



CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 1)

Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

- A. Reverse engineering
- B. Fuzzing
- C. Penetration testing
- D. Network mapping

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

- A. the public relations department
- B. senior leadership
- C. law enforcement
- D. the human resources department

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

Which of the following is the MOST important objective of a post-incident review?

- A. Capture lessons learned and improve incident response processes
- B. Develop a process for containment and continue improvement efforts
- C. Identify new technologies and strategies to remediate
- D. Identify a new management strategy

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

Answer: E

NEW QUESTION 5

- (Exam Topic 1)

A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

- A. Motion detection
- B. Perimeter fencing
- C. Monitored security cameras
- D. Badged entry

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

- A. Patching logs
- B. Threat feed
- C. Backup logs
- D. Change requests
- E. Data classification matrix

Answer: D

NEW QUESTION 7

- (Exam Topic 1)

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has

compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

- A. Post of the company blog
- B. Corporate-hosted encrypted email
- C. VoIP phone call
- D. Summary sent by certified mail
- E. Externally hosted instant message

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.

Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

- A. Development of a hypothesis as part of threat hunting
- B. Log correlation, monitoring, and automated reporting through a SIEM platform
- C. Continuous compliance monitoring using SCAP dashboards
- D. Quarterly vulnerability scanning using credentialed scans

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

An organization developed a comprehensive modern response policy Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

- A. A simulated breach scenario evolving the incident response team
- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

- A. 10.200.2.0/24 is infected with ransomware.
- B. 10.200.2.0/24 is not routable address space.
- C. 10.200.2.5 is a rogue endpoint.
- D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

- A. TPM
- B. eFuse
- C. FPGA
- D. HSM
- E. UEFI

Answer: D

NEW QUESTION 15

- (Exam Topic 1)

Which of the following are components of the intelligence cycle? (Select TWO.)

- A. Collection
- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

Answer: BE

NEW QUESTION 17

- (Exam Topic 1)

A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.

Which of the following data privacy standards does this violate?

- A. Purpose limitation
- B. Sovereignty
- C. Data minimization
- D. Retention

Answer: A

Explanation:

Reference:

<http://www.isitethical.eu/portfolio-item/purpose-limitation/>

NEW QUESTION 18

- (Exam Topic 1)

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

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

- A. 192.168.1.1
- B. 192.168.1.10
- C. 192.168.1.12
- D. 192.168.1.193

Answer: C

NEW QUESTION 19

- (Exam Topic 1)

During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.

Which of the following is the BEST place to acquire evidence to perform data carving?

- A. The system memory
- B. The hard drive
- C. Network packets
- D. The Windows Registry

Answer: A

Explanation:

Reference: <https://resources.infosecinstitute.com/memory-forensics/#gref> <https://www.computerhope.com/jargon/d/data-carving.htm>

NEW QUESTION 21

- (Exam Topic 1)

The help desk provided a security analyst with a screenshot of a user's desktop:

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

Answer: B

NEW QUESTION 23

- (Exam Topic 1)

A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

- A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
- B. Depending on system critically remove each affected device from the network by disabling wired and wireless connections
- C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addressesIdentify potentially affected systems by creating a correlation
- D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 24

- (Exam Topic 1)

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:

Which of the following should the analyst review to find out how the data was exfiltrated?

- A. Monday's logs
- B. Tuesday's logs
- C. Wednesday's logs
- D. Thursday's logs

Answer: D

NEW QUESTION 28

- (Exam Topic 1)

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

- A. Organizational policies
- B. Vendor requirements and contracts
- C. Service-level agreements
- D. Legal requirements

Answer: D

NEW QUESTION 30

- (Exam Topic 1)

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

- A. Write detection logic.
- B. Establish a hypothesis.
- C. Profile the threat actors and activities.
- D. Perform a process analysis.

Answer: C

Explanation:

Reference: <https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting>

NEW QUESTION 33

- (Exam Topic 1)

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

- A. Run `crontab -r; rm -rf /tmp/.t` to remove and disable the malware on the system.
- B. Examine the server logs for further indicators of compromise of a web application.
- C. Run `kill -9 1325` to bring the load average down so the server is usable again.
- D. Perform a binary analysis on the `/tmp/.t/t` file, as it is likely to be a rogue SSHD server.

Answer: B

NEW QUESTION 34

- (Exam Topic 1)

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

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

Answer: C

NEW QUESTION 37

- (Exam Topic 1)

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment. Which of the following is the BEST solution?

- A. Virtualize the system and decommission the physical machine.
- B. Remove it from the network and require air gapping.
- C. Only allow access to the system via a jumpbox.
- D. Implement MFA on the specific system.

Answer: A

NEW QUESTION 38

- (Exam Topic 1)

Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:

File access auditing is turned off.

When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.

All processes running appear to be legitimate processes for this user and machine.

Network traffic spikes when the space is cleared on the laptop.

No browser is open.

Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

- A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
- B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.
- C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
- D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer: B

NEW QUESTION 43

- (Exam Topic 1)

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

- A. Enumeration and OS fingerprinting
- B. Email harvesting and host scanning
- C. Social media profiling and phishing
- D. Network and host scanning

Answer: C

NEW QUESTION 44

- (Exam Topic 1)

While analyzing logs from a WAF, a cybersecurity analyst finds the following:

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

- A. This is an encrypted GET HTTP request
- B. A packet is being used to bypass the WAF
- C. This is an encrypted packet
- D. This is an encoded WAF bypass

Answer: D

NEW QUESTION 48

- (Exam Topic 1)

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Answer: A

NEW QUESTION 51

- (Exam Topic 1)

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware.

Which of the following is the MOST appropriate action to take in the situation?

- A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

Answer: C

NEW QUESTION 53

- (Exam Topic 1)

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

- A. Self-encrypting drive
- B. Bus encryption
- C. TPM
- D. HSM

Answer: A

NEW QUESTION 55

- (Exam Topic 1)

During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?

- A)
- B)
- C)
- D)
- E)

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: D

NEW QUESTION 60

- (Exam Topic 1)

Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

- A. Parameterized queries
- B. Session management
- C. Input validation
- D. Output encoding
- E. Data protection
- F. Authentication

Answer: AC

Explanation:

Reference: <https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/>

NEW QUESTION 61

- (Exam Topic 1)

Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

- A. Security regression testing
- B. Stress testing
- C. Static analysis testing
- D. Dynamic analysis testing
- E. User acceptance testing

Answer: B

NEW QUESTION 65

- (Exam Topic 1)

Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

- A. Data custodian

- B. Data owner
- C. Data processor
- D. Senior management

Answer: B

Explanation:

Reference: <https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3>

NEW QUESTION 67

- (Exam Topic 1)

During a cyber incident, which of the following is the BEST course of action?

- A. Switch to using a pre-approved, secure, third-party communication system.
- B. Keep the entire company informed to ensure transparency and integrity during the incident.
- C. Restrict customer communication until the severity of the breach is confirmed.
- D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Answer: D

NEW QUESTION 68

- (Exam Topic 1)

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use.

- A. an 802.11ac wireless bridge to create an air gap.
- B. a managed switch to segment the lab into a separate VLAN.
- C. a firewall to isolate the lab network from all other networks.
- D. an unmanaged switch to segment the environments from one another.

Answer: C

NEW QUESTION 72

- (Exam Topic 1)

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

Which of the following can the analyst conclude?

- A. Malware is attempting to beacon to 128.50.100.3.
- B. The system is running a DoS attack against ajgidwle.com.
- C. The system is scanning ajgidwle.com for PII.
- D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 75

- (Exam Topic 1)

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.

Which of the following is the MOST appropriate threat classification for these incidents?

- A. Known threat
- B. Zero day
- C. Unknown threat
- D. Advanced persistent threat

Answer: D

NEW QUESTION 80

- (Exam Topic 1)

A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Answer: A

NEW QUESTION 84

- (Exam Topic 1)

A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:

Based on the output, which of the following services should be further tested for vulnerabilities?

- A. SSH
- B. HTTP
- C. SMB
- D. HTTPS

Answer: A

NEW QUESTION 87

- (Exam Topic 1)

Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2.

Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

- A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
- B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
- C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
- D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

Answer: A

NEW QUESTION 92

- (Exam Topic 1)

Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

- A. It automatically performs remedial configuration changes to enterprise security services
- B. It enables standard checklist and vulnerability analysis expressions for automation
- C. It establishes a continuous integration environment for software development operations
- D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 97

- (Exam Topic 1)

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore it
- D. This is false positive, and the organization needs to focus its efforts on other findings.
- E. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

NEW QUESTION 101

- (Exam Topic 1)

An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.

Which of the following is MOST likely to be a false positive?

- A. OpenSSH/OpenSSL Package Random Number Generator Weakness
- B. Apache HTTP Server Byte Range DoS
- C. GDI+ Remote Code Execution Vulnerability (MS08-052)
- D. HTTP TRACE / TRACK Methods Allowed (002-1208)
- E. SSL Certificate Expiry

Answer: C

NEW QUESTION 102

- (Exam Topic 1)

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.

Which of the following is the BEST example of the level of sophistication this threat actor is using?

- A. Social media accounts attributed to the threat actor
- B. Custom malware attributed to the threat actor from prior attacks
- C. Email addresses and phone numbers tied to the threat actor
- D. Network assets used in previous attacks attributed to the threat actor
- E. IP addresses used by the threat actor for command and control

Answer: B

NEW QUESTION 106

- (Exam Topic 1)

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

- A. Critical asset list
- B. Threat vector
- C. Attack profile
- D. Hypothesis

Answer: D

NEW QUESTION 111

- (Exam Topic 1)

A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

- A. The parties have an MOU between them that could prevent shutting down the systems
- B. There is a potential disruption of the vendor-client relationship
- C. Patches for the vulnerabilities have not been fully tested by the software vendor
- D. There is an SLA with the client that allows very little downtime

Answer: D

NEW QUESTION 112

- (Exam Topic 1)

A security analyst is reviewing the following web server log:

Which of the following BEST describes the issue?

- A. Directory traversal exploit
- B. Cross-site scripting
- C. SQL injection
- D. Cross-site request forgery

Answer: A

NEW QUESTION 114

- (Exam Topic 1)

A security team wants to make SaaS solutions accessible from only the corporate campus Which of the following would BEST accomplish this goal?

- A. Geofencing
- B. IP restrictions
- C. Reverse proxy
- D. Single sign-on

Answer: A

Explanation:

Reference: <https://bluedot.io/library/what-is-geofencing/>

NEW QUESTION 119

- (Exam Topic 1)

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

- A. web servers on private networks
- B. HVAC control systems
- C. smartphones
- D. firewalls and UTM devices

Answer: B

NEW QUESTION 123

- (Exam Topic 1)

A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?

- A. Run an anti-malware scan on the system to detect and eradicate the current threat
- B. Start a network capture on the system to look into the DNS requests to validate command and control traffic.
- C. Shut down the system to prevent further degradation of the company network
- D. Reimage the machine to remove the threat completely and get back to a normal running state.
- E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

Answer: B

NEW QUESTION 127

- (Exam Topic 1)

A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

- A. Establish an alternate site with active replication to other regions
- B. Configure a duplicate environment in the same region and load balance between both instances
- C. Set up every cloud component with duplicated copies and auto scaling turned on
- D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

NEW QUESTION 131

- (Exam Topic 1)

A security analyst was alerted to a file integrity monitoring event based on a change to the vhost-payments.c on file. The output of the diff command against the known-good backup reads as follows

Which of the following MOST likely occurred?

- A. The file was altered to accept payments without charging the cards
- B. The file was altered to avoid logging credit card information
- C. The file was altered to verify the card numbers are valid.
- D. The file was altered to harvest credit card numbers

Answer: A

NEW QUESTION 136

- (Exam Topic 1)

A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached.

Which of the following risk actions has the security committee taken?

- A. Risk exception
- B. Risk avoidance
- C. Risk tolerance
- D. Risk acceptance

Answer: D

NEW QUESTION 139

- (Exam Topic 1)

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptiA.org. The testing is successful, and the security technician is prepared to fully implement the solution.

Which of the following actions should the technician take to accomplish this task?

- A. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the DNS record.
- B. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the email server.
- C. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the domain controller.
- D. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the web server.

Answer: A

Explanation:

Reference: <https://blog.finjan.com/email-spoofing/>

NEW QUESTION 140

- (Exam Topic 1)

A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

- A. Nikto
- B. Aircrack-ng
- C. Nessus
- D. tcpdump

Answer: B

NEW QUESTION 141

- (Exam Topic 1)

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

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

- A. strace /proc/1301
- B. rpm -V openash-server
- C. /bin/ls -l /proc/1301/exe
- D. kill -9 1301

Answer: A

NEW QUESTION 146

- (Exam Topic 1)

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.

Which of the following will remediate this software vulnerability?

- A. Enforce unique session IDs for the application.
- B. Deploy a WAF in front of the web application.
- C. Check for and enforce the proper domain for the redirect.
- D. Use a parameterized query to check the credentials.
- E. Implement email filtering with anti-phishing protection.

Answer: C

NEW QUESTION 149

- (Exam Topic 1)

A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

- A. Quarantine the web server
- B. Deploy virtual firewalls
- C. Capture a forensic image of the memory and disk
- D. Enable web server containerization

Answer: B

NEW QUESTION 154

- (Exam Topic 1)

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

The analyst runs the following command next:

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 156

- (Exam Topic 1)

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.

Which of the following should be considered FIRST prior to disposing of the electronic data?

- A. Sanitization policy
- B. Data sovereignty
- C. Encryption policy
- D. Retention standards

Answer: D

NEW QUESTION 160

- (Exam Topic 2)

A contained section of a building is unable to connect to the Internet A security analyst. A security analyst investigates me issue but does not see any connections to the corporate web proxy However the analyst does notice a small spike in traffic to the Internet. The help desk technician verifies all users are connected to the connect SSID. but there are two of the same SSIDs listed in the network connections. Which of the following BEST describes what is occurring?

- A. Bandwidth consumption
- B. Denial of service
- C. Beaconsing
- D. Rogue device on the network

Answer: A

NEW QUESTION 164

- (Exam Topic 2)

The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?

- A. A cloud access service broker system
- B. NAC to ensure minimum standards are met
- C. MFA on all workstations
- D. Network segmentation

Answer: D

NEW QUESTION 166

- (Exam Topic 2)

Which of the following threat classifications would MOST likely use polymorphic code?

- A. Known threat
- B. Zero-day threat
- C. Unknown threat
- D. Advanced persistent threat

Answer: D

NEW QUESTION 168

- (Exam Topic 2)

A company's senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?

- A. Mandatory-based
- B. Host-based
- C. Federated access
- D. Role-based

Answer: D

NEW QUESTION 169

- (Exam Topic 2)

A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

- A. Scrum
- B. IoC feeds
- C. ISAC
- D. VSS scores

Answer: C

NEW QUESTION 173

- (Exam Topic 2)

A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

- A. Use a DLP product to monitor the data sets for unauthorized edits and changes.
- B. Use encryption first and then hash the data at regular, defined times.
- C. Automate the use of a hashing algorithm after verified users make changes to their data
- D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Answer: D

NEW QUESTION 178

- (Exam Topic 2)

A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?

- A. Implement IPSec rules on the application servers through a GPO that limits RDP access from only the jump host
- B. Patch the jump host
- C. Since it does not run the application natively, it will not affect the software's operation and functionality
- D. Do not patch the application servers until the compatibility issue is resolved.
- E. Implement IPSec rules on the jump host server through a GPO that limits RDP access from only the other application server
- F. Do not patch the jump host
- G. Since it does not run the application natively, it is at less risk of being compromised
- H. Patch the application servers to secure them.
- I. Implement IPSec rules on the application servers through a GPO that limits RDP access to only other application server
- J. Do not patch the jump host
- K. Since it does not run the application natively, it is at less risk of being compromised
- L. Patch the application servers to secure them.
- M. Implement firewall rules on the application servers through a GPO that limits RDP access to only other application server
- N. Manually check the jump host to see if it has been compromised
- O. Patch the application servers to secure them.

Answer: A

NEW QUESTION 179

- (Exam Topic 2)

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

- A. verification of mitigation
- B. false positives
- C. false negatives
- D. the criticality index
- E. hardening validation.

Answer: A

NEW QUESTION 180

- (Exam Topic 2)

Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

- A. IP whitelisting
- B. Certificate-based authentication
- C. Virtual private network
- D. Web application firewall

Answer: A

NEW QUESTION 182

- (Exam Topic 2)

An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?

- A. Perform a vulnerability scan against a test instance.
- B. Download the product security white paper.
- C. Check industry news feeds for product reviews.
- D. Ensure a current non-disclosure agreement is on file

Answer: D

NEW QUESTION 184

- (Exam Topic 2)

An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors.

Which of the following would be the BEST recommendation for the security analyst to provide'?

- A. The organization should evaluate current NDAs to ensure enforceability of legal actions.
- B. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
- C. The organization should ensure all motherboards are equipped with a TPM.
- D. The organization should use a certified, trusted vendor as part of the supply chain.

Answer: D

NEW QUESTION 189

- (Exam Topic 2)

An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: "cat access.log.1 | grep "union". The output shown below appears:

```
<68.71.54.117> -- [31/Jan/2020:10:02:31 -0400] "Get
```

```
/cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1" Which of the following attacks has occurred on the server?
```

- A. Cross-site request forgery
- B. SQL injection
- C. Cross-site scripting
- D. Directory traversal

Answer: C

NEW QUESTION 193

- (Exam Topic 2)

Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night.

Which of the following actions should the analyst take NEXT?

- A. Initiate the incident response plan.
- B. Disable the privileged account
- C. Report the discrepancy to human resources.
- D. Review the activity with the user.

Answer: D

NEW QUESTION 197

- (Exam Topic 2)

Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?

- A. Information sharing and analysis membership
- B. Open-source intelligence, such as social media and blogs
- C. Real-time and automated firewall rules subscriptions
- D. Common vulnerability and exposure bulletins

Answer: A

NEW QUESTION 202

- (Exam Topic 2)

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

Which of the following MOST likely occurred?

- A. The attack used an algorithm to generate command and control information dynamically.
- B. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
- C. The attack caused an internal host to connect to a command and control server.
- D. The attack attempted to contact www.google.com to verify Internet connectivity.

Answer: C

NEW QUESTION 203

- (Exam Topic 2)

The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organization. Which of the following actions would work BEST to prevent against this type of attack?

- A. Turn on full behavioral analysis to avert an infection
- B. Implement an EDR mail module that will rewrite and analyze email links.
- C. Reconfigure the EDR solution to perform real-time scanning of all files
- D. Ensure EDR signatures are updated every day to avert infection.
- E. Modify the EDR solution to use heuristic analysis techniques for malware.

Answer: B

Explanation:

If you're concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over traditional antivirus.

NEW QUESTION 207

- (Exam Topic 2)

A security analyst needs to obtain the footprint of the network. The footprint must identify the following information;

- TCP and UDP services running on a targeted system
- Types of operating systems and versions
- Specific applications and versions

Which of the following tools should the analyst use to obtain the data?

- A. ZAP
- B. Nmap
- C. Prowler
- D. Reaver

Answer: B

NEW QUESTION 211

- (Exam Topic 2)

A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

- A. proprietary and timely
- B. proprietary and accurate
- C. relevant and deep
- D. relevant and accurate

Answer: D

NEW QUESTION 215

- (Exam Topic 2)

A security analyst reviews SIEM logs and detects a well-known malicious executable running in a Windows machine. The up-to-date antivirus cannot detect the malicious executable. Which of the following is the MOST likely cause of this issue?

- A. The malware is being executed with administrative privileges.
- B. The antivirus does not have the malware's signature.
- C. The malware detects and prevents its own execution in a virtual environment.
- D. The malware is fileless and exists only in physical memory.

Answer: A

NEW QUESTION 218

- (Exam Topic 2)

While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst's supervisor to use additional controls?

- A. FPGAs are vulnerable to malware installation and require additional protections for their codebase.
- B. FPGAs are expensive to produce
- C. Anti-counterfeiting safeguards are needed.
- D. FPGAs are expensive and can only be programmed once
- E. Code deployment safeguards are needed.
- F. FPGAs have an inflexible architecture
- G. Additional training for developers is needed

Answer: B

Explanation:

Ethernet switches are mass-produced and offered at discounts on not so widely-used chips with massive economies of scale. While in case of FPGAs, they are used as Ethernet switches and hence cost more since the expense of development and infrastructure are distributed among fewer clients.

NEW QUESTION 223

- (Exam Topic 2)

A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

- A. The server is receiving a secure connection using the new TLS 1.3 standard
- B. Someone has configured an unauthorized SMTP application over SSL
- C. The traffic is common static data that Windows servers send to Microsoft
- D. A connection from the database to the web front end is communicating on the port

Answer: B

NEW QUESTION 227

- (Exam Topic 2)

During an investigation, an analyst discovers the following rule in an executive's email client: IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>

The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

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

Answer: A

NEW QUESTION 231

- (Exam Topic 2)

A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons-learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?

- A. Enabling application blacklisting
- B. Enabling sandboxing technology
- C. Purchasing cyber insurance
- D. Installing a firewall between the workstations and Internet

Answer: B

NEW QUESTION 234

- (Exam Topic 2)

The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

- A. Whitelisting authorized IP addresses
- B. Enforcing more complex password requirements
- C. Blacklisting unauthorized IP addresses
- D. Establishing a sinkhole service

Answer: C

NEW QUESTION 235

- (Exam Topic 2)

A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level

authentication is enabled

Which of the following is the BEST remediation for this vulnerability?

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

- B. Verify the corresponding patch for the vulnerability is installed^
- C. Verify the system logs do not contain indicator of compromise.
- D. Verify the threat intelligence feed is updated with the latest solutions

Answer: A

NEW QUESTION 238

- (Exam Topic 2)

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

- A. Open Source Security Information Management (OSSIM)
- B. Software Assurance Maturity Model (SAMM)
- C. Open Web Application Security Project (OWASP)
- D. Spoofing, Tamperin
- E. Repudiation, Information disclosur
- F. Denial of service, Elevation of privileges (STRIDE)

Answer: C

NEW QUESTION 241

- (Exam Topic 2)

A security analyst needs to develop a brief that will include the latest incidents and the attack phases of the incidents. The goal is to support threat intelligence and identify whether or not the incidents are linked.

Which of the following methods would be MOST appropriate to use?

- A. An adversary capability model
- B. The MITRE ATT&CK framework
- C. The Cyber Kill Chain
- D. The Diamond Model of Intrusion Analysis

Answer: B

NEW QUESTION 242

- (Exam Topic 2)

An organization is experiencing issues with emails that are being sent to external recipients Incoming emails to the organization are working fine. A security analyst receives the following screenshot of email error from the help desk.

The analyst checks the email server and sees many of the following messages in the logs. Error 550 - Message rejected
Which of the following is MOST likely the issue?

- A. The DMARC queue is full
- B. SPF is failing.
- C. Port 25 is not open.
- D. The DKIM private key has expired

Answer: A

NEW QUESTION 247

- (Exam Topic 2)

A custom script currently monitors real-time logs of a SAML authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

- A. Logs may contain incorrect information.
- B. SAML logging is not supported for cloud-based authentication.
- C. Access to logs may be delayed for some time.
- D. Log data may be visible to other customers.

Answer: C

Explanation:

Threats & Vulnerabilities Associated with the Cloud, Subsection "Logging and Monitoring"

"Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse."

CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).

NEW QUESTION 249

- (Exam Topic 2)

An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

- A. tcpdump -X dst port 21
- B. ftp ftp.server -p 21
- C. nmap -o ftp.server -p 21
- D. telnet ftp.server 21

Answer: A

NEW QUESTION 253

- (Exam Topic 2)

The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network.

Which of the following would work BEST to prevent the issue?

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

Answer: A

NEW QUESTION 255

- (Exam Topic 2)

As part of an organization's information security governance process, a Chief Information Security Officer (CISO) is working with the compliance officer to update policies to include statements related to new regulatory and legal requirements. Which of the following should be done to BEST ensure all employees are appropriately aware of changes to the policies?

- A. Conduct a risk assessment based on the controls defined in the newly revised policies
- B. Require all employees to attend updated security awareness training and sign an acknowledgement
- C. Post the policies on the organization's intranet and provide copies of any revised policies to all active vendors
- D. Distribute revised copies of policies to employees and obtain a signed acknowledgement from them

Answer: B

NEW QUESTION 257

- (Exam Topic 2)

An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization's network and identify active hosts. An analyst sees the following output from a packet capture:

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

- A. flags=RA indicates the testing team is using a Christmas tree attack
- B. ttl=64 indicates the testing team is setting the time to live below the firewall's threshold
- C. 0 data bytes indicates the testing team is crafting empty ICMP packets
- D. NO FLAGS are set indicates the testing team is using hping

Answer: D

NEW QUESTION 262

- (Exam Topic 2)

The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

- A. Implement an IPS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
- B. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
- C. Implement an IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
- D. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability

Answer: A

NEW QUESTION 267

- (Exam Topic 2)

A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:

The analyst then compares the following results for port 22: nmap returns "Closed"

hping3 returns "flags=RA"

Which of the following BEST describes the firewall rule?

- A. DNAT --to-destination 1.1.1.1:3000
- B. REJECT with --tcp-reset
- C. LOG --log-tcp-sequence
- D. DROP

Answer: B

Explanation:

No doubt does the nmap result mean its being rejected as it returns closed. However, what threw me for a loop was the hping3 response. After further web surfing I found that the "flag=RA" means actually means "flag= RST, ACK" which means that it too was rejected.

NEW QUESTION 272

- (Exam Topic 2)

A security analyst has discovered malware is spreading across multiple critical systems and is originating from a single workstations, which belongs to a member of the cyber-infrastructure team who has legitimate administrator credentials. An analysis of the traffic indicates the workstation swept the networking looking for

vulnerable hosts to infect. Which of the following would have worked BEST to prevent the spread of this infection?

- A. Vulnerability scans of the network and proper patching.
- B. A properly configured and updated EDR solution.
- C. A honeypot used to catalog the anomalous behavior and update the IPS.
- D. Logical network segmentation and the use of jump boxes

Answer: D

NEW QUESTION 273

- (Exam Topic 2)

A company's data is still being exfiltrated to business competitors after the implementation of a DLP solution. Which of the following is the most likely reason why the data is still being compromised?

- A. Printed reports from the database contain sensitive information
- B. DRM must be implemented with the DLP solution
- C. Users are not labeling the appropriate data sets
- D. DLP solutions are only effective when they are implemented with disk encryption

Answer: B

NEW QUESTION 276

- (Exam Topic 2)

A company creates digitally signed packages for its devices. Which of the following BEST describes the method by which the security packages are delivered to the company's customers?

- A. Trusted firmware updates
- B. SELinux
- C. eFuse
- D. Anti-tamper mechanism

Answer: A

NEW QUESTION 280

- (Exam Topic 2)

An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?

- A. Use the MITRE ATT&CK framework to develop threat models.
- B. Conduct internal threat research and establish indicators of compromise.
- C. Review the perimeter firewall rules to ensure rule-set accuracy.
- D. Use SCAP scans to monitor for configuration changes on the network.

Answer: D

NEW QUESTION 285

- (Exam Topic 2)

An application server runs slowly and then triggers a high CPU alert. After investigating, a security analyst finds an unauthorized program is running on the server. The analyst reviews the application log below.

Which of the following conclusions is supported by the application log?

- A. An attacker was attempting to perform a buffer overflow attack to execute a payload in memory.
- B. An attacker was attempting to perform an XSS attack via a vulnerable third-party library.
- C. An attacker was attempting to download files via a remote command execution vulnerability
- D. An attacker was attempting to perform a DoS attack against the server.

Answer: C

Explanation:

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

NEW QUESTION 286

- (Exam Topic 2)

A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:

```
> dig domain._domainkey.comptia.org TXT
```

Which of the following email protection technologies is the analyst MOST likely validating?

- A. SPF
- B. DNSSEC
- C. DMARC
- D. DKIM

Answer: A

NEW QUESTION 287

- (Exam Topic 2)

Which of the following is a best practice when sending a file/data to another individual in an organization?

- A. Encrypt the file but do not compress it.
- B. When encrypting, split the file: and then compress each file.
- C. Compress and then encrypt the file.
- D. Encrypt and then compress the file.

Answer: C

NEW QUESTION 290

- (Exam Topic 2)

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

- A. Pyramid of Pain
- B. MITRE ATT&CK
- C. Diamond Model of Intrusion Analysts
- D. CVSS v3.0

Answer: B

NEW QUESTION 293

- (Exam Topic 2)

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

Which of the following is the MOST likely reason for this vulnerability?

- A. The developer set input validation protection on the specific field of search.aspx.
- B. The developer did not set proper cross-site scripting protections in the header.
- C. The developer did not implement default protections in the web application build.
- D. The developer did not set proper cross-site request forgery protections.

Answer: A

NEW QUESTION 297

- (Exam Topic 2)

A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

- A. Kill chain
- B. Diamond Model of Intrusion Analysis
- C. MITRE ATT&CK
- D. ITIL

Answer: C

NEW QUESTION 298

- (Exam Topic 3)

A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot be reused. Which of the following is the BEST approach?

- A. Degaussing
- B. Shredding
- C. Formatting
- D. Encrypting

Answer: B

Explanation:

<https://legalshred.com/degaussing-vs-hard-drive-shredding/>

The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding

NEW QUESTION 301

- (Exam Topic 3)

Due to a rise in cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally. Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

- A. Implement privileged access management
- B. Implement a risk management process
- C. Implement multifactor authentication
- D. Add more security resources to the environment

Answer: C

NEW QUESTION 306

- (Exam Topic 3)

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

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

Answer: EF

NEW QUESTION 311

- (Exam Topic 3)

An analyst is responding to an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the field. Malware was loaded on the device via the installation of a third-party software package. The analyst has baselined the device. Which of the following should the analyst do to BEST mitigate future attacks?

- A. Implement MDM
- B. Update the malware catalog
- C. Patch the mobile device's OS
- D. Block third-party applications

Answer: A

NEW QUESTION 312

- (Exam Topic 3)

Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

- A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from non-authorized access
- B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition
- C. Perform a disk sanitation using the command `dd if=/dev/zero of=/dev/zero bs=1M` over the media that will receive a copy of the collected data
- D. Execute the command `#dd if=/dev/ada of=/dev/adc bs=512` to clone the evidence data to external media to prevent any further change

Answer: B

NEW QUESTION 317

- (Exam Topic 3)

A vulnerability assessment solution is hosted in the cloud. This solution will be used as an accurate inventory data source for both the configuration management database and the governance, risk, and compliance tool. An analyst has been asked to automate the data acquisition. Which of the following would be the BEST way to acquire the data?

- A. CSV export
- B. SOAR
- C. API
- D. Machine learning

Answer: C

Explanation:

An example of API is Google Weather app, using the weather channel's API to collect accurate weather data and broadcast it on Google Weather app, so Google doesn't have to do it themselves.

NEW QUESTION 318

- (Exam Topic 3)

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

- A. Physical key
- B. Retinal scan
- C. Passphrase
- D. Fingerprint

Answer: D

NEW QUESTION 321

- (Exam Topic 3)

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

Which of the following is MOST likely happening?

- A. The hosts are part of a reflective denial-of-service attack.
- B. Information is leaking from the memory of host 10.20.30.40.
- C. Sensitive data is being exfiltrated by host 192.168.1.10.

D. Host 291.168.1.10 is performing firewall port knocking.

Answer: C

NEW QUESTION 322

- (Exam Topic 3)

A business recently acquired a software company. The software company's security posture is unknown. However, based on an assessment, there are limited security controls. No significant security monitoring exists. Which of the following is the NEXT step that should be completed to obtain information about the software company's security posture?

- A. Develop an asset inventory to determine the systems within the software company
- B. Review relevant network drawings, diagrams and documentation
- C. Perform penetration tests against the software company's Internal and external networks
- D. Baseline the software company's network to determine the ports and protocols in use.

Answer: A

NEW QUESTION 324

- (Exam Topic 3)

A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

- A. Implement UEM on an systems and deploy security software.
- B. Implement DLP on all workstations and block company data from being sent outside the company
- C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
- D. Implement centralized monitoring and logging for an company systems.

Answer: C

Explanation:

Cloud Access Security Broker (CASB): An enterprise management software designed to mediate access to cloud services by users across all types of devices

NEW QUESTION 328

- (Exam Topic 3)

An organization is developing software to match customers' expectations. Before the software goes into production, it must meet the following quality assurance guidelines

- Uncover all the software vulnerabilities.
- Safeguard the interest of the software's end users.
- Reduce the likelihood that a defective program will enter production.
- Preserve the Interests of me software producer Which of me following should be performed FIRST?

- A. Run source code against the latest OWASP vulnerabilities.
- B. Document the life-cycle changes that look place.
- C. Ensure verification and vacation took place during each phase.
- D. Store the source code in a s oftware escrow.
- E. Conduct a static analysis of the code.

Answer: A

NEW QUESTION 330

- (Exam Topic 3)

During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

- A. Set the web page to redirect to an application support page when a bad password is entered.
- B. Disable error messaging for authentication
- C. Recognize that error messaging does not provide confirmation of the correct element of authentication
- D. Avoid using password-based authentication for the application

Answer: C

NEW QUESTION 332

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 337

- (Exam Topic 3)

A company is experiencing a malware attack within its network. A security engineer notices many of the impacted assets are connecting outbound to a number of

remote destinations and exfiltrating data. The security engineer also see that deployed, up-to-date antivirus signatures are ineffective. Which of the following is the BEST approach to prevent any impact to the company from similar attacks in the future?

- A. IDS signatures
- B. Data loss prevention
- C. Port security
- D. Sinkholing

Answer: B

Explanation:

"Preventing data exfiltration is possible with security solutions that ensure data loss and leakage prevention. For example, firewalls can block unauthorized access to resources and systems storing sensitive information. On the other hand, a security information and event management system (SIEM) can secure data in motion, in use, and at rest, secure endpoints, and identify suspicious data transfers" <https://www.fortinet.com/resources/cyberglossary/data-exfiltration>

NEW QUESTION 340

- (Exam Topic 3)

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment. Which of the following is the BEST solution?

- A. virtualize the system and decommission the physical machine.
- B. Remove it from the network and require air gapping.
- C. Implement privileged access management for identity access.
- D. Implement MFA on the specific system.

Answer: B

NEW QUESTION 345

- (Exam Topic 3)

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

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

Answer: D

Explanation:

The CySA+ exam outline calls out "trusted firmware updates," but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features."

NEW QUESTION 347

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 351

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 352

- (Exam Topic 3)

A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations. Which of the following steps in the intelligence cycle is the security analyst performing?

- A. Analysis and production
- B. Processing and exploitation
- C. Dissemination and evaluation
- D. Data collection
- E. Planning and direction

Answer: A

Explanation:

Analysis is a human process that turns processed information into intelligence that can inform decisions. Depending on the circumstances, the decisions might involve whether to investigate a potential threat, what actions to take immediately to block an attack, how to strengthen security controls, or how much investment in additional security resources is justified. <https://www.recordedfuture.com/threat-intelligence-lifecycle-phases>

NEW QUESTION 353

- (Exam Topic 3)

A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

- A. DNSSEC
- B. DMARC
- C. STP
- D. S/IMAP

Answer: B

NEW QUESTION 356

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 357

- (Exam Topic 3)

A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

- A. Submit a change request to have the system patched
- B. Evaluate the risk and criticality to determine if further action is necessary
- C. Notify a manager of the breach and initiate emergency procedures.
- D. Remove the application from production and inform the users.

Answer: A

NEW QUESTION 359

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 362

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 365

- (Exam Topic 3)

Which of the following are considered PII by themselves? (Select TWO).

- A. Government ID
- B. Job title

- C. Employment start date
- D. Birth certificate
- E. Employer address
- F. Mother's maiden name

Answer: AD

NEW QUESTION 366

- (Exam Topic 3)

The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.

Which of the following BEST describes what the CIS wants to purchase?

- A. Asset tagging
- B. SIEM
- C. File integrity monitor
- D. DLP

Answer: D

NEW QUESTION 370

- (Exam Topic 3)

A company wants to configure the environment to allow passive network monitoring. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

- A. Port bridging
- B. Tunnel all mode
- C. Full-duplex mode
- D. Port mirroring
- E. Promiscuous mode

Answer: D

NEW QUESTION 375

- (Exam Topic 3)

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

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

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

Answer: B

NEW QUESTION 379

- (Exam Topic 3)

A team of network security analysts is examining network traffic to determine if sensitive data was exfiltrated. Upon further investigation, the analysts believe confidential data was compromised. Which of the following capabilities would BEST defend against this type of sensitive data exfiltration?

- A. Deploy an edge firewall.
- B. Implement DLP
- C. Deploy EDR.
- D. Encrypt the hard drives

Answer: C

NEW QUESTION 381

- (Exam Topic 3)

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

- A. Resetting the phone to factory settings
- B. Rebooting the phone and installing the latest security updates
- C. Documenting the respective chain of custody
- D. Uninstalling any potentially unwanted programs
- E. Performing a memory dump of the mobile device for analysis
- F. Unlocking the device by blowing the eFuse

Answer: AE

NEW QUESTION 385

- (Exam Topic 3)

A security analyst notices the following entry while reviewing the server logs:

OR 1=1' ADD USER attacker' PW 1337password' ---- Which of the following events occurred?

- A. CSRF
- B. XSS
- C. SQLi
- D. RCE

Answer: C

NEW QUESTION 386

- (Exam Topic 3)

A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code prior to pushing it to production?

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

Answer: B

NEW QUESTION 391

- (Exam Topic 3)

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

- A. Warn the incident response team that the server can be compromised
- B. Open a ticket informing the development team about the alerts
- C. Check if temporary files are being monitored
- D. Dismiss the alert, as the new application is still being adapted to the environment

Answer: A

NEW QUESTION 392

- (Exam Topic 3)

A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

- A. Make sure the scan is credentialed, covers all hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
- B. Make sure the scan is uncredentialed, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
- C. Make sure the scan is credentialed, has the latest software and signature versions, covers all external hosts in the patch management system and is scheduled during off-business hours so it has the least impact on operations.
- D. Make sure the scan is credentialed, uses a trusted plug-in set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

Answer: D

NEW QUESTION 395

- (Exam Topic 3)

A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

- A. output encoding.
- B. data protection.
- C. query parameterization.
- D. input validation.

Answer: D

NEW QUESTION 398

- (Exam Topic 3)

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

Which of the following describes what has occurred?

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

Answer: D

NEW QUESTION 402

- (Exam Topic 3)

While investigating reports or issues with a web server, a security analyst attempts to log in remotely and receives the following message:

The analyst accesses the server console, and the following console messages are displayed:

The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:

Which of the following is the BEST step for the analyst to take next in this situation?

- A. Load the network captures into a protocol analyzer to further investigate the communication with 128.30.100.23, as this may be a botnet command server
- B. After ensuring network captures from the server are saved isolate the server from the network take a memory snapshot, reboot and log in to do further analysis.
- C. Corporate data is being exfiltrated from the server Reboot the server and log in to see if it contains any sensitive data.
- D. Cryptomining malware is running on the server and utilizing an CPU and memory
- E. Reboot the server and disable any cron jobs or startup scripts that start the mining software.

Answer: A

NEW QUESTION 405

- (Exam Topic 3)

A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

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

Answer: C

Explanation:

A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.

NEW QUESTION 407

- (Exam Topic 3)

Which of the following is a reason to use a risk-based cybersecurity framework?

- A. A risk-based approach always requires quantifying each cyber risk faced by an organization
- B. A risk-based approach better allocates an organization's resources against cyberthreats and vulnerabilities
- C. A risk-based approach is driven by regulatory compliance and is required for most organizations
- D. A risk-based approach prioritizes vulnerability remediation by threat hunting and other qualitative-based processes

Answer: B

NEW QUESTION 410

- (Exam Topic 3)

A security analyst is running a tool against an executable of an unknown source. The input supplied by the tool to the executable program and the output from the executable are shown below:

Which of the following should the analyst report after viewing this information?

- A. A dynamic library that is needed by the executable is missing
- B. Input can be crafted to trigger an infection attack in the executable
- C. The tool caused a buffer overflow in the executable's memory
- D. The executable attempted to execute a malicious command

Answer: B

NEW QUESTION 412

- (Exam Topic 3)

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct business overseas must have their mobile devices checked for malicious software or evidence of tampering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief Information Security Officer wants to implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

- A. Implement a mobile device wiping solution for use if a device is lost or stolen.
- B. Install a DLP solution to track data now
- C. Install an encryption solution on all mobile devices.

D. Train employees to report a lost or stolen laptop to the security department immediately

Answer: A

NEW QUESTION 415

- (Exam Topic 3)

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

Which of the following ports should be closed?

- A. 22
- B. 80
- C. 443
- D. 1433

Answer: D

NEW QUESTION 418

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 421

- (Exam Topic 3)

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

- A. Create an IPS rule to block the subnet.
- B. Sinkhole the IP address.
- C. Create a firewall rule to block the IP address.
- D. Close all unnecessary open ports.

Answer: C

NEW QUESTION 423

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 425

- (Exam Topic 3)

A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

- A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.
- B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.
- C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to thecloud.
- D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

Answer: C

Explanation:

"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."
<https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solutio>

NEW QUESTION 428

- (Exam Topic 3)

A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?

- A. The DNS configuration
- B. Privileged accounts
- C. The IDS rule set
- D. The firewall ACL

Answer: C

NEW QUESTION 432

- (Exam Topic 3)

A security analyst reviews SIEM logs and discovers the following error event:

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

- A. Proxy server
- B. SQL server
- C. Windows domain controller
- D. WAF appliance
- E. DNS server

Answer: E

NEW QUESTION 433

- (Exam Topic 3)

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

- A. Smart cards
- B. Multifactor authentication
- C. Biometrics
- D. Increased password-rotation frequency

Answer: D

NEW QUESTION 435

- (Exam Topic 3)

The Chief information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue

- A. Induce digital signatures on messages originating within the company.
- B. Require users authenticate to the SMTP server
- C. Implement DKIM to perform authentication that will prevent this Issue.
- D. Set up an email analysis solution that looks for known malicious links within the email.

Answer: C

NEW QUESTION 437

- (Exam Topic 3)

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

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

- A. Review the known Apache vulnerabilities to determine if a compromise actually occurred
- B. Contact the application owner for connect example local tor additional information
- C. Mark the alert as a false positive scan coming from an approved source.
- D. Raise a request to the firewall team to block 203.0.113.15.

Answer: D

NEW QUESTION 438

.....

Relate Links

100% Pass Your CS0-003 Exam with ExamBible Prep Materials

<https://www.exambible.com/CS0-003-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>