the backup approach so that the organization can recover data to a known time.

Answer: A

NEW QUESTION 208
- (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 212
- (Exam Topic 2)
Which of the following processes will eliminate data using a method that will allow the storage device to be reused after the process is complete?

A. Pulverizing

B. Overwriting
C. Shredding
D. Degaussing

Answer: D

Explanation:
https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/

NEW QUESTION 215
- (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 216
- (Exam Topic 2)
A security analyst is receiving several alerts per user and is trying to determine If various logins are malicious. The security analyst would like to create a baseline of normal operations and reduce noise. Which of the following actions should the security analyst perform?

A. Adjust the data flow from authentication sources to the SIEM.
B. Disable email alerting and review the SIEM directly.
C. Adjust the sensitivity levels of the SIEM correlation engine.
D. Utilize behavioral analysis to enable the SIEM's learning mode.

Answer: D

NEW QUESTION 221
- (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 224
- (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 228
- (Exam Topic 2)
Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?

A. Smart card
B. push notifications
C. Attestation service
D. HMAC-based, one-time password

Answer: B

NEW QUESTION 232
- (Exam Topic 2)
Which of the following is an example of risk avoidance?

A. Installing security updates directly in production to expedite vulnerability fixes
B. Buying insurance to prepare for financial loss associated with exploits

C. Not installing new software to prevent compatibility errors
D. Not taking preventive measures to stop the theft of equipment

Answer: C

NEW QUESTION 234
- (Exam Topic 2)
Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?

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

Answer: A

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

NEW QUESTION 239
- (Exam Topic 2)
An audit Identified Pll being utilized In the development environment of a critical application. The Chief Privacy Officer (CPO) Is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to BEST satisfy both the CPO's and the development team's requirements?

A. Data anonymlzallon
B. Data encryption
C. Data masking
D. Data tokenization

Answer: C

Explanation:
Data masking can mean that all or part of the contents of a field are redacted, by substituting all character strings with "x" for example. A field might be partially redacted to preserve metadata for analysis purposes. For example, in a telephone number, the dialing prefix might be retained, but the subscriber number redacted.
Data masking can also use techniques to preserve the original format of the field. Data masking is an irreversible deidentification technique

NEW QUESTION 243
- (Exam Topic 2)
An analyst receives multiple alerts for beaconing activity for a host on the network, After analyzing the activity, the analyst observes the following activity:
• A user enters comptia.org into a web browser.
• The website that appears is not the comptia.org site.
• The website is a malicious site from the attacker.
• Users in a different office are not having this issue. Which of the following types of attacks was observed?

A. On-path attack
B. DNS poisoning
C. Locator (URL) redirection
D. Domain hijacking

Answer: C

NEW QUESTION 246
- (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 248
- (Exam Topic 2)
Security analysts notice a server login from a user who has been on vacation for two weeks The analysts confirm that the user did not log in to the system while on vacation After reviewing packet capture logs, the analysts notice the following:

```
username: ....smithJA.....
Password: 944d3697d8880ed401b5ba2c77811
```

Which of the following occurred?

A. A buffer overflow was exploited to gain unauthorized access
B. The user's account was compromised, and an attacker changed the login credentials

C. An attacker used a pass-the-hash attack to gain access
D. An insider threat with username smithJA logged in to the account

Answer: B

NEW QUESTION 250
- (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 252
- (Exam Topic 2)
Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?

A. Version control
B. Continuous monitoring
C. Stored procedures
D. Automation

Answer: A

Explanation:
Version control, also known as source control, is the process of tracking and managing changes to files ov time. VCS — version control systems — are software tools designed to help teams work in parallel.
https://www.perforce.com/blog/vcs/what-is-version-control

NEW QUESTION 257
- (Exam Topic 2)
Which of the following is the BEST action to foster a consistent and auditable incident response process?

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

Answer: B

NEW QUESTION 261
- (Exam Topic 2)
After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest, Which of the following compliance frameworks would address the compliance team's GREATEST concern?

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

Answer: A

NEW QUESTION 265
- (Exam Topic 2)
Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

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

Answer: C

NEW QUESTION 266
- (Exam Topic 2)
A Chief Information Security Officer wants to ensure the organization is validating and checking the Integrity of zone transfers. Which of the following solutions should be implemented?

A. DNSSEC
B. LOAPS
C. NGFW
D. DLP

Answer: D

NEW QUESTION 267
- (Exam Topic 2)
An organization just implemented a new security system. Local laws state that citizens must be notified prior to encountering the detection mechanism to deter malicious activities. Which of the following is being implemented?

A. Proximity cards with guards
B. Fence with electricity
C. Drones with alarms
D. Motion sensors with signage

Answer: D

NEW QUESTION 268
- (Exam Topic 2)
A company discovered that terabytes of data have been exfiltrated over the past year after an employee clicked on an email link. The threat continued to evolve and remain undetected until a security analyst noticed an abnormal amount of external connections when the employee was not working. Which of the following is the MOST likely threat actor?

A. Shadow IT
B. Script kiddies
C. APT
D. Insider threat

Answer: C

Explanation:
An APT attack is characterized by using toolkits to achieve a presence on a target network and then, instead of just moving to steal information, focusing on the long game by maintaining a persistent presence on the target network. The tactics, tools, and procedures of APTs are focused on maintaining administrative access to the target network and avoiding detection. Then, over the long haul, the attacker can remove intellectual property and more from the organization, typically undetected.

NEW QUESTION 270
- (Exam Topic 2)
A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?

A. Outdated software
B. Weak credentials
C. Lack of encryption
D. Backdoors

Answer: B

NEW QUESTION 275
- (Exam Topic 2)
A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?

A. SSL
B. FTP
C. SNMP
D. TLS

Answer: D

NEW QUESTION 277
- (Exam Topic 2)
A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?

A. Reverse proxy
B. Automated patch management
C. Snapshots
D. NIC teaming

Answer: A

Explanation:
A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

NEW QUESTION 279
- (Exam Topic 2)
A security analyst has identified malware spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

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

Answer: B

NEW QUESTION 282
- (Exam Topic 2)
During a security incident investigation, an analyst consults the company's SIEM and sees an event concerning high traffic to a known, malicious command-and-control server. The analyst would like to determine the number of company workstations that may be impacted by this issue. Which of the following can provide the information?

A. WAF logs
B. DNS logs
C. System logs
D. Application logs

Answer: B

NEW QUESTION 283
- (Exam Topic 2)
A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following solutions BEST fits this use case?

A. EDR
B. DLP
C. NGFW
D. HIPS

Answer: A

Explanation:
The acronym EDR stands for Endpoint Detection and Response and is also known as EDTR. It is an endpoint security solution that is responsible for continuous monitoring of endpoints. This permanent monitoring enables the technology to detect and respond to cyber threats such as malware or ransomware at an early stage. The basis for this is always the analysis of context-related information, which can be used to make corrective proposals for recovery.

NEW QUESTION 284
- (Exam Topic 2)
Which of the following is the FIRST environment in which proper, secure coding should be practiced?

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

Answer: B

Explanation:
The developer has to start writing secure code from beginning itself. Which will then be tested, staged and finally production

NEW QUESTION 289
- (Exam Topic 2)
Which of the following control types fixes a previously identified issue and mitigates a risk?

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

Answer: B

NEW QUESTION 291
- (Exam Topic 2)
A forensics investigator is examining a number of unauthorized payments the were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:
<a href-"https://www.company.com/payto.do?routing=00001111&accc=22223334&amount-250">Click here to unsubscribe
Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. CSRF
C. XSS
D. XSRF

Answer: D

NEW QUESTION 296
- (Exam Topic 3)
A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

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

Answer: EF

NEW QUESTION 299
- (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 304
- (Exam Topic 3)
A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

A. Monitoring large data transfer transactions in the firewall logs
B. Developing mandatory training to educate employees about the removable media policy
C. Implementing a group policy to block user access to system files
D. Blocking removable-media devices and write capabilities using a host-based security tool

Answer: D

NEW QUESTION 307
- (Exam Topic 3)
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: DE

NEW QUESTION 308
- (Exam Topic 3)
A security administrator checks the table of a network switch, which shows the following output: 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 312
- (Exam Topic 3)
A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

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

Answer: D

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

NEW QUESTION 317
- (Exam Topic 3)
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

Answer: C

NEW QUESTION 319
- (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 321
- (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 322
- (Exam Topic 3)
Which of the following is a difference between a DRP and a BCP?

A. A BCP keeps operations running during a disaster while a DRP does not.
B. A BCP prepares for any operational interruption while a DRP prepares for natural disasters.
C. BCP is a technical response to disasters while a DRP is operational.
D. A BCP is formally written and approved while a DRP is not.

Answer: C

NEW QUESTION 323
- (Exam Topic 3)
After a phishing scam for 9 user's credentals, the red team was able to craft a payload to deploy on @ server. The attack allowed the installaton of malicious software that intiates @ new remote session.
Which of the following types of attacks has occurred?

A. Privilege escalation
B. Session replay
C. Application programming interface

D. Directory traversal

Answer: A

NEW QUESTION 326
- (Exam Topic 3)
An organization is repairing the damage after an incident, Which of the following controls és being implemented?

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

Answer: C

NEW QUESTION 328
- (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 332
- (Exam Topic 3)
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

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

Answer: AD

NEW QUESTION 337
- (Exam Topic 3)
A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

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

Answer: A

NEW QUESTION 339
- (Exam Topic 3)
A company's Chief Information Security Officer (CISO) recently warned the security manager that the company’s Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

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

Answer: A

NEW QUESTION 343
- (Exam Topic 3)
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

A. A capture-the-flag competition
B. A phishing simulation
C. Physical security training
D. Baste awareness training

Answer: B

NEW QUESTION 348
- (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 350
- (Exam Topic 3)
A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

A. VPN
B. Drive encryption
C. Network firewall
D. File level encryption
E. USB blocker
F. MFA

Answer: BE

NEW QUESTION 351
- (Exam Topic 3)
Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the
baseline?

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

Answer: D

NEW QUESTION 355
- (Exam Topic 3)
Which of the following would an organizaton use to assign a value to risks based on probability of occurrence and impact?

A. Risk matrix
B. Risk register
C. Risk appetite
D. Risk mitgation plan

Answer: B

NEW QUESTION 359
- (Exam Topic 3)
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

A. A firewall
B. A device pin
C. A USB data blocker
D. Biometrics

Answer: C

Explanation:
https://www.promorx.com/blogs/blog/how-does-a-usb-data-blocker-work Connecting via the data port of your mobile device, the Data Blockers creates a barrier between your mobile device and the charging station. Your phone will draw power as usual, allowing you to use it normally and charge it at the same time, but this clever piece of equipment will prevent any data exchange.
“Malicious USB charging cables and plugs are also a widespread problem. As with card skimming, a device may be placed over a public charging port at airports and other transit locations. A USB data blocker can provide mitigation against these juice- jacking attacks by preventing any sort of data transfer when the smartphone or laptop is connected to a charge point ”

NEW QUESTION 360
- (Exam Topic 3)
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company’s data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer: C

NEW QUESTION 364
- (Exam Topic 3)
A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

A. iPSec
B. Always On
C. Split tunneling
D. L2TP

Answer: B

NEW QUESTION 369
- (Exam Topic 3)
A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications.
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each regio
D. limit their logon times, and alert on risky logins
E. Create a guest account for each regio
F. remember the last ten passwords, and block password reuse

Answer: C

Explanation:
https://www.crowdstrike.com/blog/service-accounts-performing-interactive-logins/

NEW QUESTION 374
- (Exam Topic 3)
A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

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

Answer: D

NEW QUESTION 378
- (Exam Topic 3)
A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner
D. A next-generation firewall

Answer: A

NEW QUESTION 381
- (Exam Topic 3)
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: AD

NEW QUESTION 383

- (Exam Topic 3)
After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

A. The public ledger
B. The NetFlow data
C. A checksum
D. The event log

Answer: A

Explanation:
https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/

NEW QUESTION 387
- (Exam Topic 3)
An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

A. Incident response
B. Communications
C. Disaster recovery
D. Data retention

Answer: C

NEW QUESTION 392
- (Exam Topic 3)
A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describes these systems?

A. DNS sinkholes
B. Hafieypots
C. Virtual machines
D. Neural networks

Answer: B

NEW QUESTION 397
- (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 400
- (Exam Topic 3)
A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

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

Answer: B

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

NEW QUESTION 401
- (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 404
- (Exam Topic 3)
An organization Chief information Security Officer a position that will be responsibles for implementing technical controls to protect data, include ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor

Answer: A

NEW QUESTION 408
- (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 410
- (Exam Topic 3)
he Chief Information Secunty Officer came across a news arbcle outining a mechan’sm thal allows certan OS passwords to be bypassed The security team was then tasked with determining which
method could be used to prevent data loss in the corporate environment in case an attacker bypasses authentication Which of the following will accomplish this objective?

A. FDE
B. Proper patch management protocols
C. TPM
D. Input validations

Answer: A

NEW QUESTION 413
- (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 415
- (Exam Topic 3)
A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

A. Directory traversal
B. SQL injection

C. API
D. Request forgery

Answer: D

NEW QUESTION 420
- (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 423
- (Exam Topic 3)
To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

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

Answer: D

NEW QUESTION 424
- (Exam Topic 3)
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company. information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

Answer: A

NEW QUESTION 426
- (Exam Topic 3)
A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following
RAID levels meets this requirements?

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

Answer: C

NEW QUESTION 430
- (Exam Topic 3)
Which of the following types of controls is a turnstile?

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

Answer: A

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

NEW QUESTION 434
- (Exam Topic 3)
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Answer: C

Explanation:
https://www.techtarget.com/searchsecurity/definition/salt

NEW QUESTION 438
- (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 441
- (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 444
- (Exam Topic 3)
A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an Item, the password for the wireless network is printed on the recent so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

A. WPA-EAP
B. WEP-TKIP
C. WPA-PSK
D. WPS-PIN

Answer: A

NEW QUESTION 446
- (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 449
- (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 450
- (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 455
- (Exam Topic 3)
The Chief information Securtty Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside cornpany. Additionally, the CISO would Ske this solution to provide the same protections even when a company laptop or mobile device ts away from # home office. Which of the following should the CISO choose?

A. CASB
B. Next-generation SWG
C. NGFW
D. Web-application firewall

Answer: A

NEW QUESTION 459
- (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 464
- (Exam Topic 3)
During an incident response, a security analyst observes the following log entry on the web server.

```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd  HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experience?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

Answer: D

NEW QUESTION 467
- (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 469
- (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 473
- (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 475
- (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

NEW QUESTION 476
- (Exam Topic 3)
After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company Which of the following risk management strategies is the manager adopting?

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

Answer: C

NEW QUESTION 479
- (Exam Topic 3)
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

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

Answer: A

NEW QUESTION 484
- (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 485
- (Exam Topic 3)
Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

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

Answer: C

NEW QUESTION 488
- (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 493
- (Exam Topic 3)
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the
presence of a rootkit in the future?

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

Answer: C

NEW QUESTION 494
- (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 499
- (Exam Topic 3)
An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has not received information about the internal architecture. Which of the following BEST represents the type of testing that will occur?

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

Answer: D

NEW QUESTION 503
- (Exam Topic 3)
A administrator needs to allow mobéle 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 practces for authentication and infrastructure security? (Select TWO)

A. Create a new network for the mobile devices and block the commurycaton to the intemal 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 intemal network.
E. Use the existing network and allow communscation to the internal network and servers
F. Use a new and updated RADIUS server to mamntain the best solution

Answer: BC

NEW QUESTION 505
- (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 510
- (Exam Topic 3)
An information security policy states that separation of duties is required for all highly sensitive database changes that involve customers' financial data. Which of the following will this be BEST to prevent?

A. Least privilege
B. An insider threat

C. Adata breach
D. A change control violation

Answer: B

NEW QUESTION 511
- (Exam Topic 3)
A security analyst reports a company policy volation ina case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized dowloads are occurring. The @nalyst also discovers a couple of WAP are using the same SSID, but they have non-siandard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS

Answer: A

NEW QUESTION 515
- (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 517
- (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 520
- (Exam Topic 3)
A user contacts the help desk to report the following:
Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
The user was able to access the Internet but had trouble accessing the department share until the next day. The user is now getting notifications from the bank about unauthorized transactions.
Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

Answer: A

NEW QUESTION 522
- (Exam Topic 3)
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming

E. Scheduled penetration testing
F. Network-attached storage

Answer: AB

Explanation:
https://searchdatacenter.techtarget.com/definition/resiliency

NEW QUESTION 527
- (Exam Topic 3)
A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

A. An external access point is engaging in an evil-twin attack.
B. The signal on the WAP needs to be increased in that section of the building.
C. The certificates have expired on the devices and need to be reinstalled.
D. The users in that section of the building are on a VLAN that is being blocked by the firewall

Answer: A

NEW QUESTION 531
- (Exam Topic 3)
A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch In a Faraday cage.
D. Install a cable lock on the switch

Answer: B

NEW QUESTION 533
- (Exam Topic 3)
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

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

Answer: A

NEW QUESTION 534
- (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 real data?

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

Answer: B

Explanation:
https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20 The main reason for applying masking to a data field is to protect data that is classified as personally
identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles
https://en.wikipedia.org/wiki/Data_masking

NEW QUESTION 539
- (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 540
- (Exam Topic 3)
A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files and can work in conjunction with proxies or UTM. Which of the following would BEST meet the CSO's requirements?

A. Fuzzing
B. Sandboxing
C. Static code analysis
D. Code review

Answer: B

NEW QUESTION 544
- (Exam Topic 3)
During an intemal penetration test, a security analyst identified a network device that had accepted cleartext authentication and was configured with a default credential. Which of the following recommendations should the security analyst make to secure this device?

A. Configure SNMPv1.
B. Configure SNMPv2c
C. Configure SNMPv3.
D. Configure the default community string.

Answer: D

NEW QUESTION 548
- (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 549
- (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 551
- (Exam Topic 3)
An application owner has requested access for an external application to upload data from the central internal website without providing credentials at any point. Which of the following authentication methods should be configured to allow this type of integration access?

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

Answer: B

NEW QUESTION 556
- (Exam Topic 3)
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

Answer: A

Explanation:

Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirementsthat help prevent fraud

NEW QUESTION 557
- (Exam Topic 3)
A manufacturer creates designs for very high security products that are required to be protected and controlled

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

Answer: B

NEW QUESTION 562
- (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 563
- (Exam Topic 3)
A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:
• The devices will be used internationally by staff who travel extensively.
• Occasional personal use is acceptable due to the travel requirements.
• Users must be able to install and configure sanctioned programs and productivity suites.
• The devices must be encrypted
• The devices must be capable of operating in low-bandwidth environments.
Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN
B. Implementing application whitelisting
C. Requiring web traffic to pass through the on-premises content filter
D. Setting the antivirus DAT update schedule to weekly

Answer: A

NEW QUESTION 566
- (Exam Topic 3)
Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:
• There must be visibility into how teams are using cloud-based services.
• The company must be able to identify when data related to payment cards is being sent to the cloud.
• Data must be available regardless of the end user's geographic location
• Administrators need a single pane-of-glass view into traffic and trends. Which of the following should the security analyst recommend?

A. Create firewall rules to restrict traffic to other cloud service providers.
B. Install a DLP solution to monitor data in transit.
C. Implement a CASB solution.
D. Configure a web-based content filter.

Answer: B

NEW QUESTION 571
- (Exam Topic 3)
A malicious actor recently penetration a company’s network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

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

Answer: C

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

NEW QUESTION 572
- (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 573
- (Exam Topic 3)
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Answer: B

NEW QUESTION 576
- (Exam Topic 3)
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

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

Answer: C

NEW QUESTION 578
- (Exam Topic 3)
A symmetric encryption algorithm Is BEST suited for:

A. key-exchange scalability.
B. protecting large amounts of data.
C. providing hashing capabilities,
D. implementing non-repudiation.

Answer: D

NEW QUESTION 581
- (Exam Topic 3)
A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

A. The examiner does not have administrative privileges to the system
B. The system must be taken offline before a snapshot can be created
C. Checksum mismatches are invalidating the disk image
D. The swap file needs to be unlocked before it can be accessed

Answer: A

NEW QUESTION 586
- (Exam Topic 3)
While checking logs, a security engineer notices a number of end users suddenly downloading files with the
.t ar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment

Answer: A

NEW QUESTION 588

- (Exam Topic 3)
A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

A. Hard token
B. Retina scan
C. SMS text
D. Keypad PIN

Answer: B

NEW QUESTION 592
- (Exam Topic 3)
A systems administrators considering diferent backup solitons forthe IT rkashuchre The company 5 looky fre sokton tha ofes the fastest recovery ime whie aso saving the most amount of storage used to maintain the backups Which of the following recovery solubons would be the BEST option to meet these requirements?

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

Answer: B

NEW QUESTION 593
- (Exam Topic 3)
A security analyst is hardening a network infrastructure. The analyst is given the following requirements:
* Preserve the use of public IP addresses assigned to equipment on the core router.
* Enable "in transport" encryption protection to the web server with the strongest ciphers.
Which of the following should the analyst implement to meet these requirements? (Select TWO).

A. Configure VLANs on the core router.
B. Configure NAT on the core router.
C. Configure BGP on the core router.
D. Enable AES encryption on the web server.
E. Enable 3DES encryption on the web server.
F. Enable TLSv2 encryption on the web server.

Answer: AE

NEW QUESTION 597
- (Exam Topic 3)
Administrators have allowed employees to access their company email from personal computers. However, the administrators are concerned that these computers are another attack Surface and can result in user accounts being breached by foreign actors. Which of the following actions would provide the MOST secure solution?

A. Enable an option in the administration center so accounts can be locked if they are accessed from different geographical areas.
B. Implement a 16-character minimum length and 30-day expiration password policy.
C. Set up a global mail rule to disallow the forwarding of any company email to email addresses outside the organization,
D. Enforce a policy that allows employees to be able to access their email only while they are connected to the Internet via VPN.

Answer: A

NEW QUESTION 602
- (Exam Topic 3)
The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Type squatting
D. Pharming

Answer: B

NEW QUESTION 606
- (Exam Topic 3)
A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, ''Special privileges assigned to new login.'' Several of these messages did not have a valid logon associated with the user before these privileges were assigned.
Which of the following attacks is MOST likely being detected?

A. Pass-the-hash
B. Buffer overflow
C. Cross-site scripting
D. Session replay

Answer: A

NEW QUESTION 610
- (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 613
- (Exam Topic 3)
A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:
* Protection from power outages
* Always-available connectivity In case of an outage
The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access.
B. Connect the business router to its own dedicated UPS.
C. Purchase services from a cloud provider for high availability
D. Replace the business's wired network with a wireless network

Answer: C

NEW QUESTION 617
- (Exam Topic 3)
Which of the following BEST helps to demonstrate integrity during a forensic investigation?

A. Event logs
B. Encryption
C. Hashing
D. Snapshots

Answer: C

NEW QUESTION 621
- (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 624
- (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 628
- (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 633
- (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 635
- (Exam Topic 3)
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-forcea

Answer: D

NEW QUESTION 638
- (Exam Topic 3)
A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

Answer: A

NEW QUESTION 639
- (Exam Topic 3)
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include: Check-in/checkout of credentials
The ability to use but not know the password Automated password changes
Logging of access to credentials
Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system
D. An OpenID Connect authentication system

Answer: D

NEW QUESTION 641
- (Exam Topic 3)
The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

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

Answer: A

NEW QUESTION 645
- (Exam Topic 3)
An organidation recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation, a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved. Which of the following attacks MOST likely explains the behavior?

A. Birthday
B. Rainbow table
C. Impersonation
D. Whaling

Answer: C

NEW QUESTION 650
- (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 652
- (Exam Topic 3)
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

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

Answer: D

NEW QUESTION 653
- (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 658
- (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

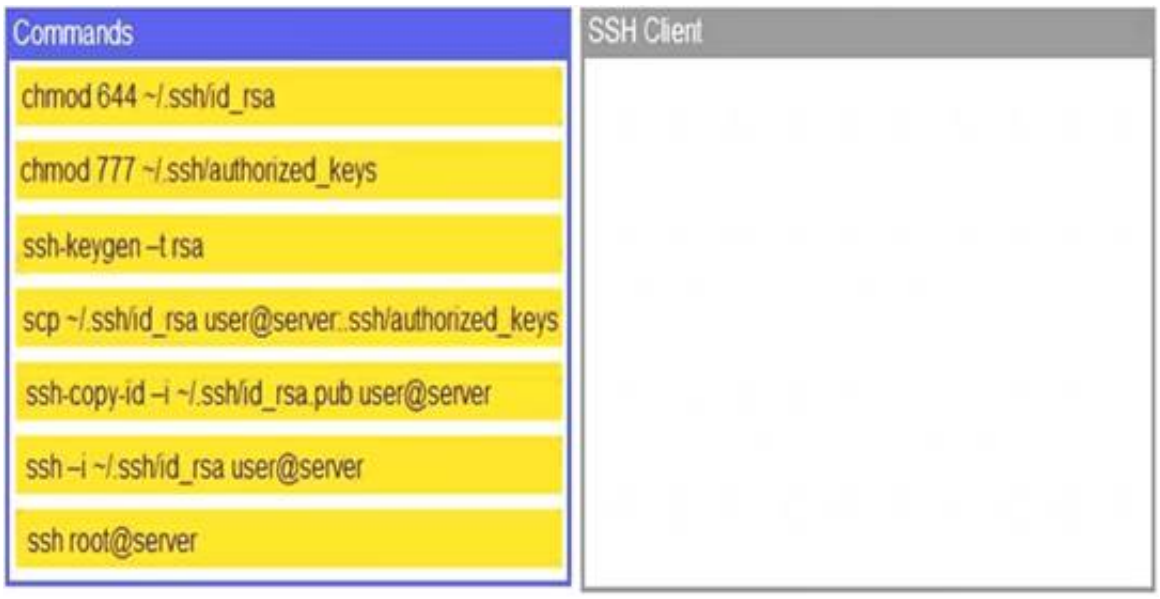
Answer: AB

NEW QUESTION 662
- (Exam Topic 3)
A web server has been compromised due to a ransomware attack. Further investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

A. The last incremental backup that was conducted 72 hours ago Most Voted
B. The last known-good configuration Most Voted
C. The last full backup that was conducted seven days ago
D. The baseline OS configuration

Answer: C

Explanation:
Ransomware will most likely render the web server unusable and must be isolated for forensic investigation. This will leave the only option to start a new web server from scratch and restore the last full backup, plus any differential or incremental backups which are sure to be clean from ransomware (if available).
DRAG DROP -A security engineer is setting up passwordless authentication for the first time.INSTRUCTIONS -Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Graphical user interface Description automatically generated



* 1. ssh-keygen -t rsa (creating the key-pair)
* 2. ssh-copy-id -i /.ssh/id_rsa.pub user@server (copy the public-key to user@server)
* 3. ssh -i ~/.ssh/id_rsa user@server (login to remote host with private-key)

NEW QUESTION 663
- (Exam Topic 3)
A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation, Which of the following would dispute the analyst's claim of innocence?

A. Legal hold
B. Order of volatility
C. Non-repudiation
D. Chain of custody

Answer: D

NEW QUESTION 668
- (Exam Topic 3)
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

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

Answer: B

NEW QUESTION 673
- (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 677
- (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 679
- (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 682
- (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 684
- (Exam Topic 3)
A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has Just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

A. Memory dumps
B. The syslog server
C. The application logs
D. The log retention policy

Answer: B

NEW QUESTION 686
- (Exam Topic 3)
An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

A. The theft of portable electronic devices
B. Geotagging in the metadata of images
C. Bluesnarfing of mobile devices
D. Data exfiltration over a mobile hot-spot

Answer: D

NEW QUESTION 691
- (Exam Topic 3)
A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

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

Answer: C

NEW QUESTION 695
- (Exam Topic 3)
A startup company is using multiple SaaS and IaaS platform 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

Explanation:
A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies
A CASB has a separate, and more distinctive role. Differing from the use case for SWG, which focuses on the broader filtering and protection against inbound threats and filtering illegitimate web traffic, a CASB is more deeply integrated and has control over your cloud application usage. It can be tied into an applications API to scan data at rest or can be used with a proxy based deployment to enforce inline policies for more real time protection.

NEW QUESTION 696
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SY0-601 Practice Exam Features:

* SY0-601 Questions and Answers Updated Frequently

* SY0-601 Practice Questions Verified by Expert Senior Certified Staff

* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year