CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Exam Topic 3)
A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:

```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.442: Flags [S], seq 1663238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr
0,nop,wscale 11], length 0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1663238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr
0,nop,wscale 11], length 0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val
719168538 ecr 3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length
0
16:06:32.910903 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [F.], seq 1, ack 2, win 64, options [nop,nop,TS val 719168538 ecr 3178342129], length
0
16:06:32.910908 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 2, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.911743 IP 192.168.0.1.56346 > 192.168.1.1.444: Flags [S], seq 862629258, win 65535, options [mss 65495,sackOK,TS val 3178342130 ecr
0,nop,wscale 11], length 0
16:06:32.911747 IP 192.168.1.1.444 > 192.168.0.1.56346: Flags [R.], seq 0, ack 862629259, win 0, length 0
16:06:32.912562 IP 192.168.0.1.52002 > 192.168.1.1.445: Flags [S], seq 1707382117, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
16:06:32.912566 IP 192.168.1.1.445 > 192.168.0.1.52002: Flags [R.], seq 0, ack 1707382118, win 0, length 0
16:06:32.913389 IP 192.168.0.1.59808 > 192.168.1.1.446: Flags [S], seq 2627951491, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
```

Which of the following generated the above output?

A. A port scan
B. A TLS connection
C. A vulnerability scan
D. A ping sweep

Answer: A

Explanation:
Port scan againts 442-446 ports. For port 443 the scanner closed the connection after SYN-ACK.

NEW QUESTION 2
- (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 3
- (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 4
- (Exam Topic 3)
According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?

A. Delete the vulnerable section of the code immediately.
B. Create a custom rule on the web application firewall.
C. Validate user input before execution and interpretation.
D. Use parameterized queries.

Answer: D

NEW QUESTION 5
- (Exam Topic 3)
The help desk is having difficulty keeping up with all onboarding and offboarding requests. Managers often submit, requests for new users at the last minute. causing the help desk to scramble to create accounts across many different Interconnected systems. Which of the following solutions would work BEST to assist

the help desk with the onboarding and offboarding process while protecting the company's assets?

A. MFA
B. CASB
C. SSO
D. RBAC

Answer: C

NEW QUESTION 6
- (Exam Topic 3)
An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by pubic users accessing the server. The results should be written to a text file and should induce the date. time, and IP address associated with any spreadsheet downloads. The web server's log file Is named webserver log, and the report We name should be accessreport.txt. Following is a sample of the web servefs.log file:
2017-0-12 21:01:12 GET /index.htlm - @4..102.33.7 - return=200 1622
Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

A. more webserver.log | grep * xls > accessreport.txt
B. more webserver.log > grep "xls > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E "return=200 | accessreport.txt
D. more webserver.log | grep -A *.xls < accessreport.txt

Answer: C

NEW QUESTION 7
- (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 8
- (Exam Topic 3)
After examining 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

NEW QUESTION 9
- (Exam Topic 3)
White reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with po mcai propaganda. Which of the following BEST Describes this type of actor?

A. Hacktivist
B. Nation-state
C. insider threat
D. Organized crime

Answer: A

NEW QUESTION 10
- (Exam Topic 3)
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

A. SCADA
B. CAN bus
C. Modbus
D. IoT

Answer: B

Explanation:
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

NEW QUESTION 10
- (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 11
- (Exam Topic 3)
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

A. Perform an assessment of the firmware to determine any malicious modifications.
B. Conduct a trade study to determine if the additional risk constitutes further action.
C. Coordinate a supply chain assessment to ensure hardware authenticity.
D. Work with IT to replace the devices with the known-altered motherboards.

Answer: D

NEW QUESTION 14
- (Exam Topic 3)
Which of following allows Secure Boot to be enabled?

A. eFuse
B. UEFI
C. MSM
D. PAM

Answer: C

NEW QUESTION 19
- (Exam Topic 3)
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

A. CI/CD
B. Software assurance
C. Anti-tamper
D. Change management

Answer: D

Explanation:
change management - process through which changes to the configuration of information systems are monitored and controlled. Each individual component should have a separate document or database record that describes its initial state and subsequent changes

NEW QUESTION 22
- (Exam Topic 3)
A secutily analyst is reviewing WAF alerts and sees the following request:

```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

Which of the following BEST describes the attack?

A. SQL injection
B. LDAP injection
C. Command iniection
D. Denial of service

Answer: A

NEW QUESTION 27
- (Exam Topic 3)
An organization has the following risk mitigation policies
• Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
• Other nsk mitigation will be pnontized based on risk value. The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

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

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

Answer: D

NEW QUESTION 29
- (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 32
- (Exam Topic 3)
A Chief Information Secunty Officer has asked for a list of hosts that have critical and high-seventy findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

A. Nessus
B. Nikto
C. Fuzzer
D. Wireshark
E. Prowler

Answer: A

NEW QUESTION 36
- (Exam Topic 3)
An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

A. Change the passwords on the devices.
B. Implement BIOS passwords.
C. Remove the assets from the production network for analysis.

D. Report the findings to the threat intel community.

Answer: C

Explanation:
If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.

NEW QUESTION 40
- (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 42
- (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 43
- (Exam Topic 3)
An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised Which of the following should Ihe analyst do FIRST?

A. Perform threat hunting in other areas of the cloud infrastructure
B. Contact law enforcement to report the incident
C. Perform a root cause analysis on the container and the service logs
D. Isolate the container from production using a predefined policy template

Answer: C

NEW QUESTION 48
- (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 50

- (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

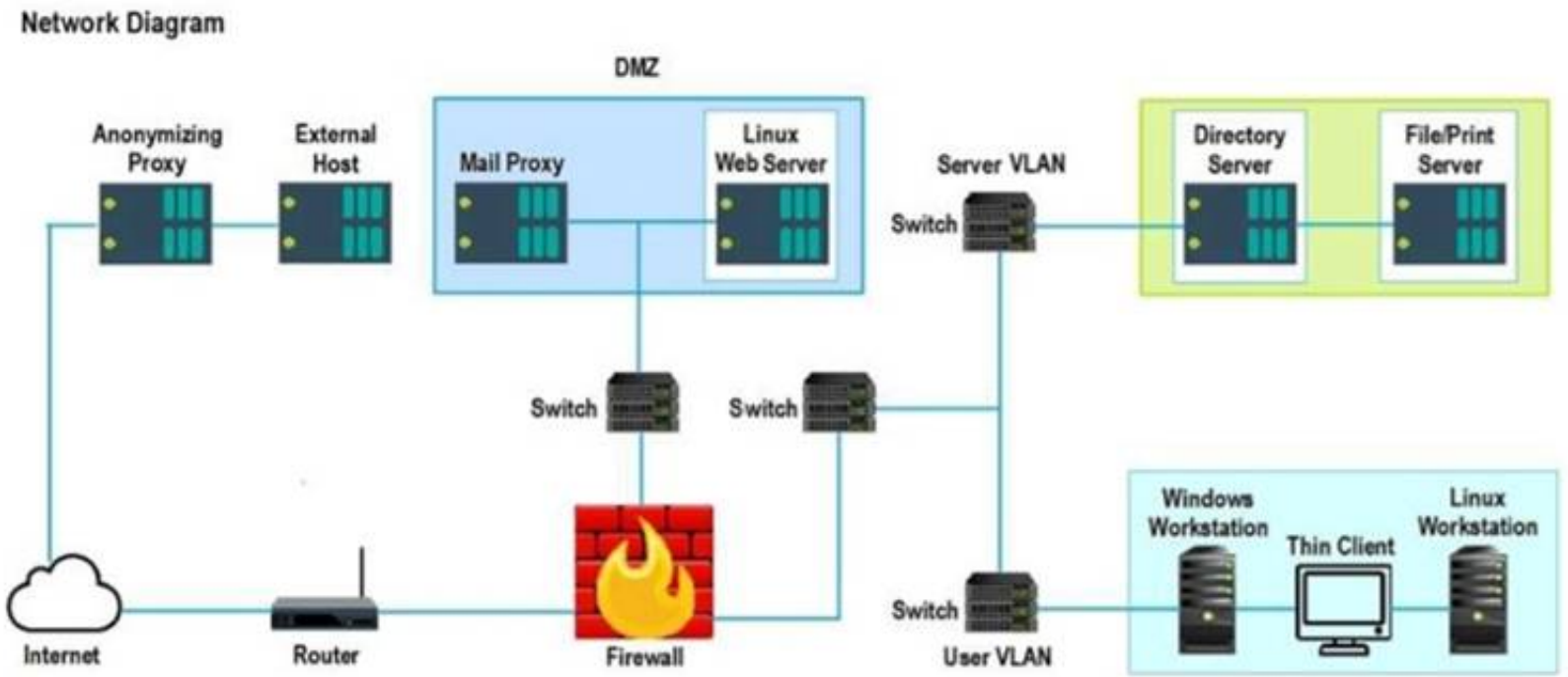
NEW QUESTION 55
- (Exam Topic 3)
Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

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

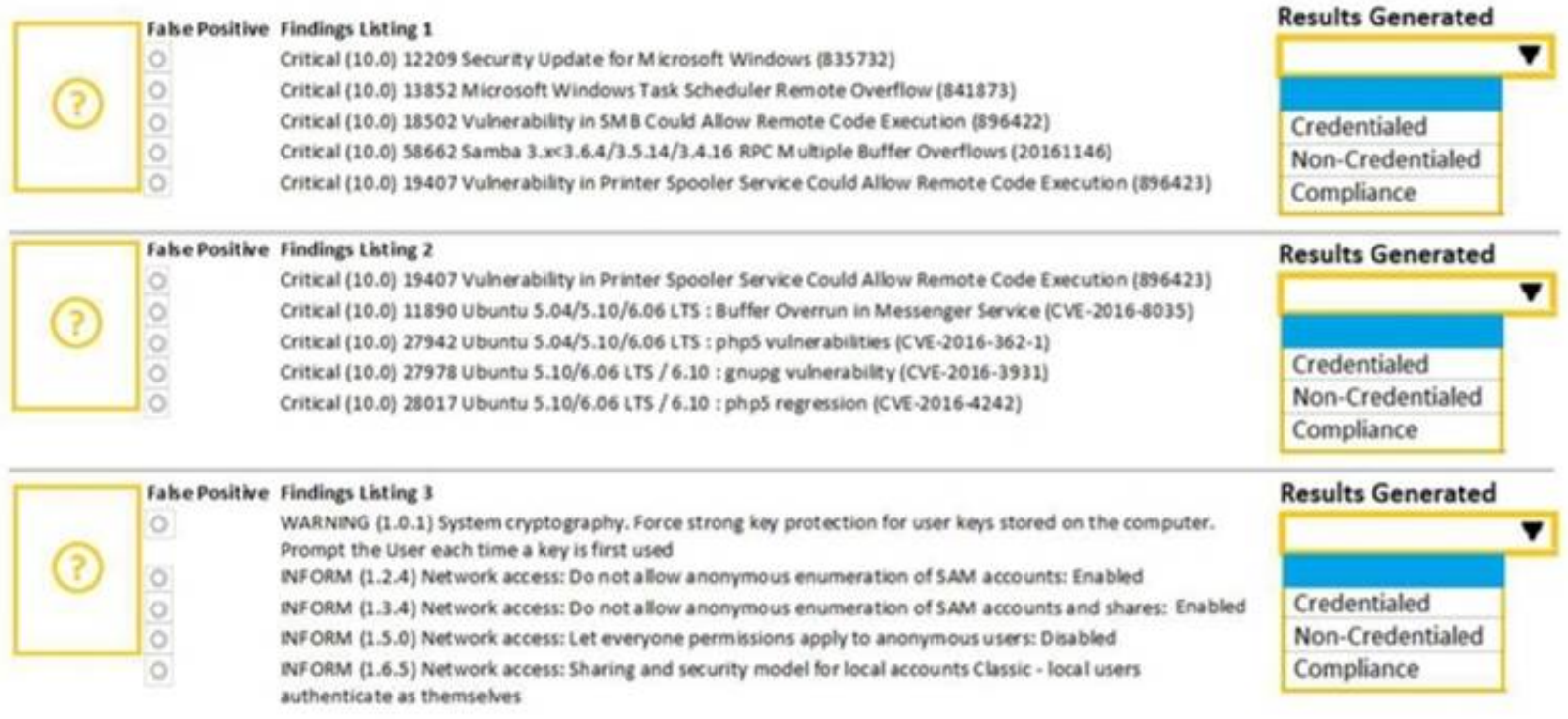
Answer: D

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

NEW QUESTION 60
- (Exam Topic 3)
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button.
When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Hot Area:

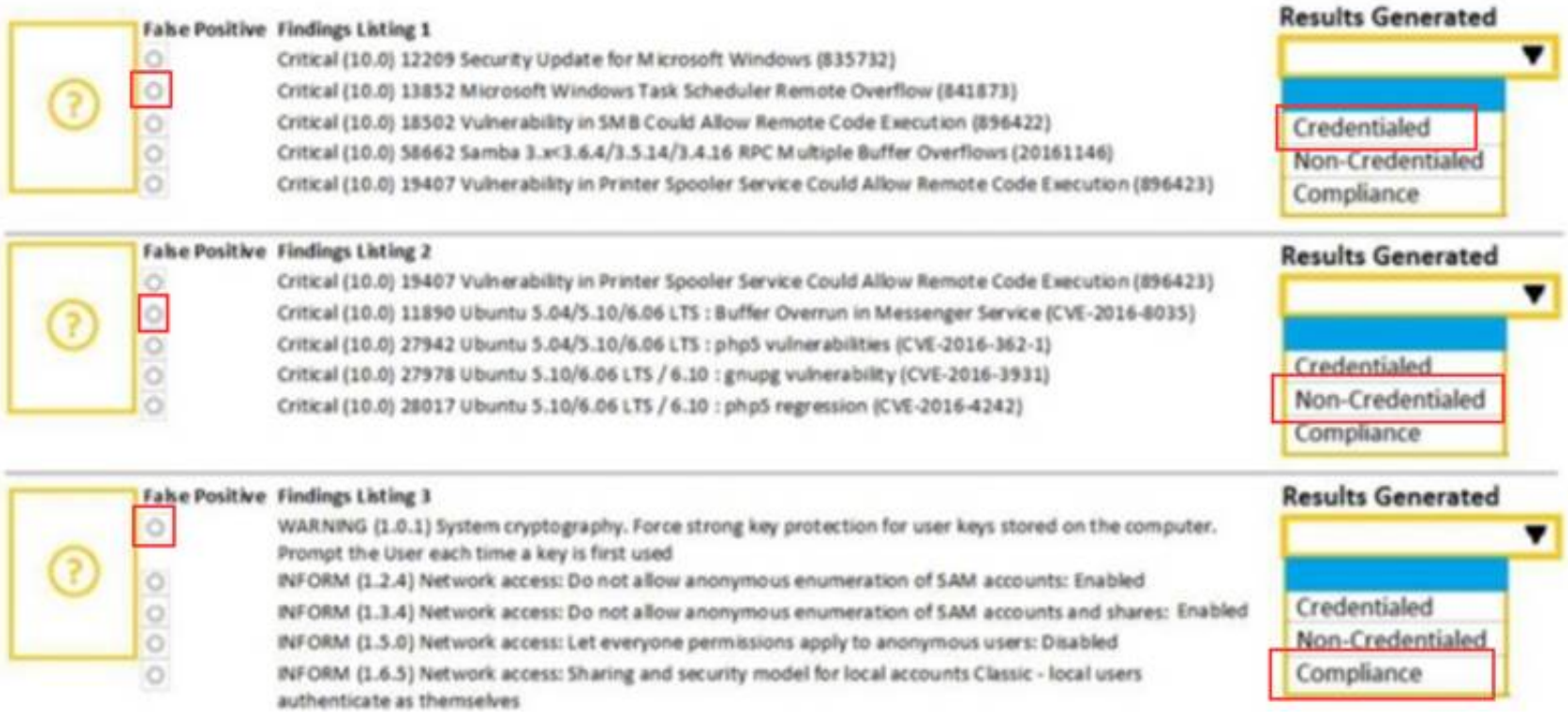


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Hot Area:



NEW QUESTION 64
- (Exam Topic 3)
The Chief information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue

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

Answer: C

NEW QUESTION 65
- (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 70
- (Exam Topic 3)
A security analyst is reviewing WAF logs and notes requests against the corporate website are increasing and starting to impact the performance of the web server. The security analyst queries the logs for requests that triggered an alert on the WAF but were not blocked. Which of the following possible TTP combinations might warrant further investigation? (Select TWO).

A. Requests identified by a threat intelligence service with a bad reputation
B. Requests sent from the same IP address using different user agents
C. Requests blocked by the web server per the input sanitization
D. Failed log-in attempts against the web application
E. Requests sent by NICs with outdated firmware
F. Existence of HTTP/501 status codes generated to the same IP address

Answer: AB

NEW QUESTION 75
- (Exam Topic 1)
A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.
Which of the following will remediate this software vulnerability?

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

Answer: C

NEW QUESTION 79
- (Exam Topic 1)
Which of the following BEST articulates the benefit of leveraging SCAP in an organization’s cybersecurity analysis toolset?

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

Answer: B

NEW QUESTION 83
- (Exam Topic 1)
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised.
Which of the following is the value of this risk?

A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Answer: A

NEW QUESTION 85
- (Exam Topic 1)
You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.
The company's hardening guidelines indicate the following:
• TLS 1.2 is the only version of TLS running.
• Apache 2.4.18 or greater should be used.
• Only default ports should be used. INSTRUCTIONS
Using the supplied data, record the status of compliance with the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.
Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8675/ssh open   ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 2

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Configuration Change Recommendations

Add recommendation for

- AppSrv1
- AppSrv2
- AppSrv3
- AppSrv4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1 Answer
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater

Part 2 Answer
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

NEW QUESTION 86
- (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 88
- (Exam Topic 1)
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

```
"GET /form.php?id=46322%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 90
- (Exam Topic 1)
After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

```
Port       State      Service    Version
80/tcp     open       http       Apache httpd 2.2.14
111/udp    open       rpcbind
443/tcp    filtered   https      Apache httpd 2.2.14
2222/tcp   open       ssh        OpenSSH 5.3p1 Debian
3306/tcp   open       mysql      5.5.40-0ubuntu0.14.1
```

Which of the following suggests the system that produced output was compromised?

A. Secure shell is operating of compromise on this system.
B. There are no indicators of compromise on this system.
C. MySQL services is identified on a standard PostgreSQL port.
D. Standard HTP is open on the system and should be closed.

Answer: A

NEW QUESTION 92
- (Exam Topic 1)
The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

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

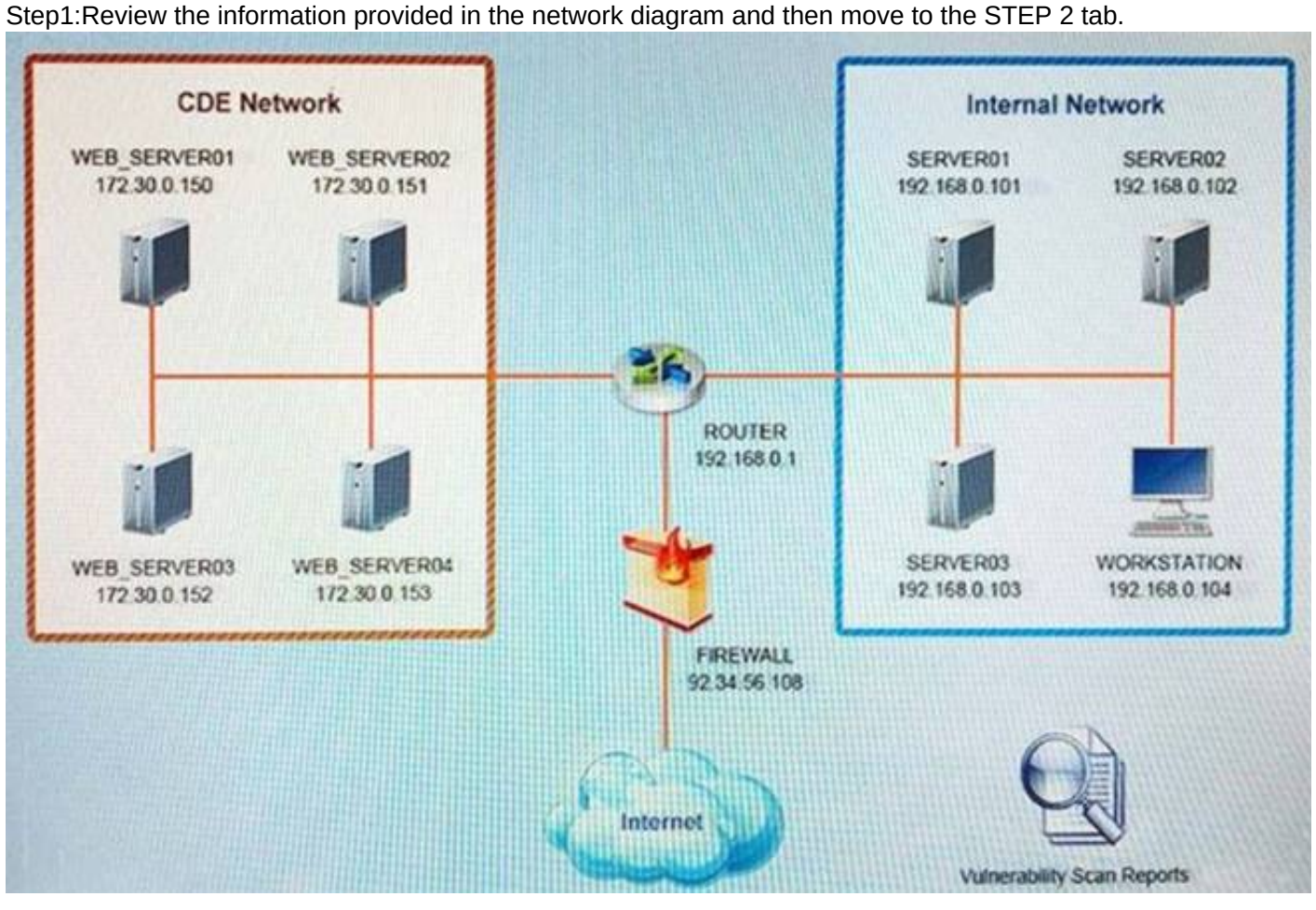
Answer: B

NEW QUESTION 97
- (Exam Topic 1)
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

A. It enables the team to prioritize the focus area and tactics within the company's environment.
B. It provide critically analyses for key enterprise servers and services.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It supports rapid response and recovery during and followed an incident.

Answer: A

NEW QUESTION 101
- (Exam Topic 3)
The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.
If the venerability is not valid, the analyst must take the proper steps to get the scan clean. If the venerability is valid, the analyst must remediate the finding.
After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.
INTRUCTIONS:
The simulation includes 2 steps.
Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

MEDIUM SEVERITY

Title:	Sensitive Cookie in HTTPS session without 'Secure' Attribute
Description:	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
Risk:	Session Sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 Certificate
Description:	The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Network Diagram

INSTRUCTIONS

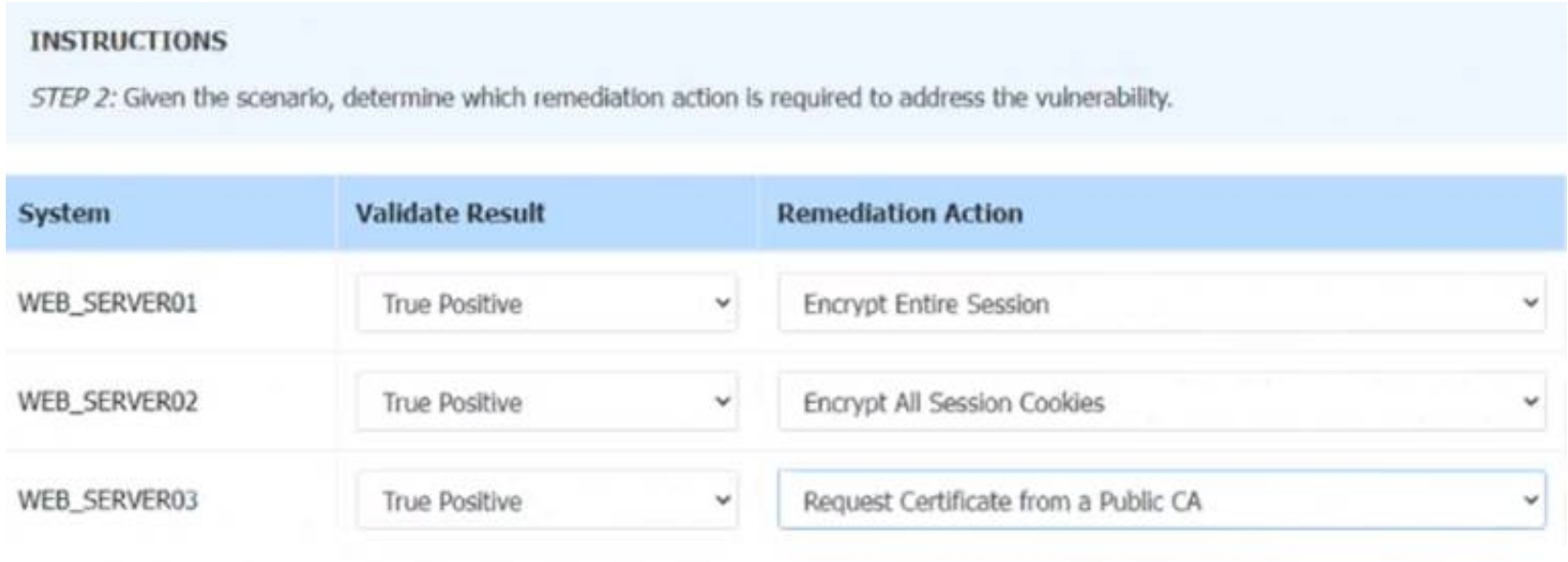
STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 102
- (Exam Topic 2)
During an investigation, an analyst discovers the following rule in an executive's email client: IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>
The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

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

Answer: A

NEW QUESTION 103
- (Exam Topic 2)
A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted The company has asked a security analyst to help improve its controls.
Which of the following will MOST likely help the security analyst develop better controls?

A. An evidence summarization
B. An indicator of compromise
C. An incident response plan
D. A lessons-learned report

Answer: C

NEW QUESTION 105
- (Exam Topic 2)
A security analyst receives a CVE bulletin, which lists several products that are used in the enterprise. The analyst immediately deploys a critical security patch.
Which of the following BEST describes the reason for the analyst's immediate action?

A. A known exploit was discovered.
B. There is an insider threat.
C. Nation-state hackers are targeting the region.
D. A new zero-day threat needs to be addressed.
E. A new vulnerability was discovered by a vendor.

Answer: E

NEW QUESTION 109
- (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 110
- (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 112
- (Exam Topic 2)
A security analyst reviews SIEM logs and detects a well-known malicious executable running in a Windows machine The up-to-date antivirus cannot detect the malicious executable Which of the following is the MOST likely cause of this issue?

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

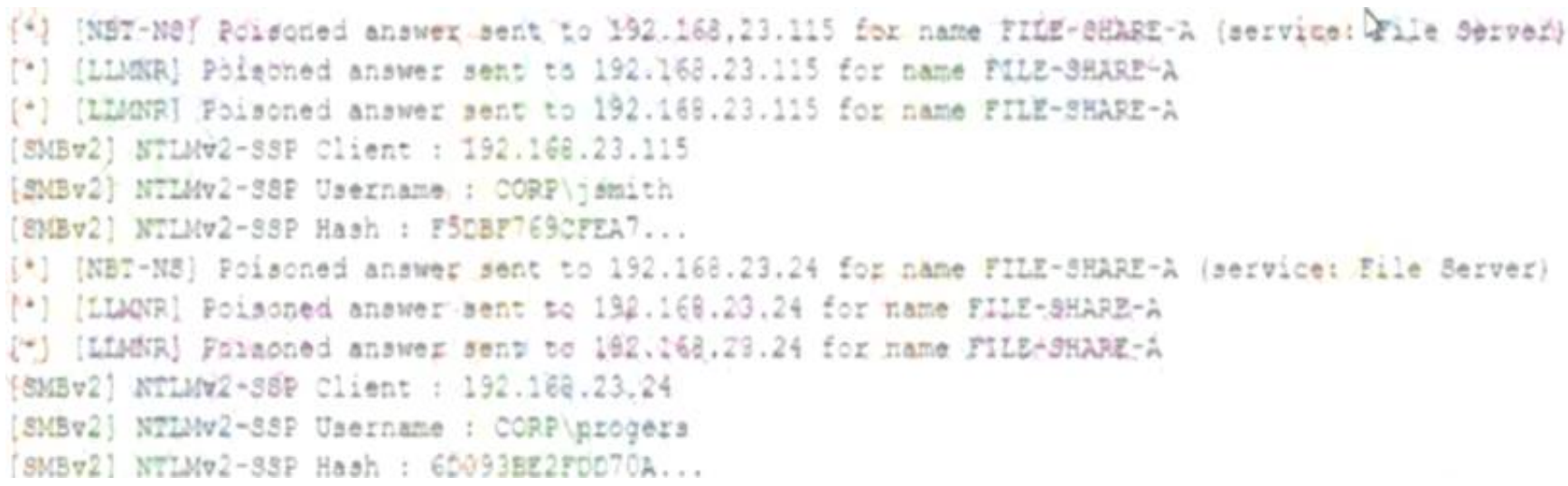
Answer: A

NEW QUESTION 116
- (Exam Topic 2)
A company wants to reduce the cost of deploying servers to support increased network growth. The company is currently unable to keep up with the demand, so it wants to outsource the infrastructure to a cloud-based solution.
Which of the following is the GREATEST threat for the company to consider when outsourcing its infrastructure?

A. The cloud service provider is unable to provide sufficient logging and monitoring.
B. The cloud service provider is unable to issue sufficient documentation for configurations.
C. The cloud service provider conducts a system backup each weekend and once a week during peak business times.
D. The cloud service provider has an SLA for system uptime that is lower than 99 9%.

Answer: B

NEW QUESTION 120
- (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:



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 125
- (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 127
- (Exam Topic 2)
An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

A. cat log xxd -r -p | egrep ' [0-9] {16}
B. egrep '(3(0-9)) (16) ' log
C. cat log | xxd -r -p egrep '(0-9) (16)'
D. egrep ' (0-9) (16) ' log | xxdc

Answer: C

NEW QUESTION 131
- (Exam Topic 2)
Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night.
Which of the following actions should the analyst take NEXT?

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

Answer: A

NEW QUESTION 134
- (Exam Topic 2)
A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level authentication is enabled
Which of the following is the BEST remediation for this vulnerability?

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

Answer: A

NEW QUESTION 138
- (Exam Topic 2)
Which of the following threat classifications would MOST likely use polymorphic code?

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

Answer: D

NEW QUESTION 142
- (Exam Topic 2)
A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

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

Answer: C

NEW QUESTION 147
- (Exam Topic 2)
While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?

A. Block the domain IP at the firewall.
B. Blacklist the new subnet
C. Create an IPS rule.
D. Apply network access control.

Answer: A

NEW QUESTION 152
- (Exam Topic 2)
An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?

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

Answer: D

NEW QUESTION 154
- (Exam Topic 2)
When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

```
root@ldap1:~# cat .pass.txt
jsmith:Welcome123:18073:0:99999:7:::
mjones4:Welcome123:18073:0:99999:7:::
egreen1:Welcome123:18073:0:99999:7:::
rbarger:Welcome123:18073:0:99999:7:::
mheme14:Welcome123:18073:0:99999:7:::
mgill:Welcome123:18073:0:99999:7:::
cyoung1:Welcome123:18073:0:99999:7:::
gkiepper3:Welcome123:18073:0:99999:7:::
```

Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?

A. A rogue LDAP server is installed on the system and is connecting password
B. The analyst should recommend wiping and reinstalling the server.
C. A password spraying attack was used to compromise the password
D. The analyst should recommend that all users receive a unique password.
E. A rainbow tables attack was used to compromise the account
F. The analyst should recommend that future password hashes contains a salt.
G. A phishing attack was used to compromise the accoun
H. The analyst should recommend users install endpoint protection to disable phishing links.

Answer: B

NEW QUESTION 159
- (Exam Topic 2)
A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?

A. Web content filter
B. Access control list
C. Network access control
D. Data loss prevention

Answer: B

NEW QUESTION 160
- (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 165
- (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 168
- (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 169
- (Exam Topic 2)
A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?

A. To complicate the network and frustrate a potential malicious attacker
B. To reduce the number of IP addresses that are used on the network
C. To reduce the attack surface of those systems by segmenting the network based on risk
D. To create a design that simplifies the supporting network

Answer: C

NEW QUESTION 173
- (Exam Topic 2)
An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users1 laptops?

A. Use whole disk encryption.
B. Require the use of VPNs.
C. Require employees to sign an NDA.
D. implement a DLP solution.

Answer: A

NEW QUESTION 174
- (Exam Topic 2)

An analyst is reviewing the following output:

```
if (searchname != null)
 {
   %>
      employee <%searchname%> not found
  <%
 }
```

Which of the following was MOST likely used to discover this?

A. Reverse engineering using a debugger
B. A static analysis vulnerability scan
C. A passive vulnerability scan
D. A web application vulnerability scan

Answer: C

NEW QUESTION 179
- (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 182
- (Exam Topic 2)
Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

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

Answer: A

NEW QUESTION 184
- (Exam Topic 2)
A user reports the system is behaving oddly following the installation of an approved third-party software application. The application executable was sourced from an internal repository Which of the following will
ensure the application is valid?

A. Ask the user to refresh the existing definition file for the antivirus software
B. Perform a malware scan on the file in the internal repository
C. Hash the application's installation file and compare it to the hash provided by the vendor
D. Remove the user's system from the network to avoid collateral contamination

Answer: C

NEW QUESTION 189
- (Exam Topic 2)
An organization's network administrator uncovered a rogue device on the network that is emulating the charactenstics of a switch. The device is trunking protocols and inserting tagging va the flow of traffic at the data link layer
Which of the following BEST describes this attack?

A. VLAN hopping
B. Injection attack
C. Spoofing
D. DNS pharming

Answer: A

NEW QUESTION 194
- (Exam Topic 2)
A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

A. Data masking
B. Data loss prevention
C. Data minimization
D. Data sovereignty

Answer: A

NEW QUESTION 199
- (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 203
- (Exam Topic 2)
A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

A. Establish a recovery time objective and a recovery point objective for the systems being moved
B. Calculate the resource requirements for moving the systems to the cloud
C. Determine recovery priorities for the assets being moved to the cloud-based systems
D. Identify the business processes that will be migrated and the criticality of each one
E. Perform an inventory of the servers that will be moving and assign priority to each one

Answer: D

NEW QUESTION 207
- (Exam Topic 2)
The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?

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

Answer: D

NEW QUESTION 209
- (Exam Topic 2)
A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

A. To reject email from servers that are not listed in the SPF record
B. To reject email from email addresses that are not digitally signed.
C. To accept email to the company's domain.
D. To reject email from users who are not authenticated to the network.

Answer: A

NEW QUESTION 210
- (Exam Topic 2)
A critical server was compromised by malware, and all functionality was lost. Backups of this server were taken; however, management believes a logic bomb may have been injected by a rootkit. Which of the following should a security analyst perform to restore functionality quickly?

A. Work backward, restoring each backup until the server is clean
B. Restore the previous backup and scan with a live boot anti-malware scanner
C. Stand up a new server and restore critical data from backups
D. Offload the critical data to a new server and continue operations

Answer: B

NEW QUESTION 214
- (Exam Topic 2)
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 216
- (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 220
- (Exam Topic 2)
Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

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

Answer: A

NEW QUESTION 221
- (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 225
- (Exam Topic 2)
D18912E1457D5D1DDCBD40AB3BF70D5D
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.

```
Nmap -Pn 10.233.117.0/24

Host is up (0.0021s latency)
Not shown: 987 filtered ports

PORT      STATE     SERVICE
22/tcp    open      ssh
135/tcp   open      msrpc
445/tcp   open      microsoft-ds
137/udp   open      netbios-ns
3389/tcp  open      ms-term-serv
```

Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?

A. Port 22
B. Port 135
C. Port 445

D. Port 3389

Answer: B

NEW QUESTION 226
- (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 227
- (Exam Topic 2)
A security analyst needs to perform a search for connections with a suspicious IP on the network traffic. The company collects full packet captures at the Internet gateway and retains them for one week. Which of the following will enable the analyst to obtain the BEST results?

A. tcpdump –n –r internet.pcap host <suspicious ip>
B. strings internet.pcap | grep <suspicious ip>
C. grep –a <suspicious ip> internet.pcap
D. npcapd internet.pcap | grep <suspicious ip>

Answer: A

NEW QUESTION 230
- (Exam Topic 2)
A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company's internal network. Although there is a negligible impact to performance, the following symptom present on each of the affected systems:
• Existence of a new and unexpected svchost exe process
• Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred
• DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain If this situation remains unresolved, which of the following will MOST likely occur?

A. The affected hosts may participate in a coordinated DDoS attack upon command
B. An adversary may leverage the affected hosts to reconfigure the company's router ACLs.
C. Key files on the affected hosts may become encrypted and require ransom payment for unlock.
D. The adversary may attempt to perform a man-in-the-middle attack.

Answer: C

NEW QUESTION 234
- (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 236
- (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 239
- (Exam Topic 2)
While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful?

A. Implement MFA on the email portal using out-of-band code delivery.
B. Create a new rule in the IDS that triggers an alert on repeated login attempts
C. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
D. Alter the lockout policy to ensure users are permanently locked out after five attempts.

E. Configure a WAF with brute force protection rules in block mode

Answer: A

NEW QUESTION 242
- (Exam Topic 2)
A forensic analyst took an image of a workstation that was involved in an incident To BEST ensure the image is not tampered with me analyst should use:

A. hashing
B. backup tapes
C. a legal hold
D. chain of custody.

Answer: A

NEW QUESTION 247
- (Exam Topic 2)
Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

A. Open threat exchange
B. H-ISAC
C. Dark web chatter
D. Dental forums

Answer: B

NEW QUESTION 250
- (Exam Topic 2)
A company recently experienced multiple DNS DDoS attacks, and the information security analyst must provide a DDoS solution to deploy in the company's datacenter Which of the following would BEST prevent future attacks?

A. Configure a sinkhole on the router.
B. Buy a UTM to block the number of requests.
C. Route the queries on the DNS server to 127.0.0.1.
D. Call the Internet service provider to block the attack.

Answer: A

NEW QUESTION 254
- (Exam Topic 2)
An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization’s network and identify active hosts. An analyst sees the following output from a packet capture:

```
192.168.2.3 (eth0 192.168.2.3): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.2.3 ttl=64 id=12345 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
```

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

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

Answer: D

NEW QUESTION 256
- (Exam Topic 2)
A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

A. Scrum
B. loC feeds
C. ISAC
D. VSS scores

Answer: B

NEW QUESTION 261
- (Exam Topic 2)
A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

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

Answer: C

NEW QUESTION 265
- (Exam Topic 1)
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: D

NEW QUESTION 267
- (Exam Topic 1)
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 268
- (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 269
- (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 271
- (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 273
- (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 275
- (Exam Topic 1)
An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery

time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region
D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Answer: C

Explanation:
A hot site is always ready to take over the primary site's workload, so wouldn't it be more cost-effective in the long run? Additionally, a hot site would provide faster recovery times and better protection against data loss compared to a warm site.

NEW QUESTION 280
- (Exam Topic 1)
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-the-middle attack .The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,
B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

Answer: A

NEW QUESTION 283
- (Exam Topic 1)
A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 1)
An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT     STATE     SERVICE
20/tcp   filtered  ftp-data
21/tcp   filtered  ftp
22/tcp   open      ssh
23/tcp   open      telnet
80/tcp   open      http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```

Which of the following should the analyst investigate FIRST?

A. Port 21
B. Port 22
C. Port 23
D. Port 80

Answer: A

NEW QUESTION 287
- (Exam Topic 1)
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users The application then uses a service account, to perform queries and look up data m a database A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

A. Change the security model to force the users to access the database as themselves
B. Parameterize queries to prevent unauthorized SQL queries against the database
C. Configure database security logging using syslog or a SIEM
D. Enforce unique session IDs so users do not get a reused session ID

Answer: B

NEW QUESTION 288
- (Exam Topic 1)
A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic.
Which of the following would BEST accomplish this goal?

A. Continuous integration and deployment
B. Automation and orchestration
C. Static and dynamic analysis
D. Information sharing and analysis

Answer: B

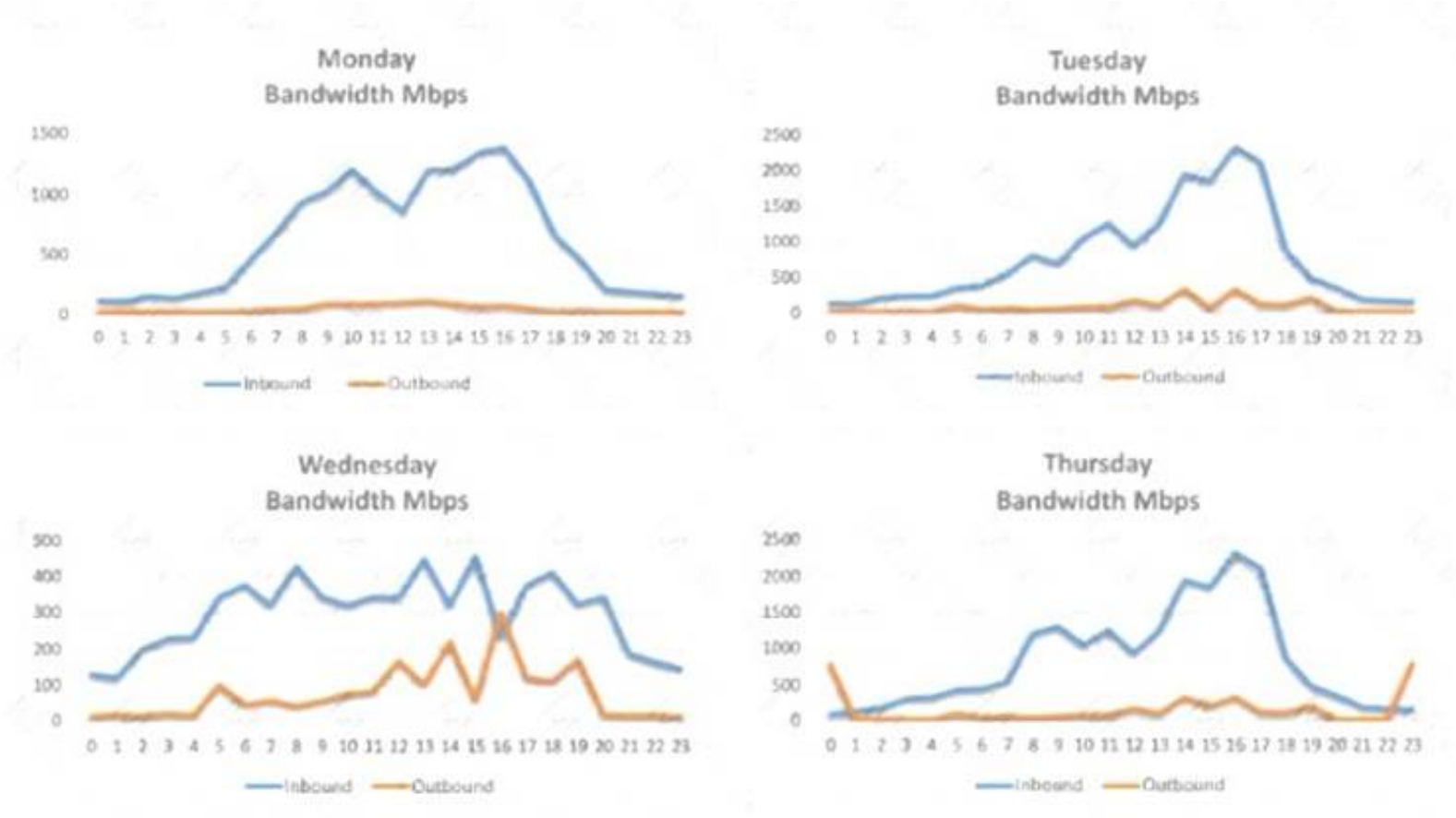
NEW QUESTION 291
- (Exam Topic 1)
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.
Which of the following BEST describes this attack?

A. Injection attack
B. Memory corruption
C. Denial of service
D. Array attack

Answer: C

Explanation:
Reference: https://economictimes.indiatimes.com/definition/memory-corruption

NEW QUESTION 293
- (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 294
- (Exam Topic 1)
A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

A. Begin blocking all IP addresses within that subnet.
B. Determine the attack vector and total attack surface.
C. Begin a kill chain analysis to determine the impact.
D. Conduct threat research on the IP addresses

Answer: D

NEW QUESTION 295
- (Exam Topic 1)
Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery
B. Cross-site scripting
C. SQL injection
D. Command injection
E. Cross-site request forgery
F. Directory traversal

Answer: B

NEW QUESTION 296
- (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 301
- (Exam Topic 1)
A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

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

Answer: C

NEW QUESTION 302
- (Exam Topic 1)
The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

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

Answer: B

NEW QUESTION 305
- (Exam Topic 1)
An organization has several systems 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: A

NEW QUESTION 310
- (Exam Topic 1)
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 311
- (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 312
- (Exam Topic 1)
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?

A. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
D. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
E. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

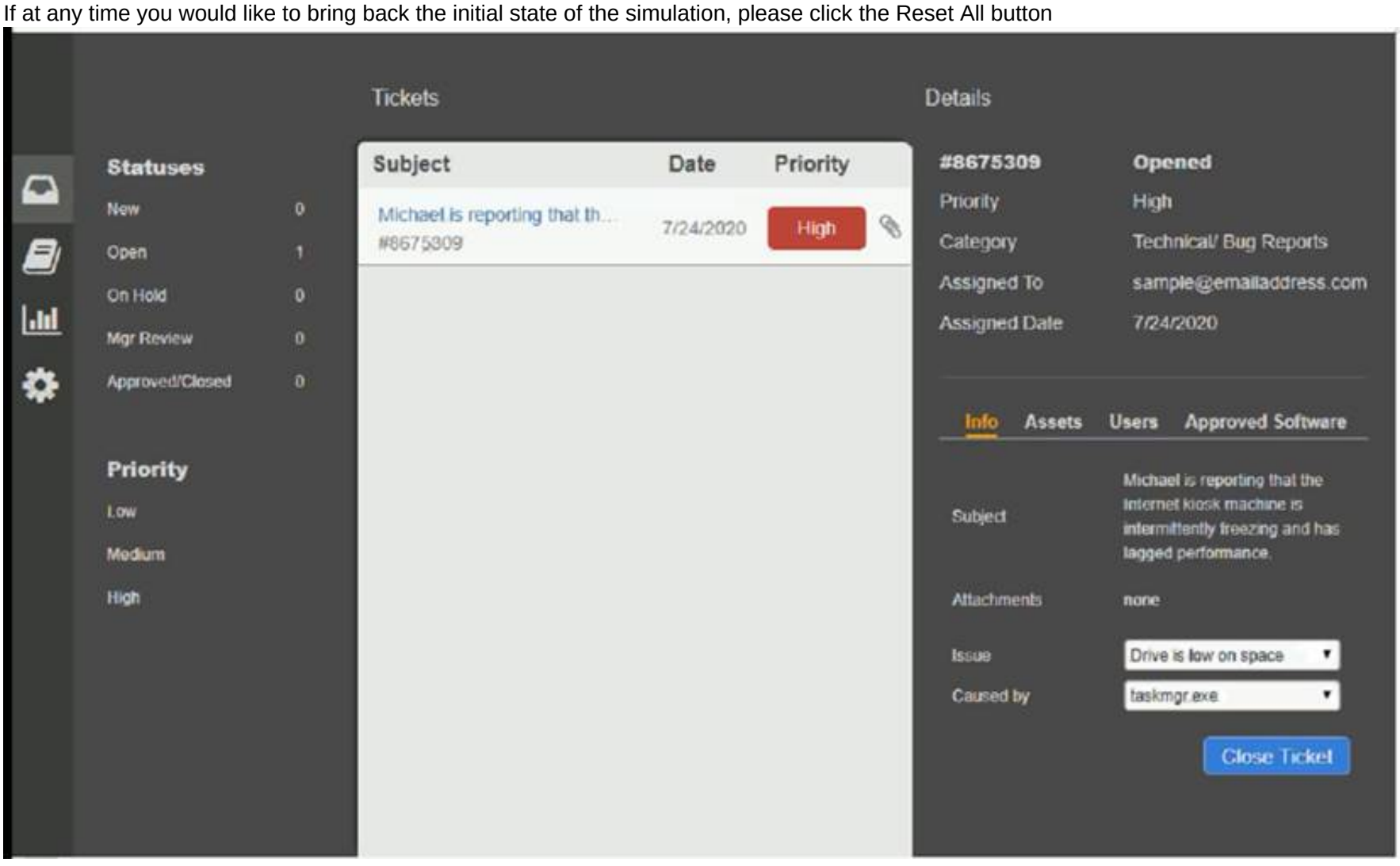
Answer: E

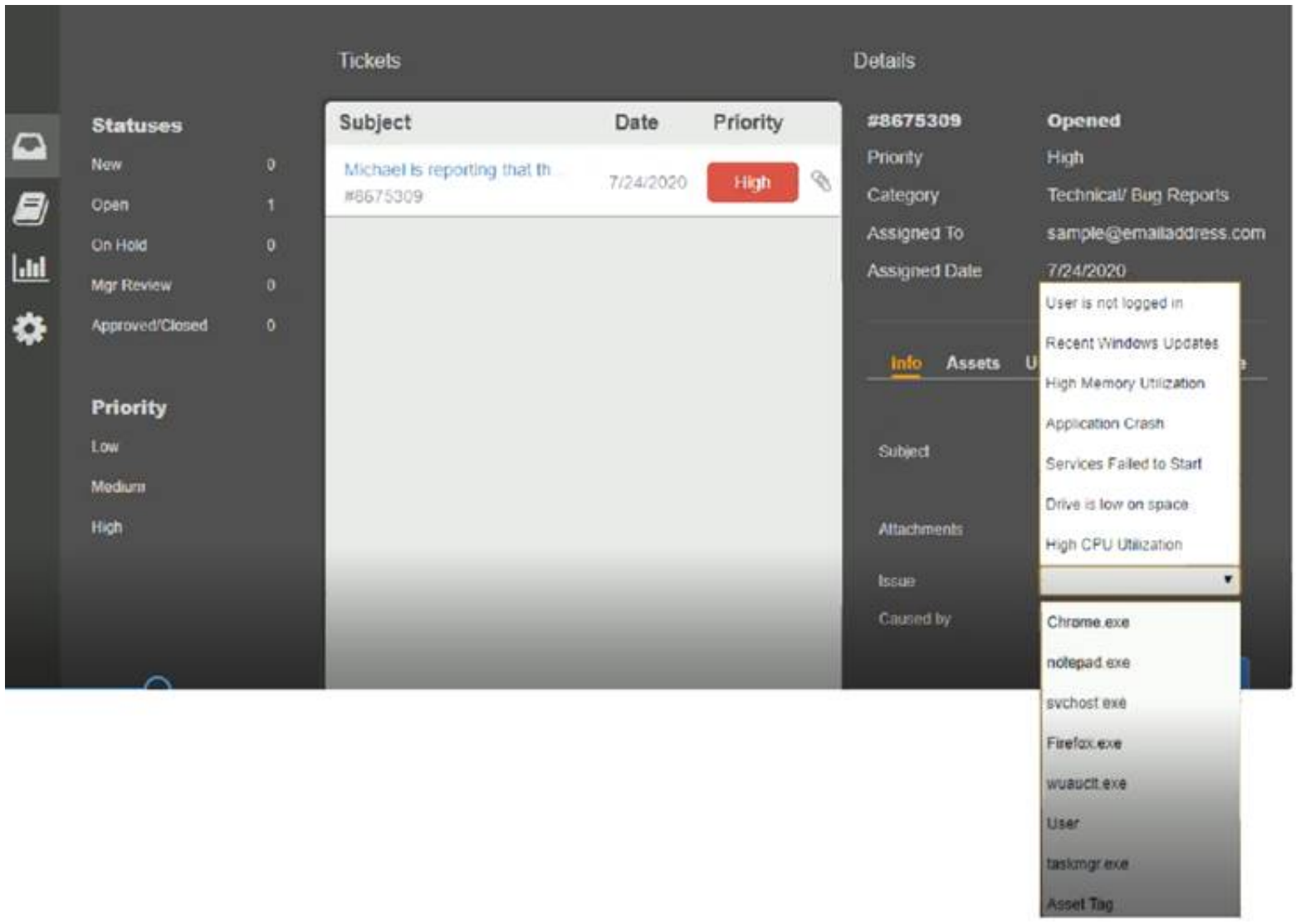
NEW QUESTION 317
- (Exam Topic 1)
A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

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

Answer: C

NEW QUESTION 322
- (Exam Topic 1)
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue. INSTRUCTIONS
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket
First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button

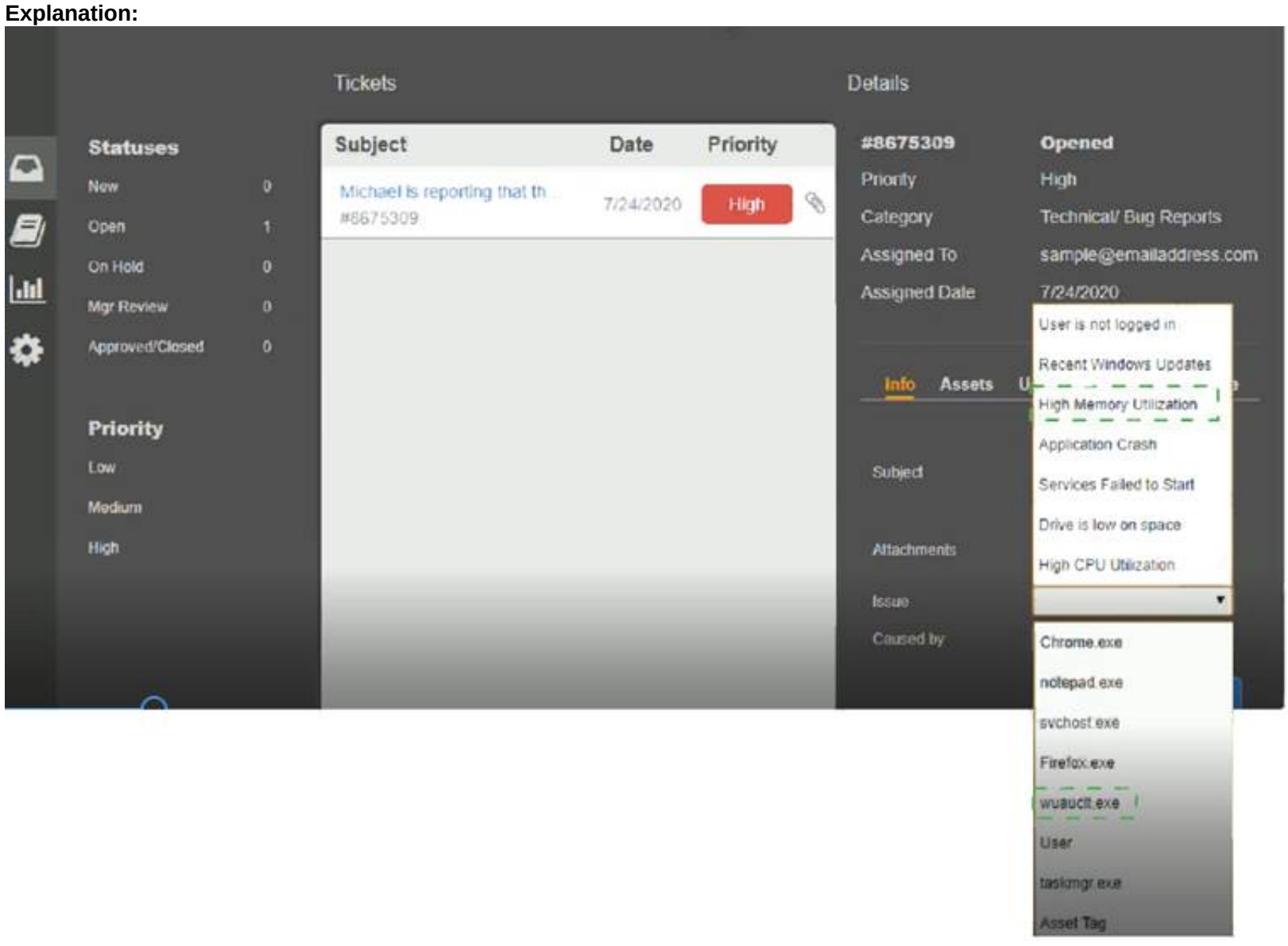




A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 326
- (Exam Topic 1)
A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed

B. Depending on system 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 Identify potentially affected systems by creating a correlation
D. Identify potentially affected system by creating a correlation search in the SIEM based on the networktraffic.

Answer: D

NEW QUESTION 330
- (Exam Topic 1)
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 331
- (Exam Topic 1)
A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.
Which of the following should be done to correct the cause of the vulnerability?

A. Deploy a WAF in front of the application.
B. Implement a software repository management tool.
C. Install a HIPS on the server.
D. Instruct the developers to use input validation in the code.

Answer: B

NEW QUESTION 333
- (Exam Topic 1)
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:
- Reduce the number of potential findings by the auditors.
- Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
- Prevent the external-facing web infrastructure used by other teams from coming into scope.
- Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 335
- (Exam Topic 1)
Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

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

Answer: AC

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

NEW QUESTION 339
- (Exam Topic 1)
An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested m 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 340
- (Exam Topic 1)
Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

A. Code of conduct policy
B. Account management policy
C. Password policy
D. Acceptable use policy

Answer: D

NEW QUESTION 345
- (Exam Topic 1)
A hybrid control is one that:

A. is implemented differently on individual systems
B. is implemented at the enterprise and system levels
C. has operational and technical components
D. authenticates using passwords and hardware tokens

Answer: B

NEW QUESTION 349
- (Exam Topic 1)
A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer datA. Developers use personal workstations, giving the company little to no visibility into the development activities.
Which of the following would be BEST to implement to alleviate the CISO's concern?

A. DLP
B. Encryption
C. Test data
D. NDA

Answer: D

NEW QUESTION 351
- (Exam Topic 1)
Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

A. Use a UEFl boot password.
B. Implement a self-encrypted disk.
C. Configure filesystem encryption
D. Enable Secure Boot using TPM

Answer: C

NEW QUESTION 353
- (Exam Topic 1)
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 356
- (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 360
- (Exam Topic 1)
A security analyst implemented a solution that would analyze the attacks that the organization’s firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.
S sudo nc -1 -v -c maildemon . py 25 caplog, txt
Which of the following solutions did the analyst implement?

A. Log collector
B. Crontab mail script
C. Snikhole
D. Honeypot

Answer: A

NEW QUESTION 363
- (Exam Topic 1)
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?
A)

```
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 368
- (Exam Topic 1)
A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.
Which of the following is the BEST example of the level of sophistication this threat actor is using?

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

Answer: B

NEW QUESTION 371
- (Exam Topic 1)
A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.
Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

A. Deidentification

B. Encoding
C. Encryption
D. Watermarking

Answer: A

NEW QUESTION 374
- (Exam Topic 1)
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:

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

Answer: C

NEW QUESTION 377
- (Exam Topic 1)
A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?

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

Answer: B

NEW QUESTION 381
- (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 382
- (Exam Topic 1)
A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.
Which of the following commands would MOST likely indicate if the email is malicious?

A. sha256sum ~/Desktop/file.pdf
B. file ~/Desktop/file.pdf
C. strings ~/Desktop/file.pdf | grep "<script"
D. cat < ~/Desktop/file.pdf | grep -i .exe

Answer: A

NEW QUESTION 387
- (Exam Topic 1)
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.
Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus

Answer: E

NEW QUESTION 391
- (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 393
- (Exam Topic 1)
A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics. cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

A. Cloning procedures
B. Chain of custody
C. Hashing procedures
D. Virtualization

Answer: B

NEW QUESTION 398
- (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 402
- (Exam Topic 1)
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 403
- (Exam Topic 1)
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 406
- (Exam Topic 1)
An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.
Which of the following should be considered FIRST prior to disposing of the electronic data?

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

Answer: D

NEW QUESTION 407
- (Exam Topic 1)
A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.
Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

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

Answer: A

NEW QUESTION 412
- (Exam Topic 1)
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

A. Review the firewall logs.
B. Review syslogs from critical servers.
C. Perform fuzzing.
D. Install a WAF in front of the application server.

Answer: B

NEW QUESTION 414
- (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 419
- (Exam Topic 1)
A security analyst needs to reduce the overall attack surface.
Which of the following infrastructure changes should the analyst recommend?

A. Implement a honeypot.
B. Air gap sensitive systems.
C. Increase the network segmentation.
D. Implement a cloud-based architecture.

Answer: B

Explanation:
Reference: https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface

NEW QUESTION 424
- (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 425
- (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 430
- (Exam Topic 1)
A security analyst has discovered trial developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

A. Create a security rule that blocks Internet access in the development VPC
B. Place a jumpbox m between the developers' workstations and the development VPC
C. Remove the administrator profile from the developer user group in identity and access management
D. Create an alert that is triggered when a developer installs an application on a server

Answer: A

NEW QUESTION 433
- (Exam Topic 3)
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

A. To identify weaknesses in an organization's security posture
B. To identify likely attack scenarios within an organization
C. To build a business security plan for an organization
D. To build a network segmentation strategy

Answer: B

NEW QUESTION 434
- (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 438
- (Exam Topic 3)
An organizational policy requires one person to input accounts payable and another to do accounts receivable.
A separate control requires one person to write a check and another person to sign all checks greater than
$5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?

A. Segregation of duties
B. Job rotation
C. Non-repudiaton
D. Dual control

Answer: D

NEW QUESTION 442
- (Exam Topic 3)
A Chief Executive Officer (CEO) is concerned the company will be exposed to data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: D

Explanation:
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner. You're only worried about that if you're in multiple locations. .
https://www.virtru.com/blog/gdpr-data-sovereignty-matters-globally

NEW QUESTION 443
- (Exam Topic 3)
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6….HTTP/1.1 200 OK
Server: nginx/1.6.2
-
```

Which of the following describes what has occurred?

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

Answer: B

Explanation:
This is based from the Info "(Application/octet-stream) https://isotropic.co/what-is-octet-stream/
"Connection: close" mean when used in the response message? Bookmark this question. Show activity on this post. When the client uses the Connection: close header in the request message, this means that it wants the server to close the connection after sending the response message. 200 OK is the most common HTTP status code. It generally means that the HTTP request succeeded. https://evertpot.com/http/200-ok
https://evertpot.com/http/200-ok

NEW QUESTION 445
- (Exam Topic 3)
An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device Which of the following should the analyst do to BEST mitigate future attacks?

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

Answer: A

NEW QUESTION 450
- (Exam Topic 3)
A team of network security analysts is examining network traffic to determine if sensitive data was exfitrated Upon further investigation, the analysts believe confidential data was compromised. Which of me following capattlnes would BEST defend against tnts type of sensitive data eifiitraUon?

A. Deploy an edge firewal.
B. Implement DLP
C. Deploy EDR.
D. Enaypi the hard drives

Answer: C

NEW QUESTION 451
- (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 456
- (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] [COMMAND=/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 ; COMMAND=/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 459
- (Exam Topic 3)
A cybersecurity analyst routinely checks logs, querying for login attempts. While querying for unsuccessful login attempts during a five-day period, the analyst produces the following report:

Users	Login Attempts
User 1	4
User 2	8
User 3	5
User 4	50
User 5	40
User 6	10
User 7	10
User 8	4
User 9	8
User 10	2

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

A. Users 4 and 5 are using their credentials to transfer files to multiple servers.
B. Users 4 and 5 are using their credentials to run an unauthorized scheduled task targeting some servers In the cloud.
C. An unauthorized user is using login credentials in a script.
D. A bot is running a brute-force attack in an attempt to log in to the domain.

Answer: D

NEW QUESTION 463
- (Exam Topic 3)
A new vanant of malware is spreading on ihe company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

A. Implement a sinkhole with a high entropy level
B. Disable TCP/53 at the penmeter firewall
C. Block TCP/443 at the edge router
D. Configure the DNS forwarders to use recursion

Answer: A

NEW QUESTION 467
- (Exam Topic 3)
A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

A. Enforce the existing security standards and controls.
B. Perform a risk analysis and qualify the risk with legal.
C. Perform research and propose a better technology.
D. Enforce the standard permits.

Answer: B

Explanation:

The International Standards Organization, or ISO, develops standards for businesses around the world so that they may operate using a uniform set of best practices. These standards are not enforceable laws, but companies who choose to follow them stand to gain international credibility from their compliance; standards are set as guidance for best practices but are not enforceable laws

NEW QUESTION 472
- (Exam Topic 3)
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

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

Answer: D

NEW QUESTION 476
- (Exam Topic 3)
A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

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

Answer: C

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

NEW QUESTION 479
- (Exam Topic 3)
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?
A)

```
dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5,sha1 hashlog=/mnt/usb/evidence.bin.hashlog
```

B)

```
dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
```

C)

```
tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt ;sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
```

D)

```
find / -type f -exec cp {} /mnt/usb/evidence/ \; shalsum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash
```

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

Answer: B

NEW QUESTION 483
- (Exam Topic 3)
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:
• The partners' PCs must not connect directly to the laboratory network.
• The tools the partners need to access while on the laboratory network must be available to all partners
• The partners must be able to run analyses on the laboratory network, which may take hours to complete Which of the following capabilities will MOST likely meet the security objectives of the request?

A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools tor analysis
C. Deployment of a firewall to allow access to the laboratory network and use of VDI In persistent mode to provide the necessary tools for analysis
D. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

Answer: C

NEW QUESTION 487
- (Exam Topic 3)
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?

A. Insert the hard drive on a test computer and boot the computer.
B. Record the serial numbers of both hard drives.

C. Compare the file-directory "sting of both hard drives.
D. Run a hash against the source and the destination.

Answer: D

NEW QUESTION 488
- (Exam Topic 3)
During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity The analyst also notes there is no other alert in place for this traffic After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

A. Share details of the security incident with the organization's human resources management team
B. Note the security incident so other analysts are aware the traffic is malicious
C. Communicate the security incident to the threat team for further review and analysis
D. Report the security incident to a manager for inclusion in the daily report

Answer: C

NEW QUESTION 491
- (Exam Topic 3)
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
C. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
D. Unsupervised algorithms produce more false positive
E. Than supervised algorithms.

Answer: B

NEW QUESTION 492
- (Exam Topic 3)
Which of the following can detect vulnerable third-parly libraries before code deployment?

A. Impact analysis
B. Dynamic analysis
C. Static analysis
D. Protocol analysis

Answer: C

NEW QUESTION 495
- (Exam Topic 3)
While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1.
C. Delete access key 1.
D. Delete access key 2.

Answer: D

NEW QUESTION 497
- (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 500
- (Exam Topic 3)
industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

A. Multifactor authentication
B. Manual access reviews
C. Endpoint detection and response
D. Role-based access control

Answer: C

NEW QUESTION 501
- (Exam Topic 3)
A SIEM analyst receives an alert containing the following URL:

http://companywebsite.com/displayPicture?filename=../../../etc/passwd

Which of the following BEST describes the attack?

A. Password spraying
B. Buffer overflow
C. insecure object access
D. Directory traversal

Answer: D

NEW QUESTION 506
- (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 511
- (Exam Topic 3)
A security team has begun updating the risk management plan incident response plan and system security plan to ensure compliance with secunty review guidelines Which of the (olowing can be executed by internal managers to simulate and validate the proposed changes'?

A. Internal management review
B. Control assessment
C. Tabletop exercise
D. Peer review

Answer: B

NEW QUESTION 513
- (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 515
- (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 518
- (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 519
- (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 524
- (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 526
- (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 531
- (Exam Topic 3)
While investigating reports or issues with a web server, a security analyst attempts to log in remotely and recedes the following message:

```
[root@localhost /root]# ssh user1@10.254.2.25
Connection timed out.
```

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

```
Out of memory: Kill process 3448(httpd) score 41 or sacrifice child
Killed process 3448(httpd) totle-vm:74716kB, anon-rss: 23456kB, file-rss:1683kB
Out of memory: Kill process 3449(httpd) score 41 or sacrifice child
Killed process 3449(httpd) totle-vm:74634kB, anon-rss: 20542kB, file-rss:1357kB
Out of memory: Kill process 3452(httpd) score 41 or sacrifice child
Killed process 3452(httpd) totle-vm:73466kB, anon-rss: 29753kB, file-rss:1925kB
```

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

```
10.254.2.25.6781 > 128.50.100.23.80
10.254.2.25.6782 > 128.50.100.23.80
10.254.2.25.6783 > 128.50.100.23.80
10.254.2.25.6784 > 128.50.100.23.80
```

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

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

Answer: A

NEW QUESTION 536
- (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 537
- (Exam Topic 3)
During routine monitoring a security analyst identified the following enterpnse network traffic: Packet capture output:

No.	Source	Destination	Protocol	Info
105	66.187.224.210	192.168.12.21	DNS	Standard query response A 209.132.177.50
106	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq=0 len=0 MSS=1460 TSV=1535
107	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 len=0
108	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=1 Ack=1 len=0
109	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1

Which of the following BEST describes what the security analyst observed?

A. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
B. 192.168.12.21 made a TCP connection to 66 187 224 210
C. 192.168.12.21 made a TCP connection to 209 132 177 50
D. 209.132.177.50 set up a TCP reset attack to 192 168 12 21

Answer: C

NEW QUESTION 539
- (Exam Topic 3)
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?

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

Answer: A

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

NEW QUESTION 543
- (Exam Topic 3)
An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

A. Consult the malware analysis process
B. Consult the disaster recovery plan
C. Consult the data classification process
D. Consult the communications plan

Answer: D

NEW QUESTION 545
- (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 550
- (Exam Topic 3)
During the threal modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: C

NEW QUESTION 551
- (Exam Topic 3)
A small organization has proprietary software that is used internally. The system has not been wen maintained and cannot be updated with the rest or the environment. Which of the following is the BEST solution?

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

Answer: C

NEW QUESTION 556
- (Exam Topic 3)
A company uses an FTP server to support its critical business functions The FTP server is configured as follows:
• The FTP service is running with (he data duectory configured in /opt/ftp/data.
• The FTP server hosts employees' home aVectories in /home
• Employees may store sensitive information in their home directories
An loC revealed that an FTP director/ traversal attack resulted in sensitive data loss Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?

A. Implement file-level encryption of sensitive files
B. Reconfigure the FTP server to support FTPS
C. Run the FTP server n a chroot environment
D. Upgrade the FTP server to the latest version

Answer: C

NEW QUESTION 561
- (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 564
- (Exam Topic 3)
As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data Which of the following would be appropnate for the security analyst to coordinate?

A. A black-box penetration testing engagement
B. A tabletop exercise
C. Threat modeling
D. A business impact analysis

Answer: D

NEW QUESTION 567
- (Exam Topic 3)
A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

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

Answer: C

Explanation:
A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.
"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."

NEW QUESTION 569
- (Exam Topic 3)
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

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

Answer: A

NEW QUESTION 573
- (Exam Topic 3)
Which of the following is a difference between SOAR and SCAP?

A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts

Answer: D

NEW QUESTION 577
- (Exam Topic 3)
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?

A. Block the sender In the email gateway.
B. Delete the email from the company's email servers.
C. Ask the sender to stop sending messages.
D. Review the message in a secure environment.

Answer: D

NEW QUESTION 582
- (Exam Topic 3)
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?

A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist

Answer: D

NEW QUESTION 587
- (Exam Topic 3)
A Chief Executive Officer (CEO) is concerned about the company’s intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
B. Enable data masking and reencrypt the data sets using AES-256.
C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

Answer: C

NEW QUESTION 592
.....

Relate Links

100% Pass Your CS0-002 Exam with Exambible Prep Materials

https://www.exambible.com/CS0-002-exam/

Contact us

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

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