CompTIA

Exam Questions CS0-002

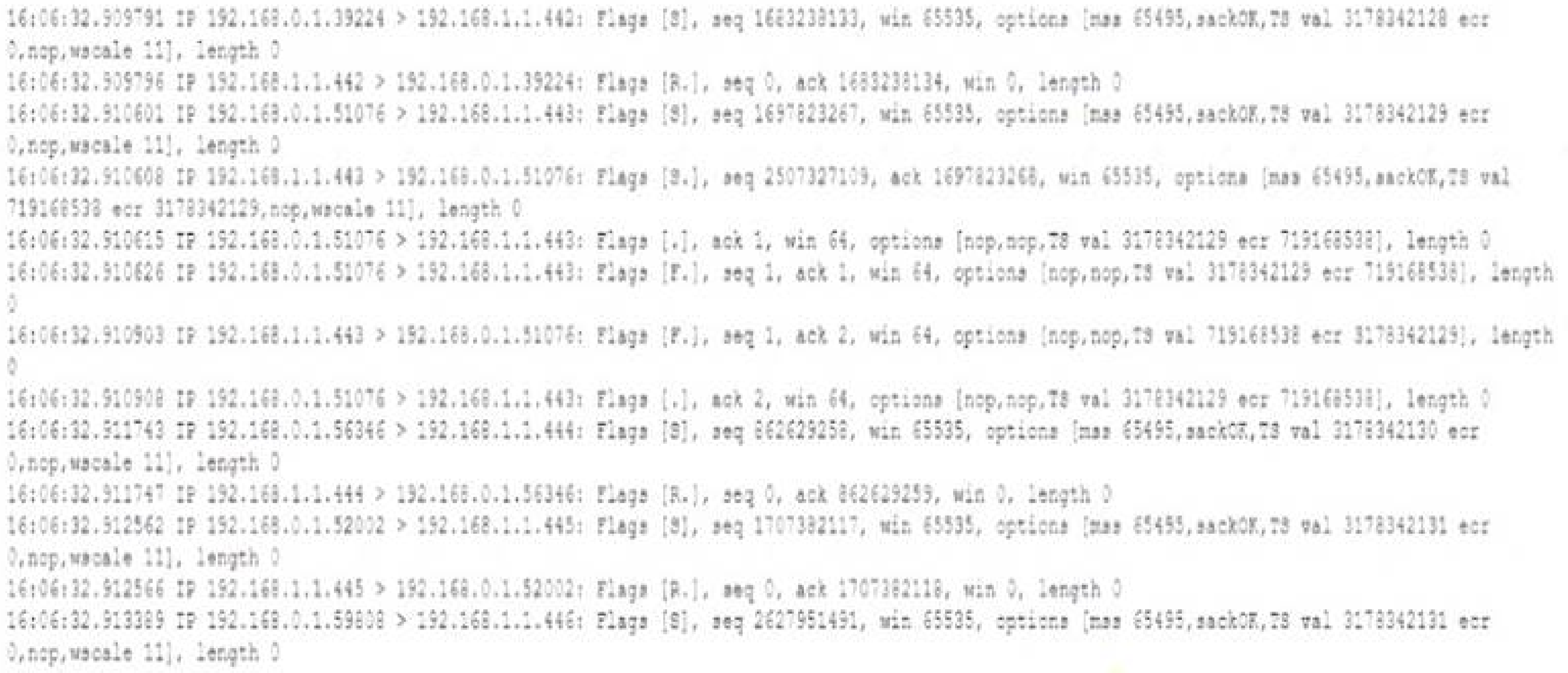
CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
- (Exam Topic 3)
An organization has specific technical nsk mitigation configurations that must be implemented before a new server can be approved for production Several critical servers were recently deployed with the antivirus missing unnecessary ports disabled and insufficient password complexity Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?

A. Perform password-cracking attempts on all devices going into production
B. Perform an Nmap scan on all devices before they are released to production
C. Perform antivirus scans on all devices before they are approved for production
D. Perform automated security controls testing of expected configurations pnor to production

Answer: D

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

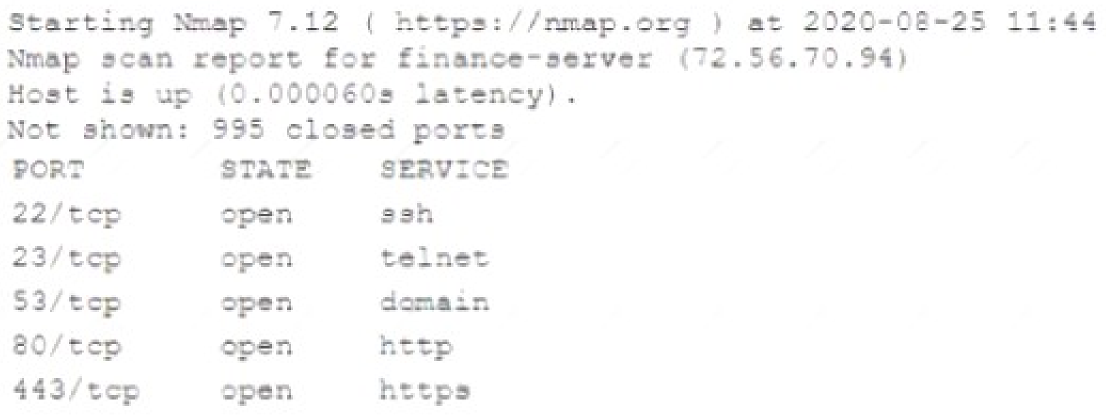
Explanation:
Port scan againts 442-446 ports. For port 443 the scanner closed the connection after SYN-ACK.

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

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

Answer: D

NEW QUESTION 4
- (Exam Topic 3)
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:



```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
```

Which of the following should the cybersecunty analyst recommend to harden the server? (Select TWO).

A. Uninstall the DNS service
B. Perform a vulnerability scan
C. Change the server's IP to a private IP address
D. Disable the Telnet service
E. Block port 80 with the host-based firewall
F. Change the SSH port to a non-standard port

Answer: BD

NEW QUESTION 5
- (Exam Topic 3)
Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

A. Set up an FTP server that both companies can access and export the required financial data to a folder.
B. Set up a VPN between Company A and Company
C. granting access only lo the ERPs within the connection
D. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
E. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.

Answer: B

NEW QUESTION 6
- (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 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 * xls > accessreport.txt
B. more webserver.log > grep ''xls > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E ''return=200 | accessreport.txt
D. more webserver.log | grep -A *.xls < accessreport.txt

Answer: C

NEW QUESTION 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)
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 12
- (Exam Topic 3)
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

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

Answer: B

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

NEW QUESTION 14
- (Exam Topic 3)
A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot oe reused. Which of the following is the BEST approach?

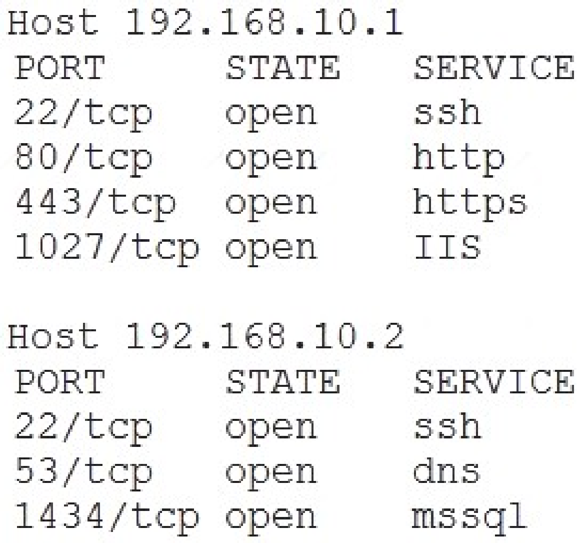
A. Degaussing
B. Shredding
C. Formatting
D. Encrypting

Answer: B

Explanation:

https://legalshred.com/degaussing-vs-hard-drive-shredding/
The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding

NEW QUESTION 17
- (Exam Topic 3)
An organization has the following policies:
*Services must run on standard ports.
*Unneeded services must be disabled.
The organization has the following servers:
*192.168.10.1 - web server
*192.168.10.2 - database server
A security analyst runs a scan on the servers and sees the following output:



```
Host 192.168.10.1
 PORT      STATE   SERVICE
 22/tcp    open    ssh
 80/tcp    open    http
 443/tcp   open    https
 1027/tcp  open    IIS

Host 192.168.10.2
 PORT      STATE   SERVICE
 22/tcp    open    ssh
 53/tcp    open    dns
 1434/tcp  open    mssql
```

Which of the following actions should the analyst take?

A. Disable HTTPS on 192.168.10.1.
B. Disable IIS on 192.168.10.1.
C. Disable DNS on 192.168.10.2.
D. Disable MSSQL on 192.168.10.2.
E. Disable SSH on both servers.

Answer: C

NEW QUESTION 22
- (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 25
- (Exam Topic 3)
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

A. A Linux-based system and mandatory training on Linux for all BYOD users
B. A firewalled environment for client devices and a secure VDI for BYOO users
C. A standardized anti-malware platform and a unified operating system vendor
D. 802.1X lo enforce company policy on BYOD user hardware

Answer: B

Explanation:
VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.

NEW QUESTION 26
- (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

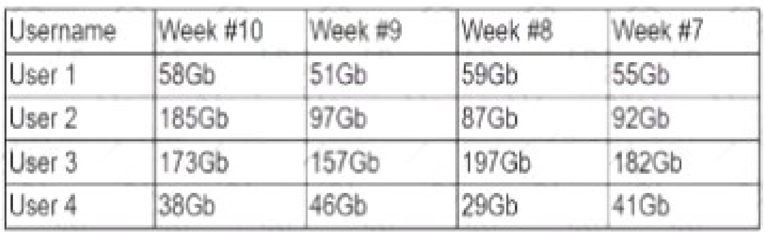
NEW QUESTION 28
- (Exam Topic 3)
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

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

Answer: D

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

NEW QUESTION 29
- (Exam Topic 3)
A security analyst is reviewing the following Internet usage trend report:



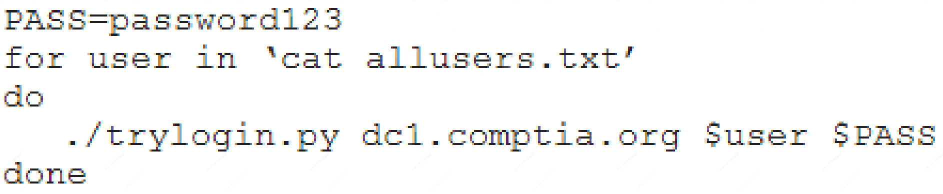
Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

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 30
- (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 34
- (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 37
- (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 39
- (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 41
- (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 46
- (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 49
- (Exam Topic 3)
A product security analyst has been assigned to evaluate and validate a new products security capabilities Part ot the evaluation involves reviewing design changes at specific intervals tor security deficiencies recommending changes and checking for changes at the next checkpoint Which of the following BEST defines the activity being conducted?

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

Answer: C

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

NEW QUESTION 53
- (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 55
- (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 60
- (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 61
- (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 63
- (Exam Topic 3)
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

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

Answer: B

NEW QUESTION 67
- (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

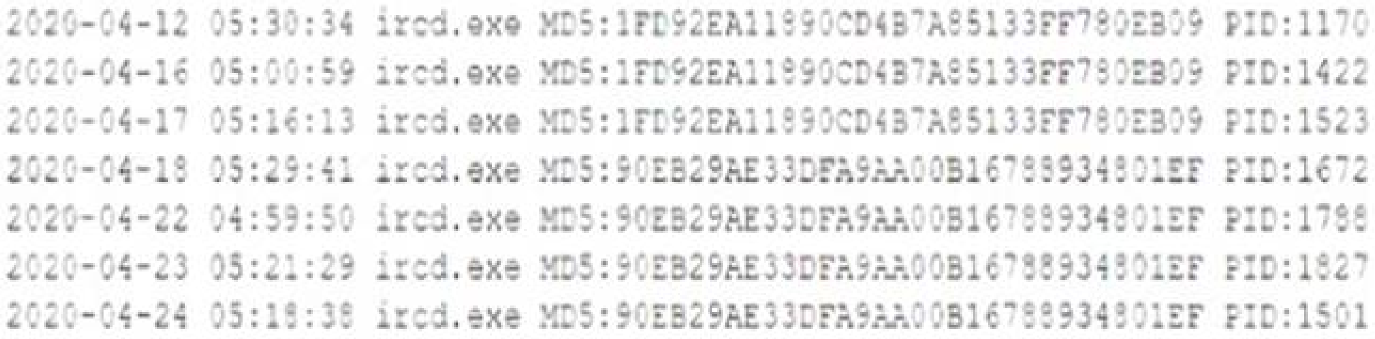
Answer: B

NEW QUESTION 68
- (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 72
- (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 74
- (Exam Topic 3)
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

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

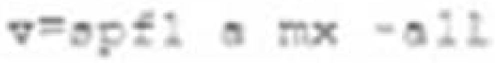
Answer: B

NEW QUESTION 75
- (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

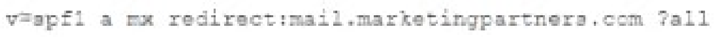
Answer: AB

NEW QUESTION 79
- (Exam Topic 1)
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:



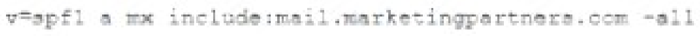
```
v=spf1 a mx -all
```

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)



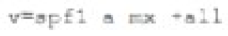
```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```

B)



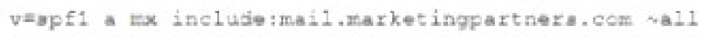
```
v=spf1 a mx include:mail.marketingpartners.com -all
```

C)



```
v=spf1 a mx +all
```

D)



```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

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

Answer: B

NEW QUESTION 84
- (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 87
- (Exam Topic 1)
A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments
B. Limiting email from the finance department to recipients on a pre-approved whitelist
C. Configuring email client settings to display all messages in plaintext when read
D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

NEW QUESTION 92
- (Exam Topic 1)
During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.
Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

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

Answer: A

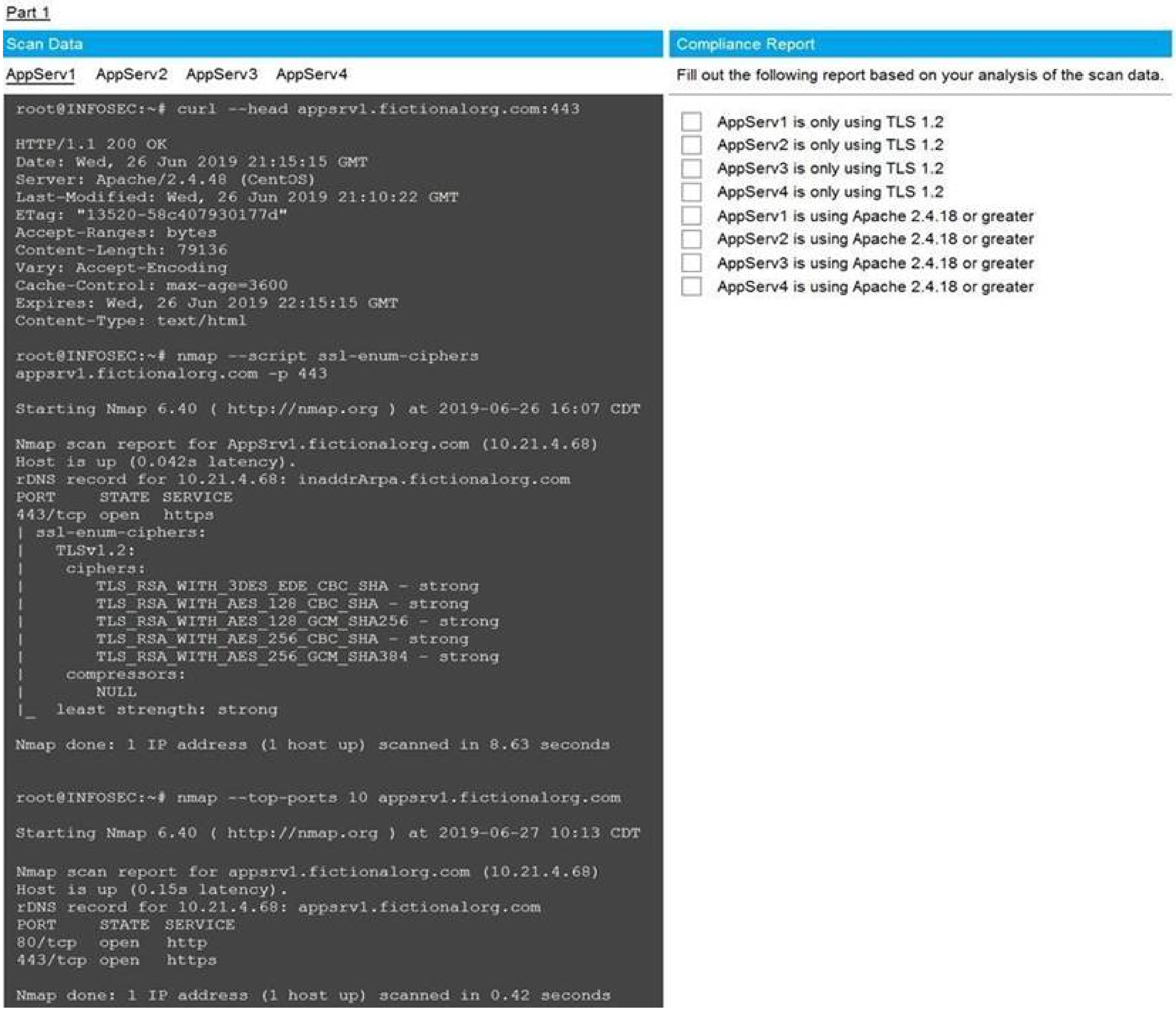
NEW QUESTION 96
- (Exam Topic 1)
Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

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

Answer: C

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

NEW QUESTION 97
- (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

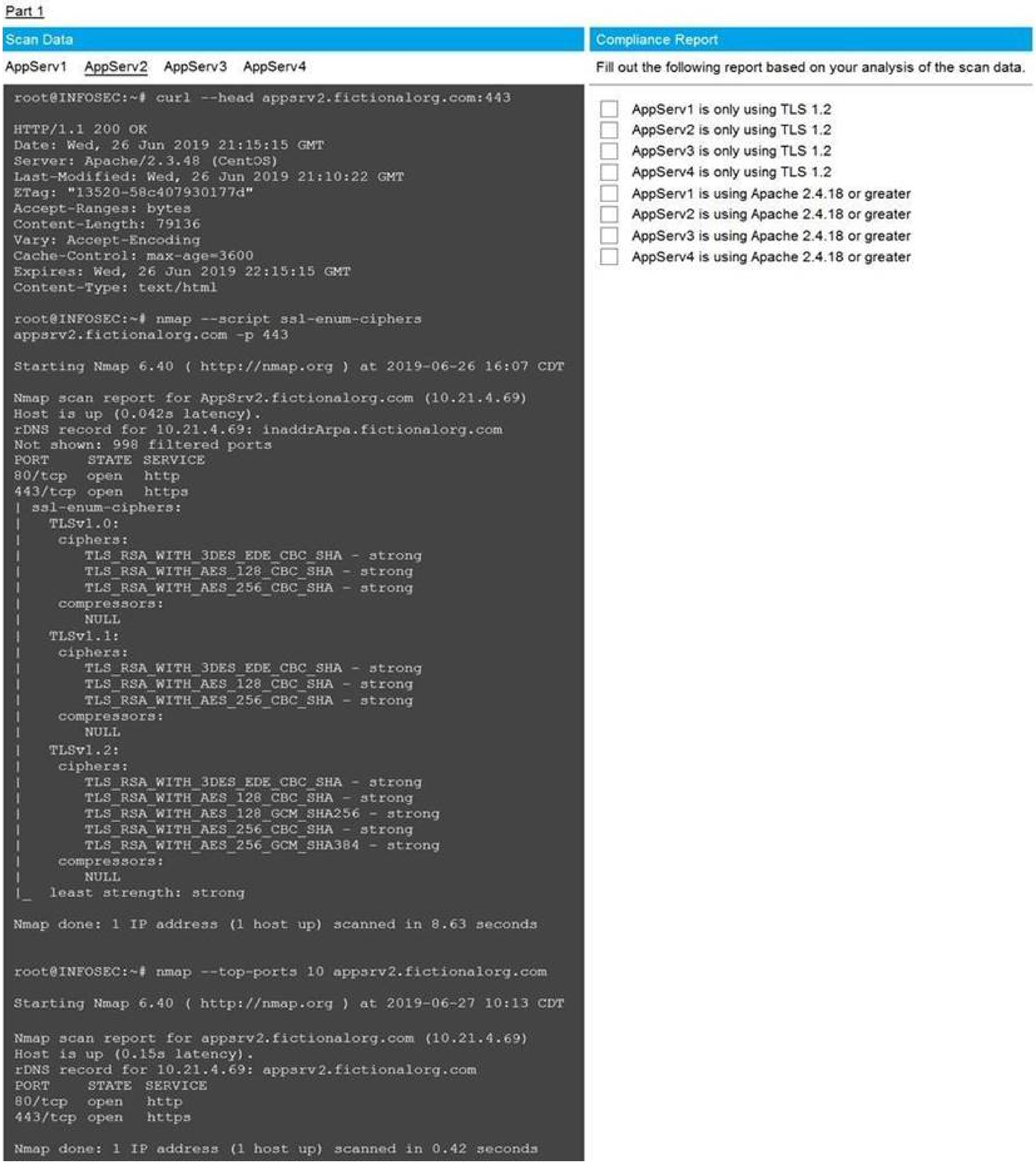
Scan Data

```
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



Part 1

Scan Data

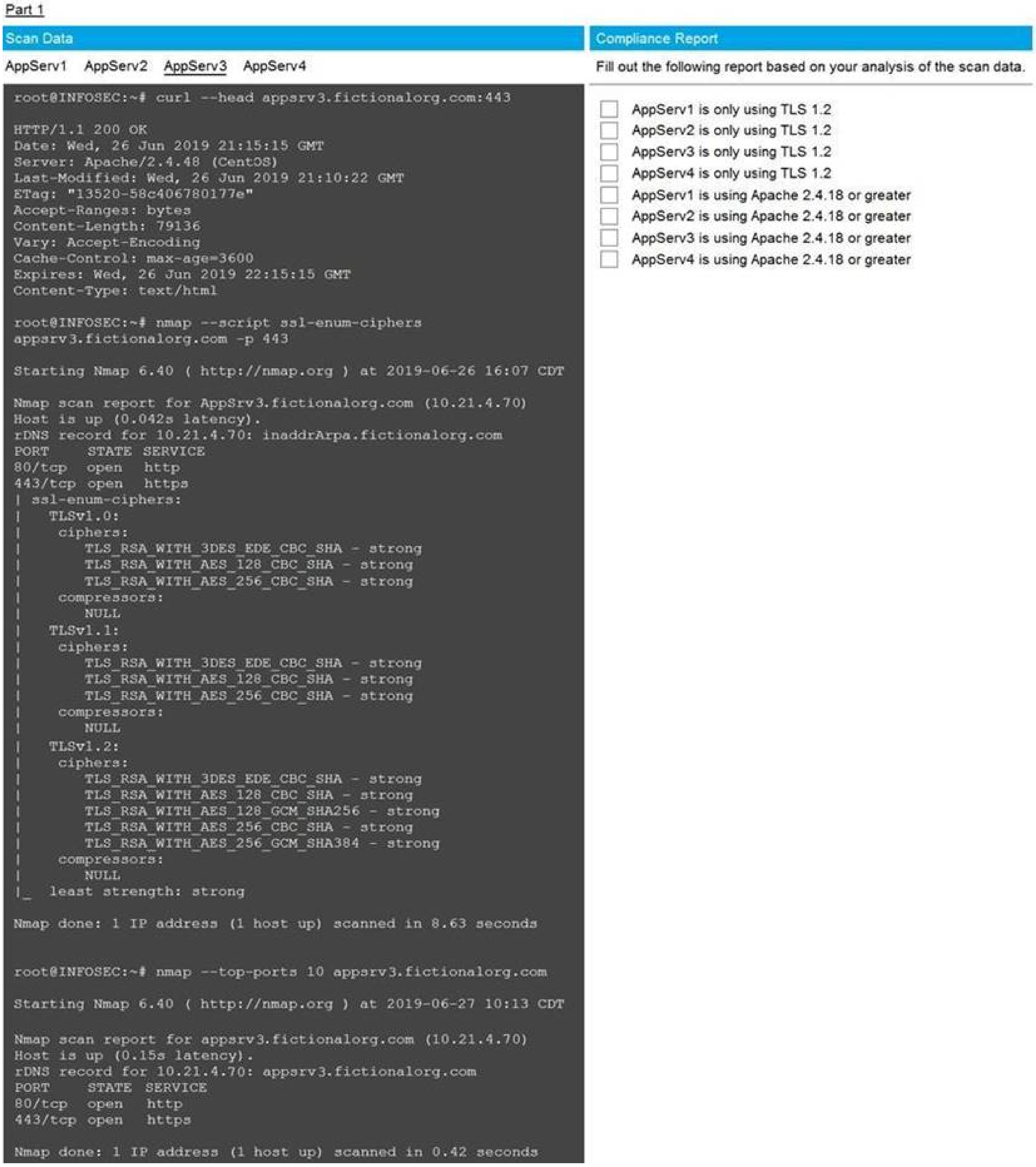
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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



Part 1

Scan Data

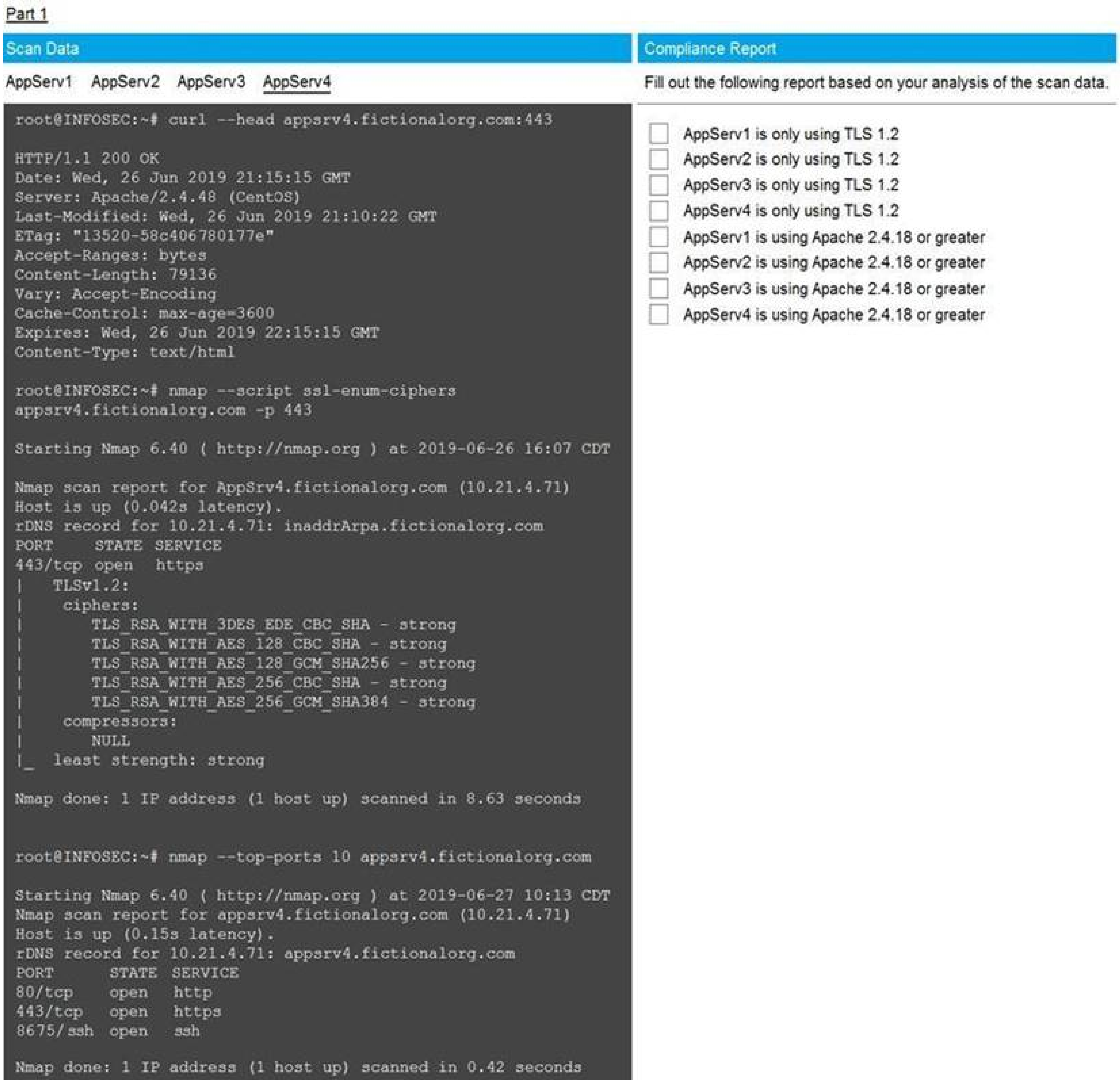
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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



Part 1

Scan Data

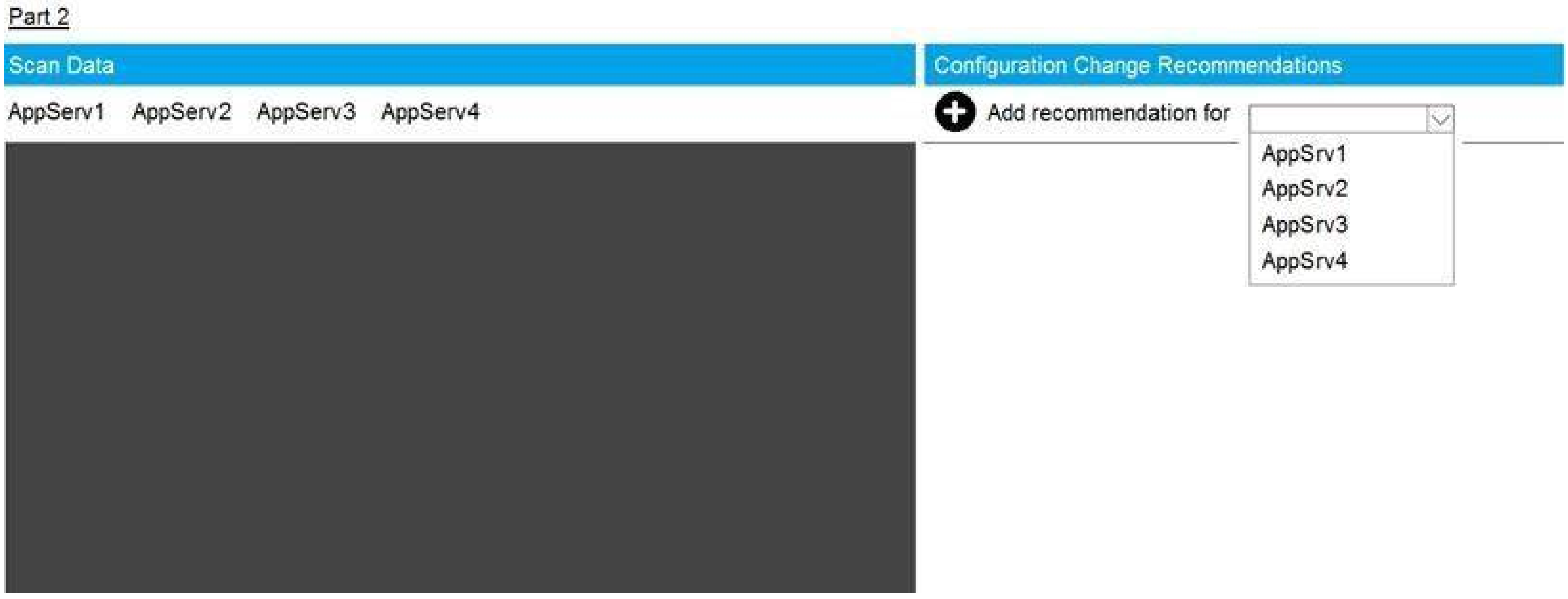
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

Compliance Report

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

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



Part 2

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

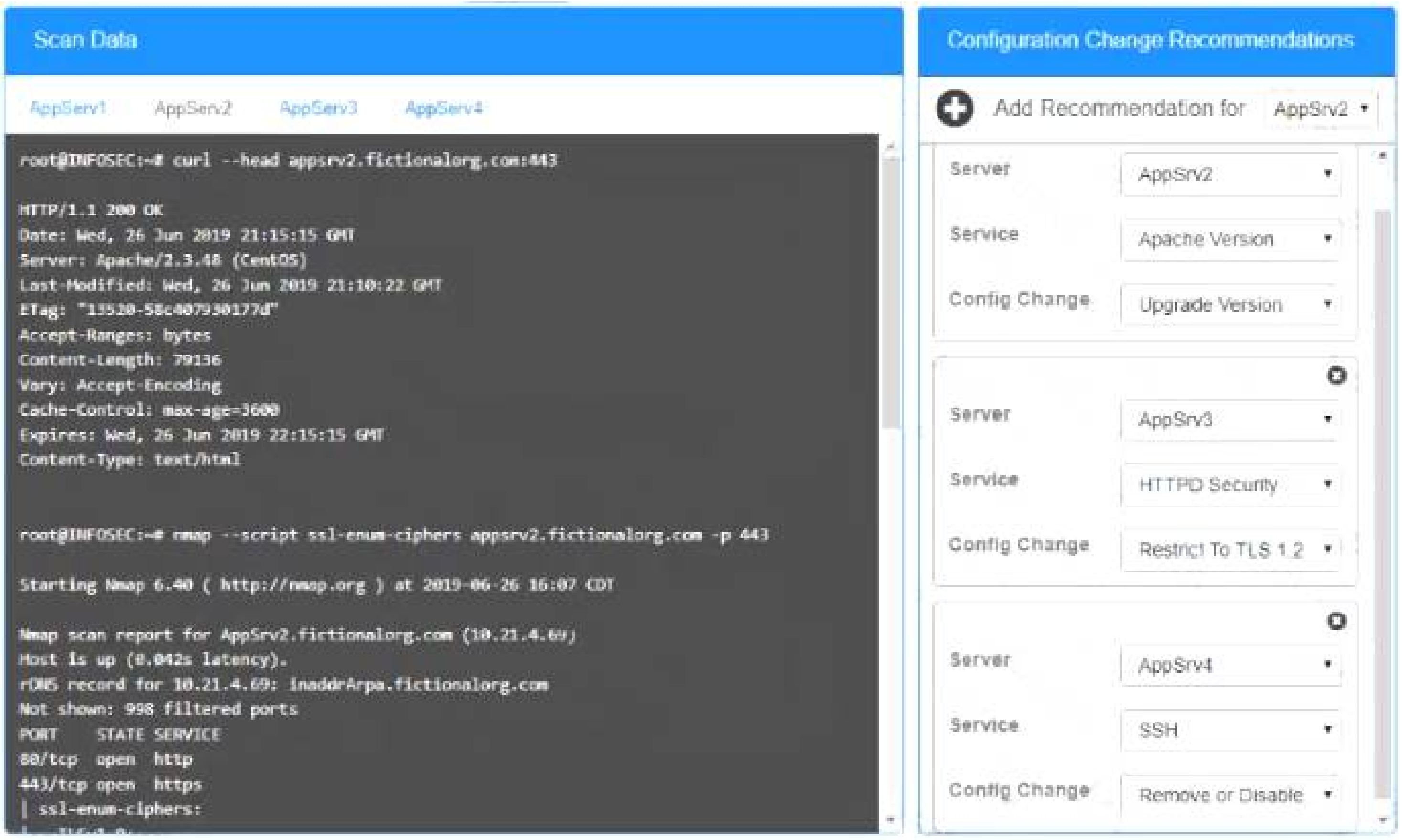
Configuration Change Recommendations

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


Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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


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

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
```

Configuration Change Recommendations

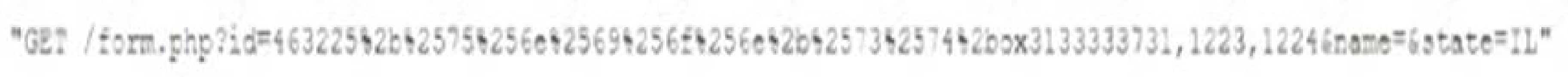
Add Recommendation for AppSrv2

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 98
- (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

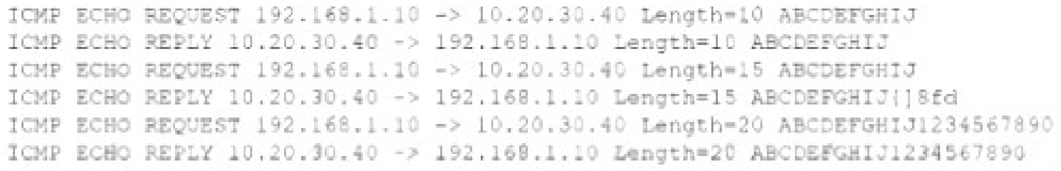
Answer: D

NEW QUESTION 102
- (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 105
- (Exam Topic 3)
An analyst is reviewing the following output as part of an incident:


```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ[]8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

Which of the Wowing is MOST likely happening?

A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20 30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.

Answer: C

NEW QUESTION 108
- (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 110
- (Exam Topic 2)
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

A. Focus on incidents that may require law enforcement support.
B. Focus on common attack vectors first.
C. Focus on incidents that have a high chance of reputation harm.
D. Focus on incidents that affect critical systems.

Answer: D

NEW QUESTION 114
- (Exam Topic 2)
During an investigation, an analyst discovers the following rule in an executive's email client: IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>
The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

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

Answer: A

NEW QUESTION 118
- (Exam Topic 2)
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Create a WAF rule In block mode for SQL injection
D. Ask the developers to implement parameterized SQL queries.

Answer: A

NEW QUESTION 120
- (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 123
- (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 127
- (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.

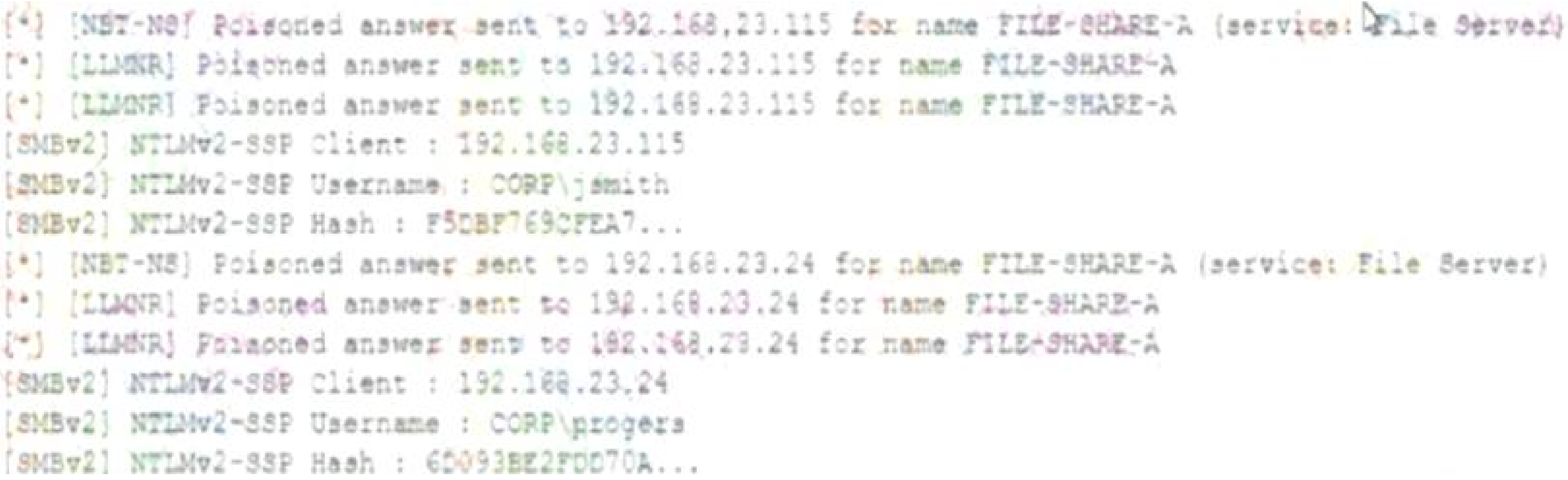
Answer: D

NEW QUESTION 128
- (Exam Topic 2)
A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?

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

Answer: A

NEW QUESTION 131
- (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 136
- (Exam Topic 2)
While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further

compromise? (Select TWO).

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

Answer: CE

NEW QUESTION 139
- (Exam Topic 2)
A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

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

Answer: D

NEW QUESTION 144
- (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 148
- (Exam Topic 2)
An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

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

Answer: D

NEW QUESTION 151
- (Exam Topic 2)
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

A. Input validation
B. Output encoding
C. Parameterized queries
D. Tokenization

Answer: D

NEW QUESTION 156
- (Exam Topic 2)
A company is moving from the use of web servers hosted in an internal datacenter to a containerized cloud platform. An analyst has been asked to identify indicators of compromise in the containerized environment. Which of the following would BEST indicate a running container has been compromised?

A. A container from an approved software image has drifted
B. An approved software orchestration container is running with root privileges
C. A container from an approved software image has stopped responding
D. A container from an approved software image fails to start

Answer: A

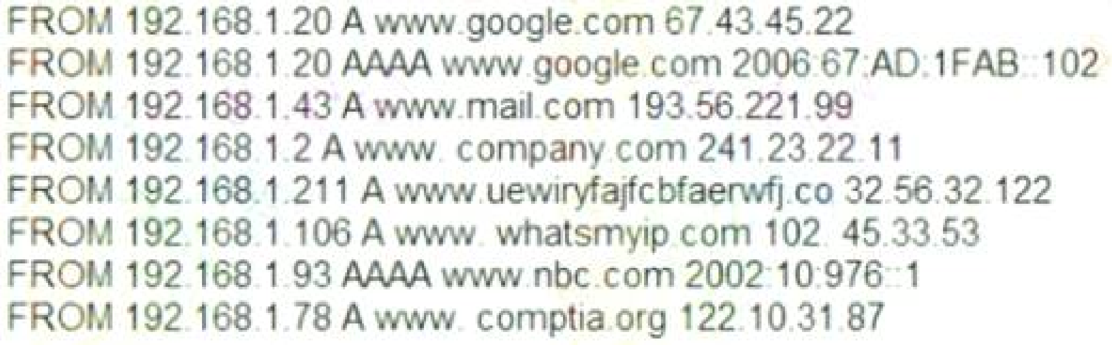
NEW QUESTION 159
- (Exam Topic 2)
An analyst needs to provide recommendations for the AUP Which of the following is the BEST recommendation to protect the company's intellectual property?

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. All Internet access must be via a proxy server.

Answer: D

NEW QUESTION 164
- (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 165
- (Exam Topic 2)
The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded
and has revealed a worm is spreading
Which of the following should be the NEXT step in this incident response?

A. Enable an ACL on all VLANs to contain each segment
B. Compile a list of loCs so the IPS can be updated to halt the spread.
C. Send a sample of the malware to the antivirus vendor and request urgent signature creation.
D. Begin deploying the new anti-malware on all uninfected systems.

Answer: A

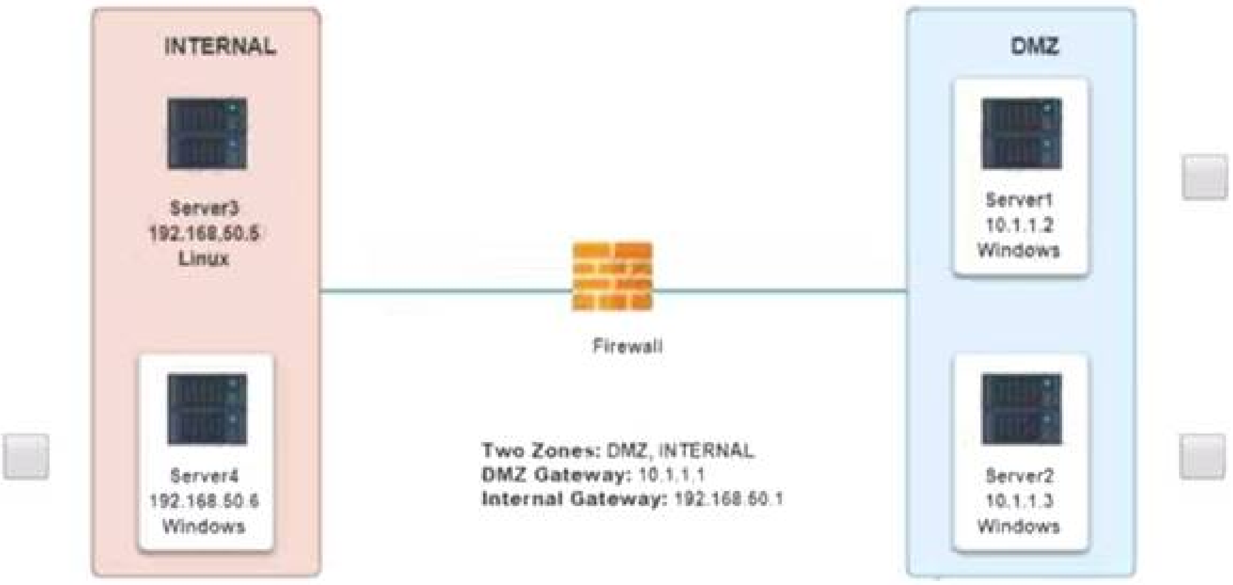
NEW QUESTION 168
- (Exam Topic 2)
An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

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

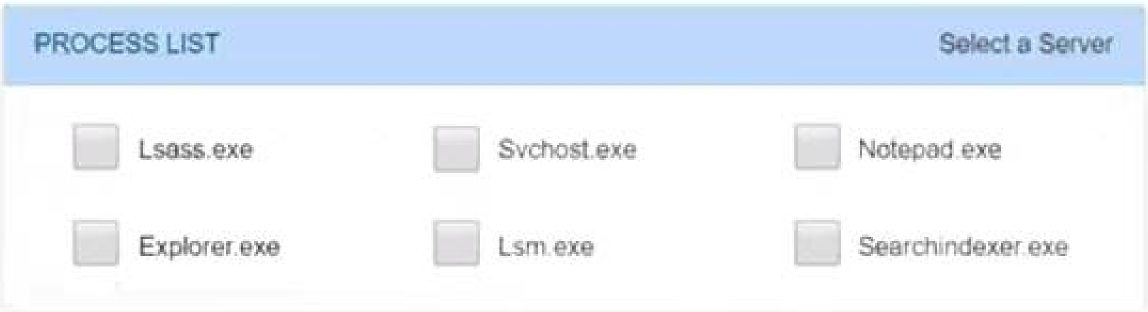
Answer: C

NEW QUESTION 171
- (Exam Topic 2)
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.
INSTRUCTIONS
Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram for Company A



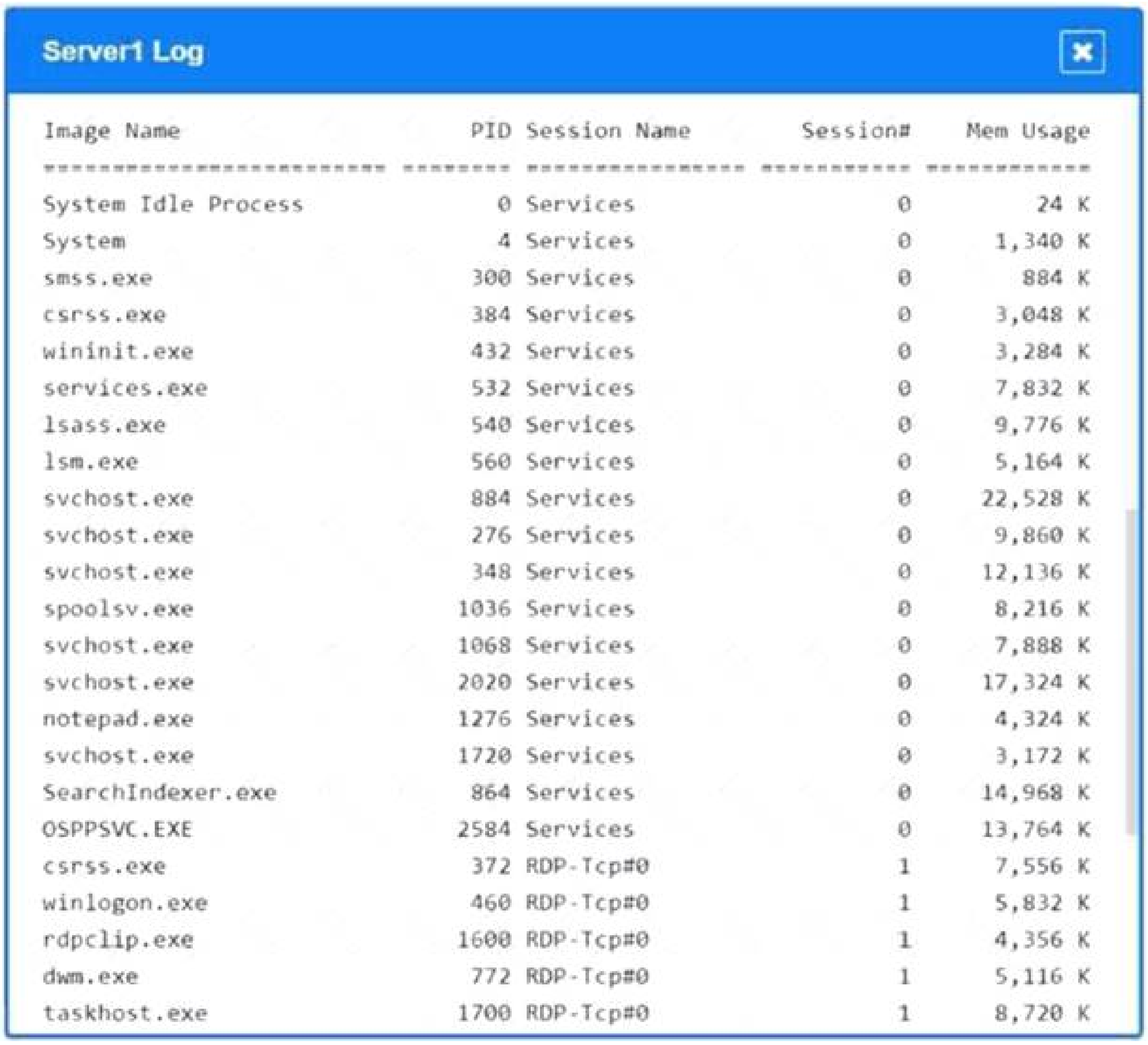
Two Zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
Internal Gateway: 192.168.50.1



PROCESS LIST   Select a Server

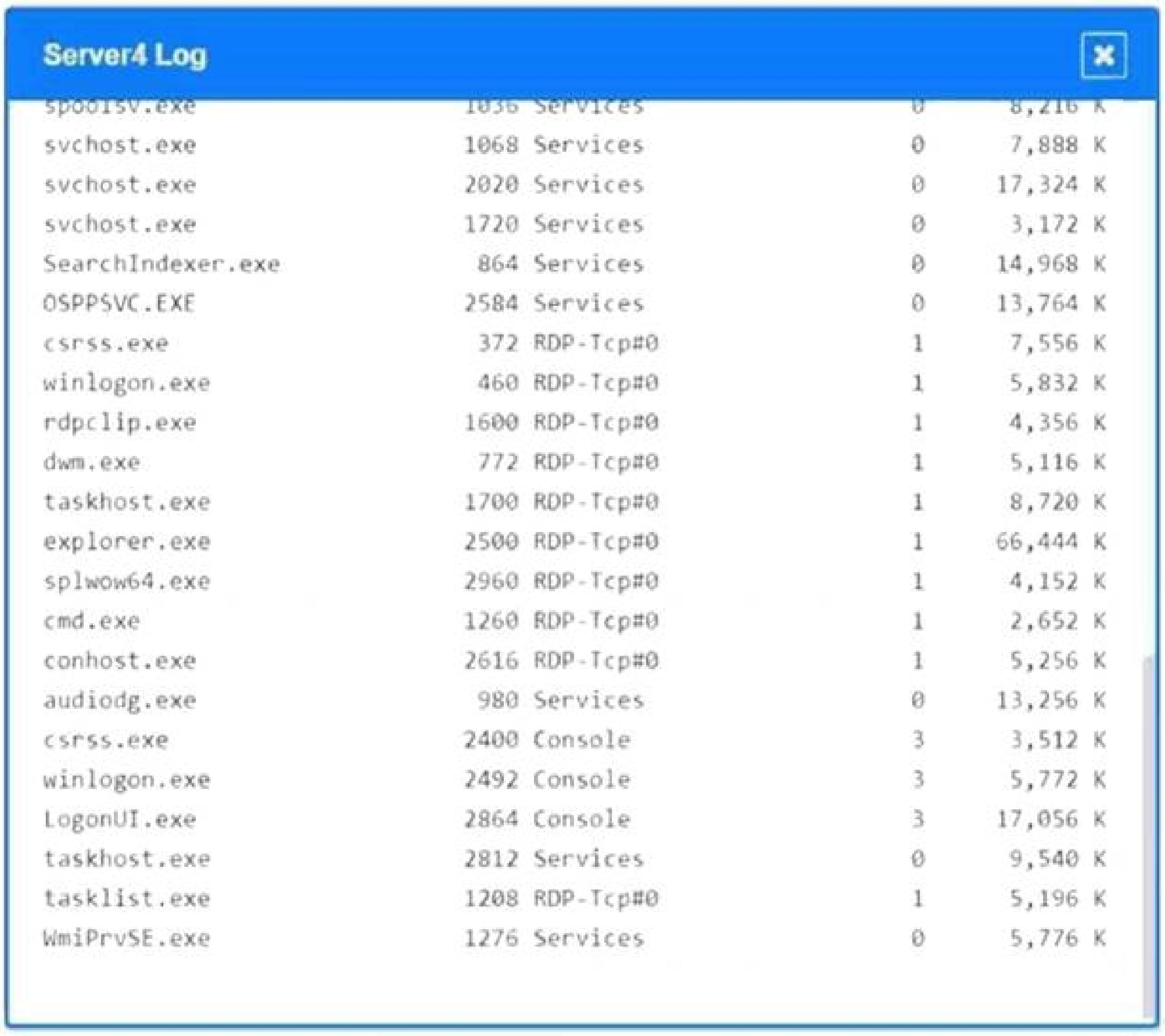
□ Lsass.exe   □ Svchost.exe   □ Notepad.exe

□ Explorer.exe   □ Lsm.exe   □ Searchindexer.exe



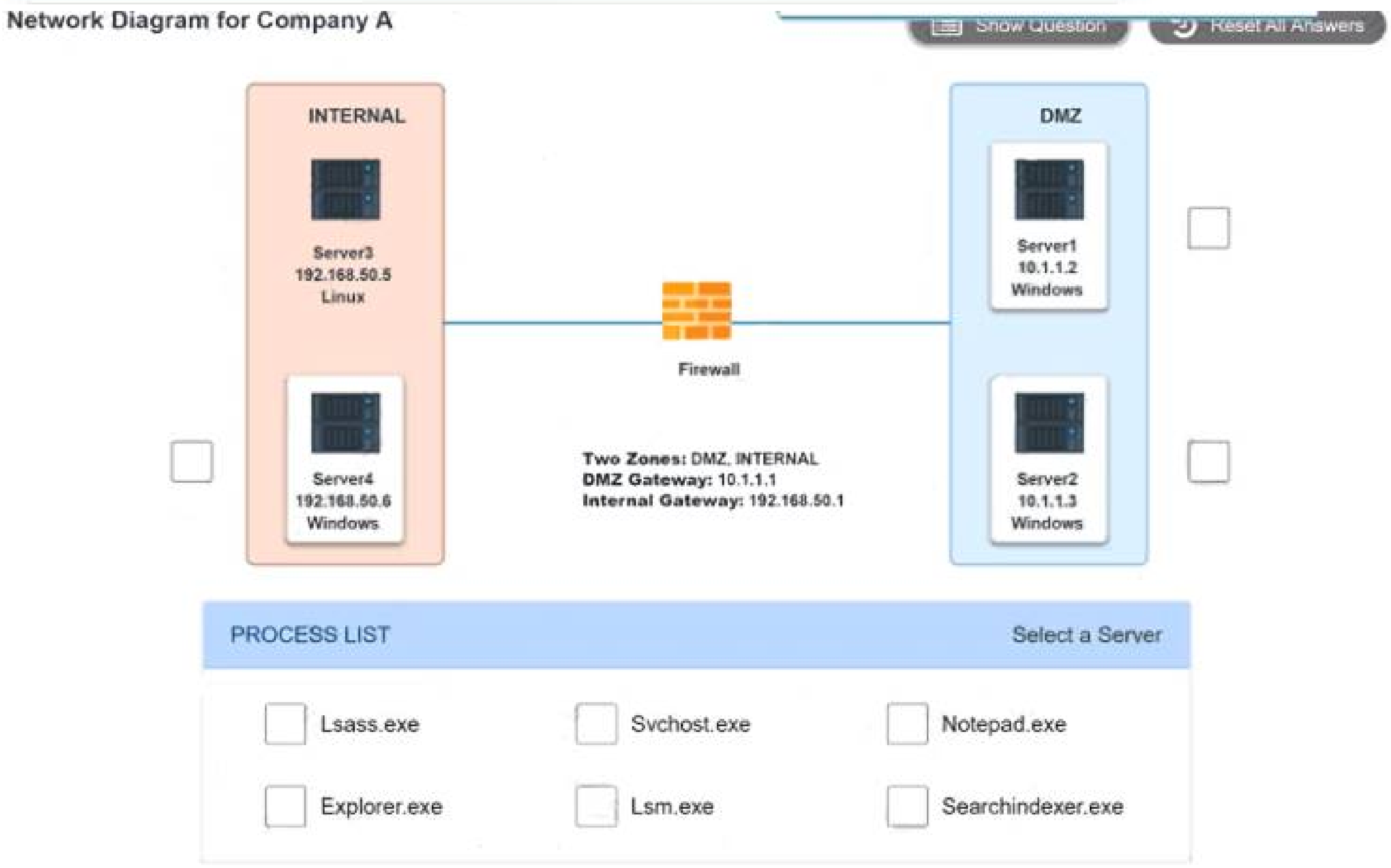
Server1 Log ☒

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



Server4 Log

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



Network Diagram for Company A

Two Zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
Internal Gateway: 192.168.50.1

PROCESS LIST

Select a Server

□ Lsass.exe □ Svchost.exe □ Notepad.exe
□ Explorer.exe □ Lsm.exe □ Searchindexer.exe

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server 4 192.168.50.6 Windows, svchost.exe

NEW QUESTION 174
- (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 175
- (Exam Topic 2)
A company has contracted with a software development vendor to design a web portal for customers to access a medical records database. Which of the following should the security analyst recommend to BEST control the unauthorized disclosure of sensitive data when sharing the development database with the vendor?

A. Establish an NDA with the vendor.
B. Enable data masking of sensitive data tables in the database.
C. Set all database tables to read only.
D. Use a de-identified data process for the development database.

Answer: D

Explanation:
https://privacy-analytics.com/resources/videos/what-is-the-difference-between-data-masking-de-identification-a

NEW QUESTION 180
- (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 181
- (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 184
- (Exam Topic 2)
The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device
mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

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

Answer: A

NEW QUESTION 185
- (Exam Topic 2)
Which of the following is MOST closely related to the concept of privacy?

A. An individual's control over personal information
B. A policy implementing strong identity management processes
C. A system's ability to protect the confidentiality of sensitive information
D. The implementation of confidentiality, integrity, and availability

Answer: A

Explanation:
"Privacy refers to whatever control you have over your personal information and how it is utilized."

NEW QUESTION 187
- (Exam Topic 2)
While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?

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

Answer: A

NEW QUESTION 191
- (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 195
- (Exam Topic 2)
Employees of a large financial company are continuously being Infected by strands of malware that are not detected by EDR tools. When of the following Is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

A. MFA on the workstations
B. Additional host firewall rules
C. VDI environment
D. Hard drive encryption
E. Network access control
F. Network segmentation

Answer: C

NEW QUESTION 196
- (Exam Topic 2)
Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?

A. Configuring a firewall to block traffic on ports that use ActiveX controls
B. Adjusting the web-browser settings to block ActiveX controls
C. Installing network-based IPS to block malicious ActiveX code
D. Deploying HIPS to block malicious ActiveX code

Answer: B

NEW QUESTION 200
- (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.

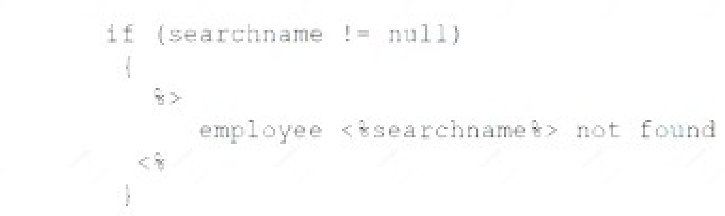
Answer: D

NEW QUESTION 204
- (Exam Topic 2)
A user reports a malware alert to the help desk A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?

A. Document the procedures and walk through the incident training guide.
B. Sanitize the workstation and verify countermeasures are restored
C. Reverse engineer the malware to determine its purpose and risk to the organization.
D. Isolate the workstation and issue a new computer to the user.

Answer: B

NEW QUESTION 206
- (Exam Topic 2)
An analyst is reviewing the following output:



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

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

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

Answer: C

NEW QUESTION 207
- (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 212
- (Exam Topic 2)
Which of the following technologies can be used to store digital certificates and is typically used in highsecurity implementations where integrity is paramount?

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

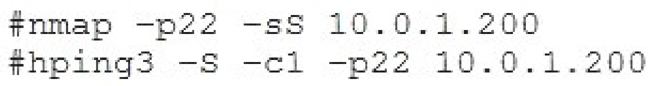
Answer: A

NEW QUESTION 216
- (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 221
- (Exam Topic 2)
A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall’s behavior and responses. The analyst executes the following commands:



```
#nmap -p22 -sS 10.0.1.200
#hping3 -S -c1 -p22 10.0.1.200
```

The analyst then compares the following results for port 22: nmap returns “Closed”
hping3 returns “flags=RA”
Which of the following BEST describes the firewall rule?

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

Answer: B

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

NEW QUESTION 226
- (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 227
- (Exam Topic 2)
Which of the following data security controls would work BEST to prevent real Pll from being used in an organization's test cloud environment?

A. Digital rights management
B. Encryption
C. Access control
D. Data loss prevention
E. Data masking

Answer: E

Explanation:
Data masking is a way to create a fake, but a realistic version of your organizational data. The goal is to protect sensitive data, while providing a functional alternative when real data is not needed—for example, in user training, sales demos, or software testing.

NEW QUESTION 229
- (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 231
- (Exam Topic 2)
In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. Burp Suite
C. OWASP ZAP
D. Unauthenticated

Answer: D

NEW QUESTION 233
- (Exam Topic 2)
A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

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

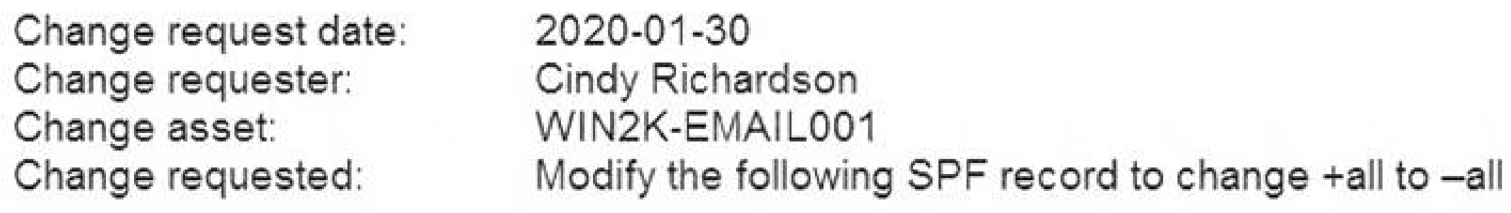
Answer: D

NEW QUESTION 238
- (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 243
- (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 245
- (Exam Topic 2)
A critical server was compromised by malware, and all functionality was lost. Backups of this server were taken; however, management believes a logic bomb may have been injected by a rootkit. Which of the following should a security analyst perform to restore functionality quickly?

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

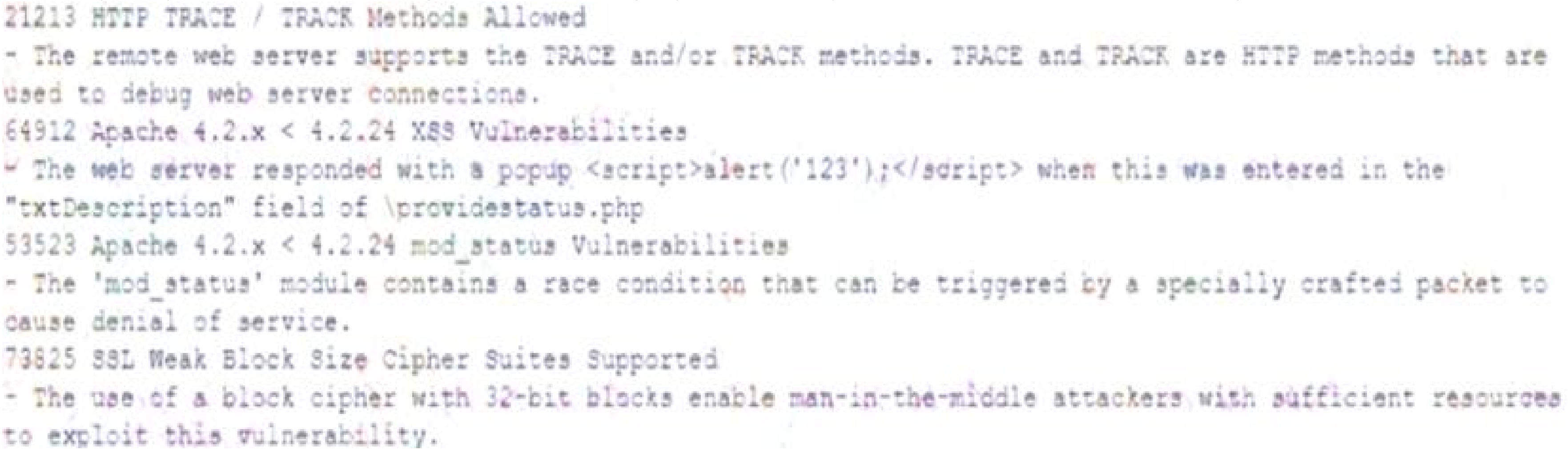
Answer: B

NEW QUESTION 248
- (Exam Topic 2)
A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:
> dig domain._domainkey.comptia.orq TXT
Which of the following email protection technologies is the analyst MOST likely validating?

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

Answer: A

NEW QUESTION 253
- (Exam Topic 2)
A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:



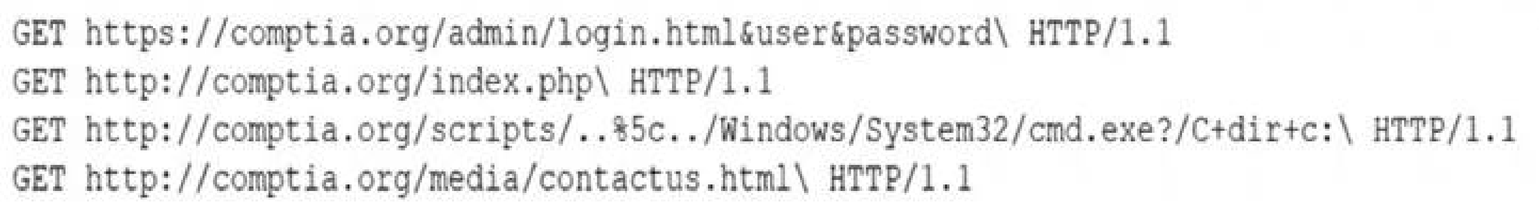
```
21213 HTTP TRACE / TRACK Methods Allowed
- The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are
used to debug web server connections.
64912 Apache 4.2.x < 4.2.24 XSS Vulnerabilities
- The web server responded with a popup <script>alert('123');</script> 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 257
- (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 259
- (Exam Topic 2)
Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

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

Answer: A

NEW QUESTION 262
- (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

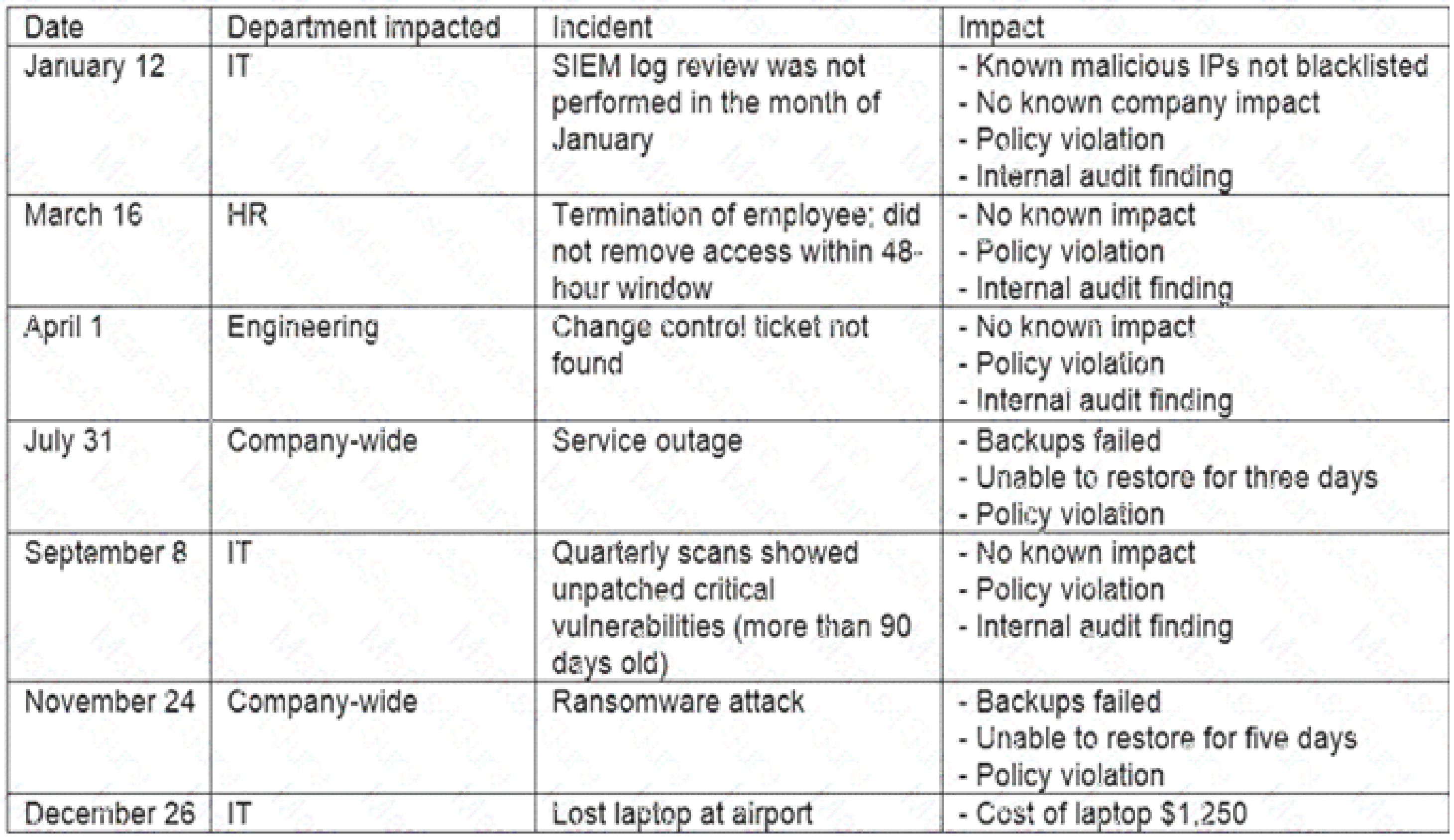
Answer: A

NEW QUESTION 264
- (Exam Topic 2)
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

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

Answer: B

NEW QUESTION 269
- (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 270
- (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 271
- (Exam Topic 2)
A security analyst needs to perform a search for connections with a suspicious IP on the network traffic. The company collects full packet captures at the Internet gateway and retains them for one week. Which of the following will enable the analyst to obtain the BEST results?

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

Answer: A

NEW QUESTION 275
- (Exam Topic 2)
A company's blocklist has outgrown the current technologies in place. The ACLS are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures.
Which of the following configuration changes to the existing controls would be the MOST appropriate to
improve performance?

A. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.
B. Implement a host-file based solution that will use a list of all domains to deny for all machines on the network
C. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.
D. Review the current blocklist and prioritize it based on the level of threat severit
E. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.

Answer: C

NEW QUESTION 278
- (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 279
- (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 283
- (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 287
- (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 288
- (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 293
- (Exam Topic 2)
A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

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

Answer: B

NEW QUESTION 297
- (Exam Topic 2)
A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute

forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

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

Answer: C

NEW QUESTION 300
- (Exam Topic 1)
A security analyst is providing a risk assessment for a medical device that will be installed on the corporate
network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk- based policy decision to review and enforce the vendor upgrade before the end of life is reached. Which of the following risk actions has the security committee taken?

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

Answer: D

NEW QUESTION 303
- (Exam Topic 1)
A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentially protection. Which of the following is the BEST technical security control to mitigate this risk?

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

Answer: D

NEW QUESTION 307
- (Exam Topic 1)
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

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

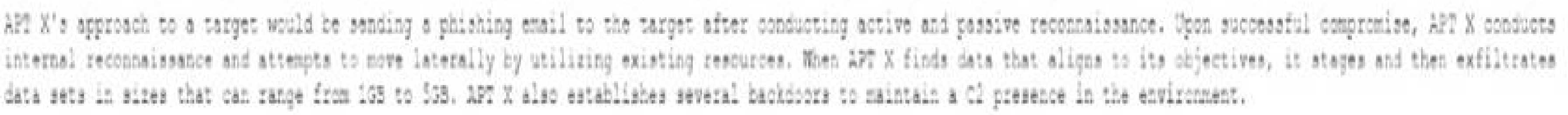
Answer: C

NEW QUESTION 310
- (Exam Topic 1)
Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

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

Answer: A

NEW QUESTION 315
- (Exam Topic 1)
A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:



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

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

A. Data collection/exfiltration
B. Defensive evasion
C. Lateral movement
D. Reconnaissance

Answer: A

NEW QUESTION 316
- (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 320
- (Exam Topic 1)
A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.
Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

A. Attack vectors
B. Adversary capability
C. Diamond Model of Intrusion Analysis
D. Kill chain
E. Total attack surface

Answer: B

Explanation:
Reference: https://www.secureworks.com/blog/advanced-persistent-threats-apt-b

NEW QUESTION 323
- (Exam Topic 1)
A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

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

Answer: B

NEW QUESTION 326
- (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 331
- (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 332
- (Exam Topic 1)
A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.
Which of the following is the BEST mitigation to prevent unauthorized access?

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

Answer: C

NEW QUESTION 334
- (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

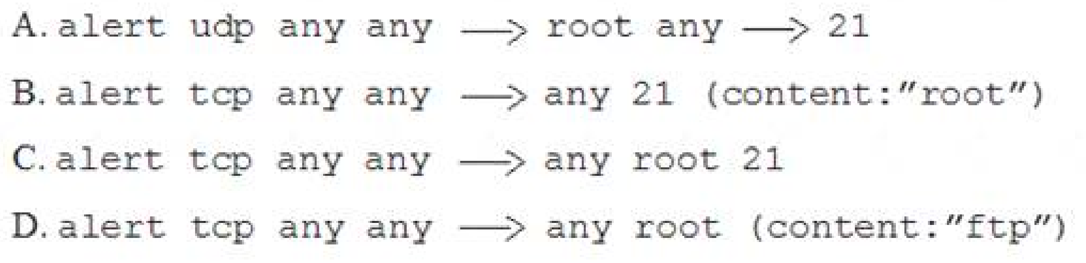
Answer: D

NEW QUESTION 336
- (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 337
- (Exam Topic 1)
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

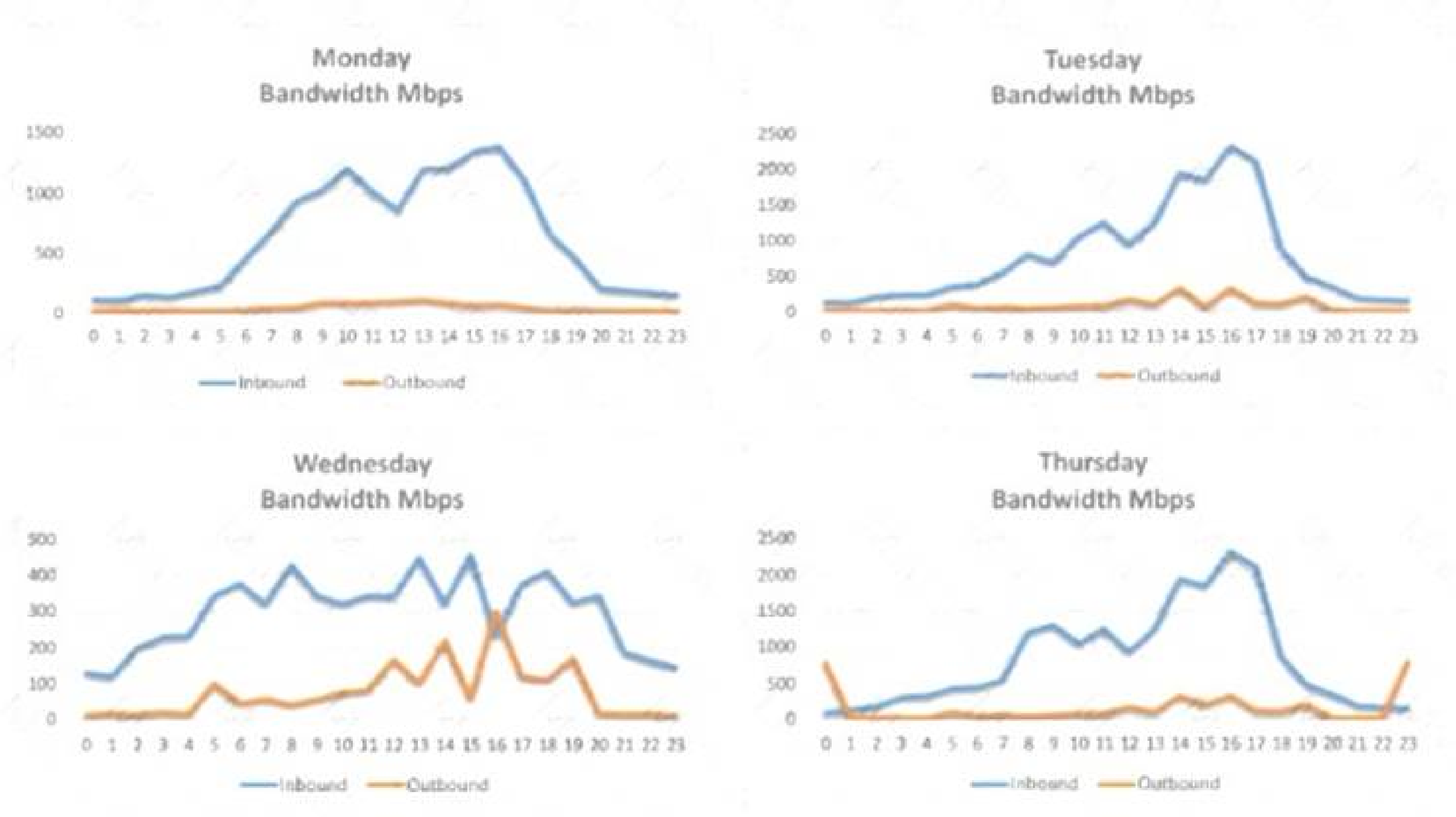


```
A. alert udp any any  ⟶ root any ⟶ 21
B. alert tcp any any  ⟶ any 21 (content:"root")
C. alert tcp any any  ⟶ any root 21
D. alert tcp any any  ⟶ any root (content:"ftp")
```

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

Answer: B

NEW QUESTION 339
- (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 344
- (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 346
- (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 351
- (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 353
- (Exam Topic 1)
An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?

A. DLP
B. Encryption
C. Data masking
D. SPF

Answer: A

NEW QUESTION 356
- (Exam Topic 1)
Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

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

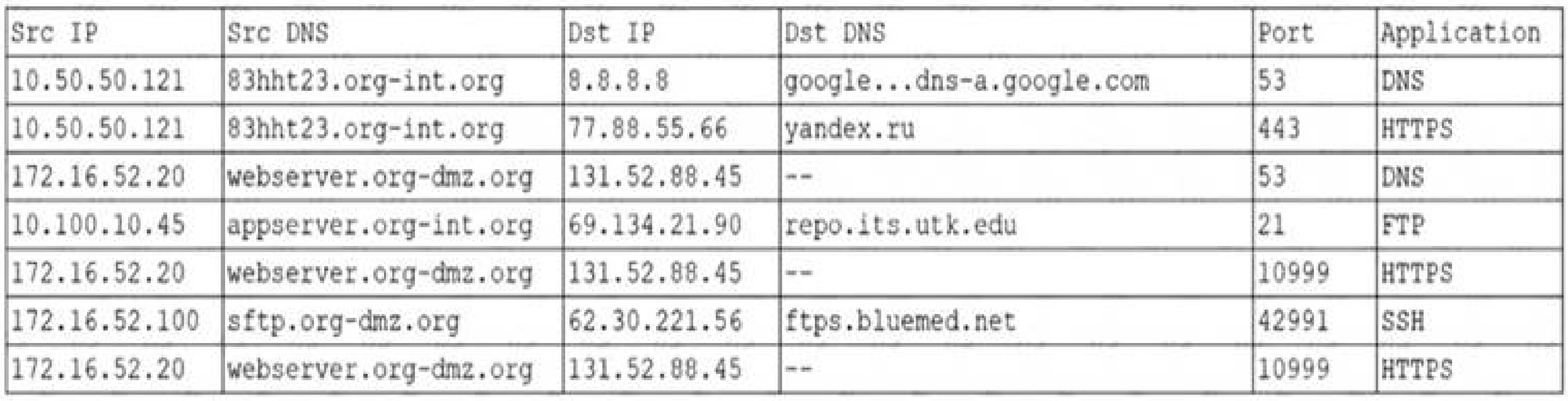
Answer: A

NEW QUESTION 361
- (Exam Topic 1)
An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

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

Answer: C

NEW QUESTION 366
- (Exam Topic 1)
An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:



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

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

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

Answer: A

NEW QUESTION 368
- (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 370
- (Exam Topic 1)
Which of the following should be found within an organization's acceptable use policy?

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

Answer: D

NEW QUESTION 375
- (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 376
- (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 380
- (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 383
- (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 385
- (Exam Topic 1)
Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/ "><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance "></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body>< 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe 192.168.5.66 - - api.somesite.com 200 0 1378 1209
48 192.168.4.89
```

Which of the following MOST likely explains how the clients' accounts were compromised?

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

Answer: B

NEW QUESTION 390
- (Exam Topic 1)
A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.
Which of the following should be done to correct the cause of the vulnerability?

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

Answer: B

NEW QUESTION 392
- (Exam Topic 1)
Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

A. Parameterized queries
B. Session management

C. Input validation
D. Output encoding
E. Data protection
F. Authentication

Answer: AC

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

NEW QUESTION 397
- (Exam Topic 1)
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

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

Answer: B

NEW QUESTION 398
- (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

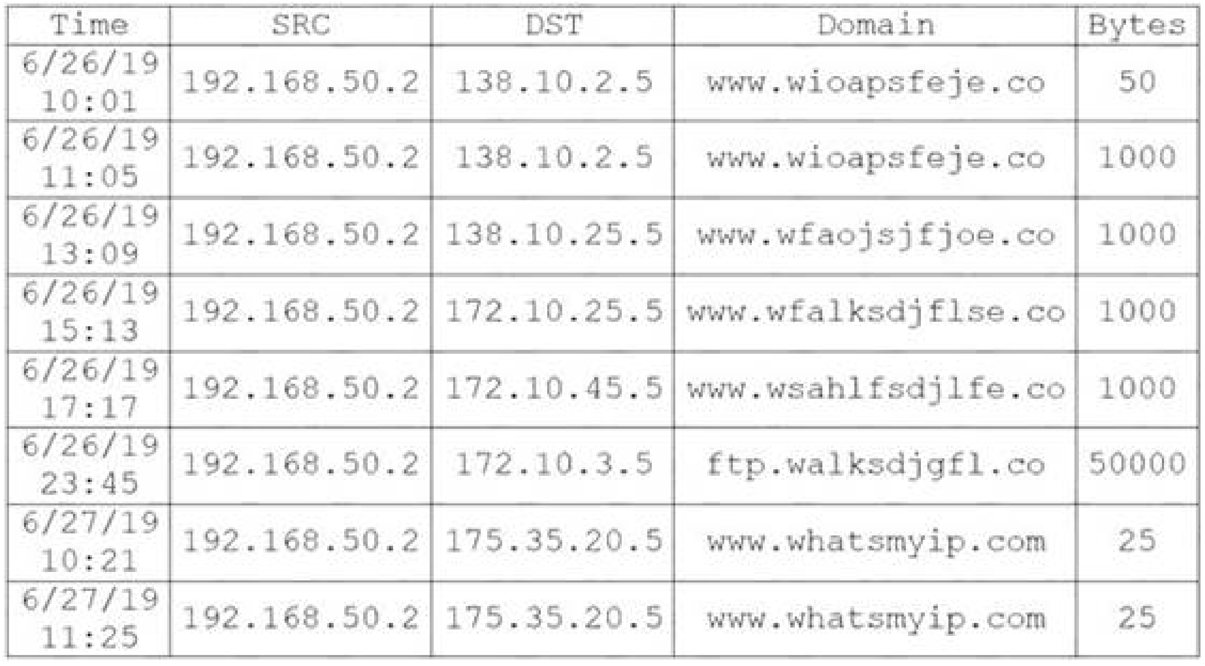
Explanation:
Reference: https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting

NEW QUESTION 401
- (Exam Topic 1)
A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

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

Answer: D

NEW QUESTION 406
- (Exam Topic 1)
During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:



Time	SRC	DST	Domain	Bytes
6/26/19 10:01	192.168.50.2	138.10.2.5	www.wioapsfeje.co	50
6/26/19 11:05	192.168.50.2	138.10.2.5	www.wioapsfeje.co	1000
6/26/19 13:09	192.168.50.2	138.10.25.5	www.wfaojsjfjoe.co	1000
6/26/19 15:13	192.168.50.2	172.10.25.5	www.wfalksdjflse.co	1000
6/26/19 17:17	192.168.50.2	172.10.45.5	www.wsahlfsdjlfe.co	1000
6/26/19 23:45	192.168.50.2	172.10.3.5	ftp.walksdjgfl.co	50000
6/27/19 10:21	192.168.50.2	175.35.20.5	www.whatsmyip.com	25
6/27/19 11:25	192.168.50.2	175.35.20.5	www.whatsmyip.com	25

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.

E. DST 175.35.20.5.

Answer: A

NEW QUESTION 411
- (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 414
- (Exam Topic 1)
A security analyst implemented a solution that would analyze the attacks that the organization’s firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.
S sudo nc -1 -v -c maildemon . py 25 caplog, txt
Which of the following solutions did the analyst implement?

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

Answer: A

NEW QUESTION 418
- (Exam Topic 1)
A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?

A. Insider threat
B. Buffer overflow
C. Advanced persistent threat
D. Zero day

Answer: D

NEW QUESTION 422
- (Exam Topic 1)
A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.
Which of the following is the BEST example of the level of sophistication this threat actor is using?

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

Answer: B

NEW QUESTION 426
- (Exam Topic 1)
A web developer wants to create a new web part within the company website that aggregates sales from individual team sites. A cybersecurity analyst wants to ensure security measurements are implemented during this process. Which of the following remediation actions should the analyst take to implement a vulnerability management process?

A. Personnel training
B. Vulnerability scan
C. Change management
D. Sandboxing

Answer: C

NEW QUESTION 428
- (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 432
- (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 436
- (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 440
- (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

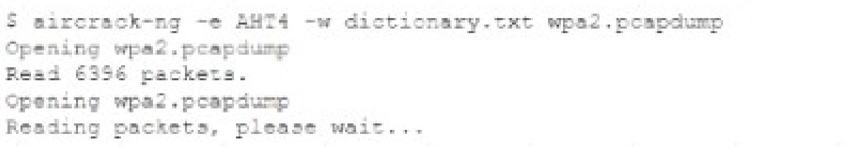
Explanation:
Reference: https://blog.finjan.com/email-spoofing/

NEW QUESTION 441
- (Exam Topic 1)
A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.
Which of the following should be done to prevent this issue from reoccurring?

A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Answer: A

NEW QUESTION 443
- (Exam Topic 1)
The help desk provided a security analyst with a screenshot of a user's desktop:



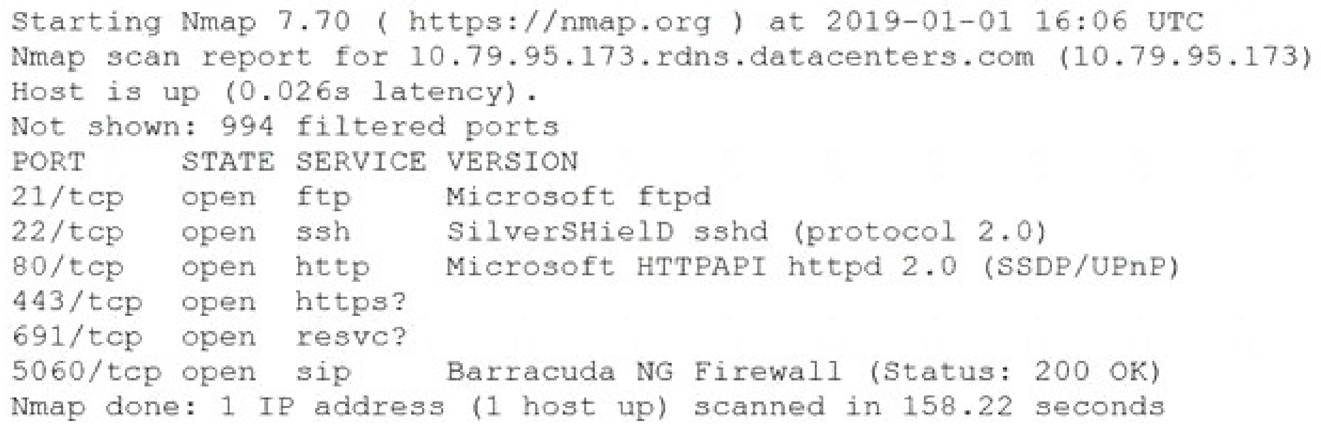
```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

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 444
- (Exam Topic 1)
An information security analyst is compiling data from a recent penetration test and reviews the following output:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
22/tcp   open  ssh     SilverSHielD sshd (protocol 2.0)
80/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  https?
691/tcp  open  resvc?
5060/tcp open  sip     Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would MOST likely provide the needed information?

A. ping -t 10.79.95.173.rdns.datacenters.com
B. telnet 10.79.95.173 443
C. ftpd 10.79.95.173.rdns.datacenters.com 443
D. tracert 10.79.95.173

Answer: B

NEW QUESTION 446
- (Exam Topic 1)
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

A. Data custodian
B. Data owner
C. Data processor
D. Senior management

Answer: B

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

NEW QUESTION 450
- (Exam Topic 1)
For machine learning to be applied effectively toward security analysis automation, it requires.

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

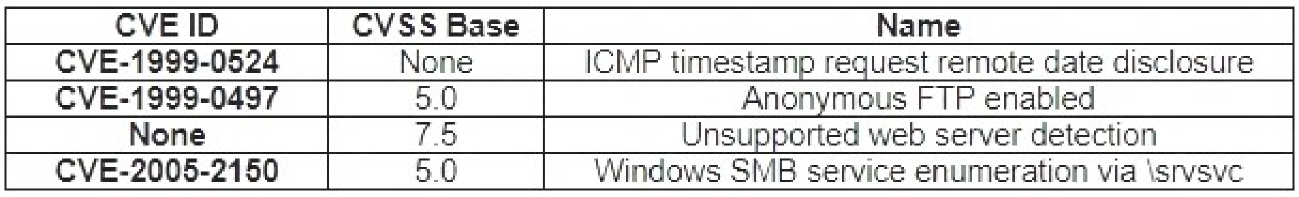
Answer: A

NEW QUESTION 451
- (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 453
- (Exam Topic 1)
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:



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

Which of the following is MOST likely a false positive?

A. ICMP timestamp request remote date disclosure
B. Windows SMB service enumeration via \srvsvc

C. Anonymous FTP enabled
D. Unsupported web server detection

Answer: B

NEW QUESTION 457
- (Exam Topic 1)
An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.
Which of the following should be considered FIRST prior to disposing of the electronic data?

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

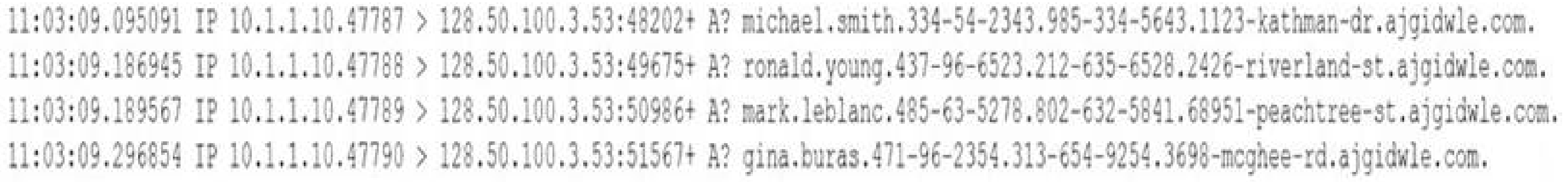
Answer: D

NEW QUESTION 459
- (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 462
- (Exam Topic 1)
A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:



```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

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

Answer: D

NEW QUESTION 464
- (Exam Topic 1)
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

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

Answer: B

NEW QUESTION 469
- (Exam Topic 1)
A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?

A. Shut down the computer
B. Capture live data using Wireshark
C. Take a snapshot
D. Determine if DNS logging is enabled.
E. Review the network logs.

Answer: D

Explanation:
The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be

gathered using packet capture tools such as network monitor.
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn80066

NEW QUESTION 472
- (Exam Topic 1)
Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

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

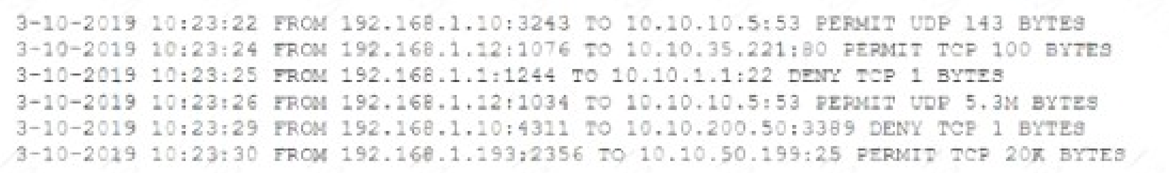
Answer: C

NEW QUESTION 477
- (Exam Topic 1)
A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two
compromised devices.
Which of the following should be used to identify the traffic?

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

Answer: C

NEW QUESTION 478
- (Exam Topic 1)
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:



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

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

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

Answer: C

NEW QUESTION 482
- (Exam Topic 1)
A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.
To BEST mitigate this risk, the analyst should use.

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

Answer: C

NEW QUESTION 483
- (Exam Topic 1)
An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

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

Answer: D

NEW QUESTION 485
- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 489
- (Exam Topic 1)
A security analyst has discovered trial developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

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

Answer: A

NEW QUESTION 493
- (Exam Topic 3)
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

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

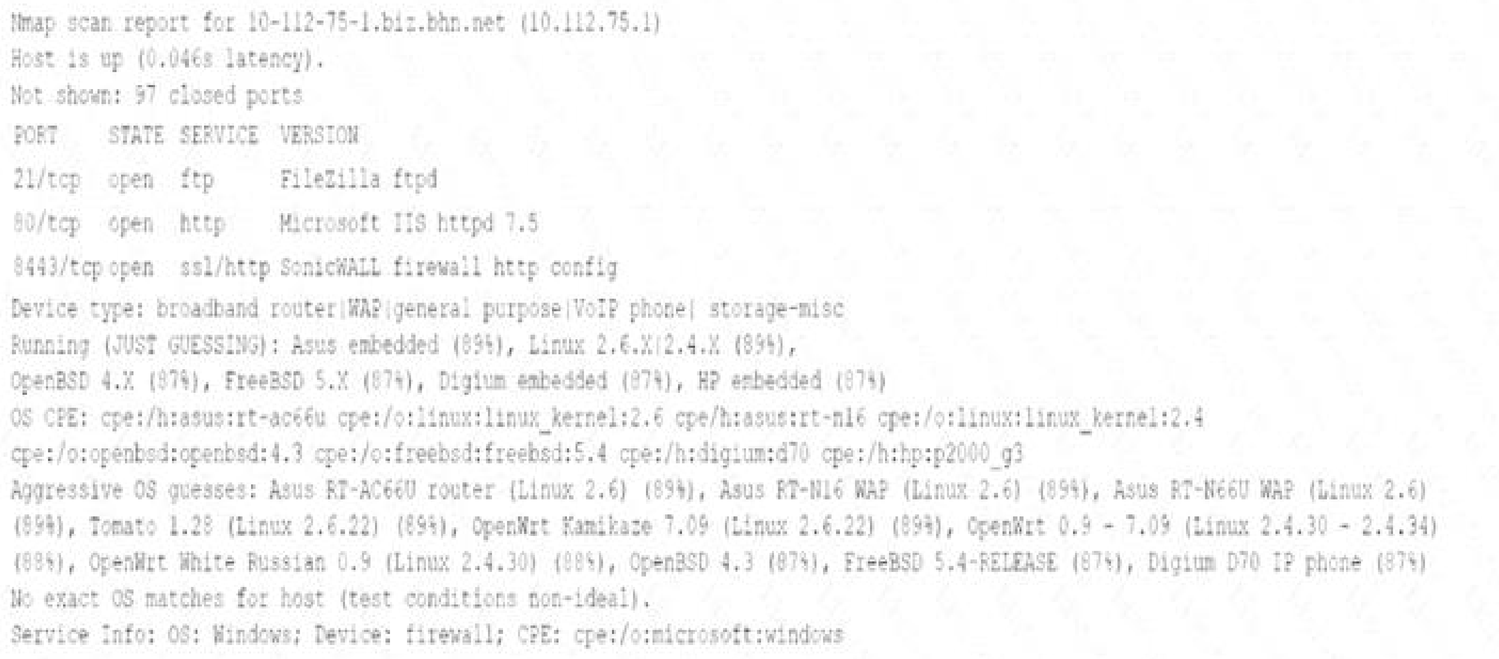
Answer: B

NEW QUESTION 498
- (Exam Topic 3)
Which of the following are considered PII by themselves? (Select TWO).

A. Government ID
B. Job title
C. Employment start date
D. Birth certificate
E. Employer address
F. Mother's maiden name

Answer: AD

NEW QUESTION 502
- (Exam Topic 3)
An analyst is reviewing the output from some recent network enumeration activities. The following entry relates to a target on the network:



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

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

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

Answer: A

NEW QUESTION 505
- (Exam Topic 3)
An organizational policy requires one person to input accounts payable and another to do accounts receivable.
A separate control requires one person to write a check and another person to sign all checks greater than
$5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?

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

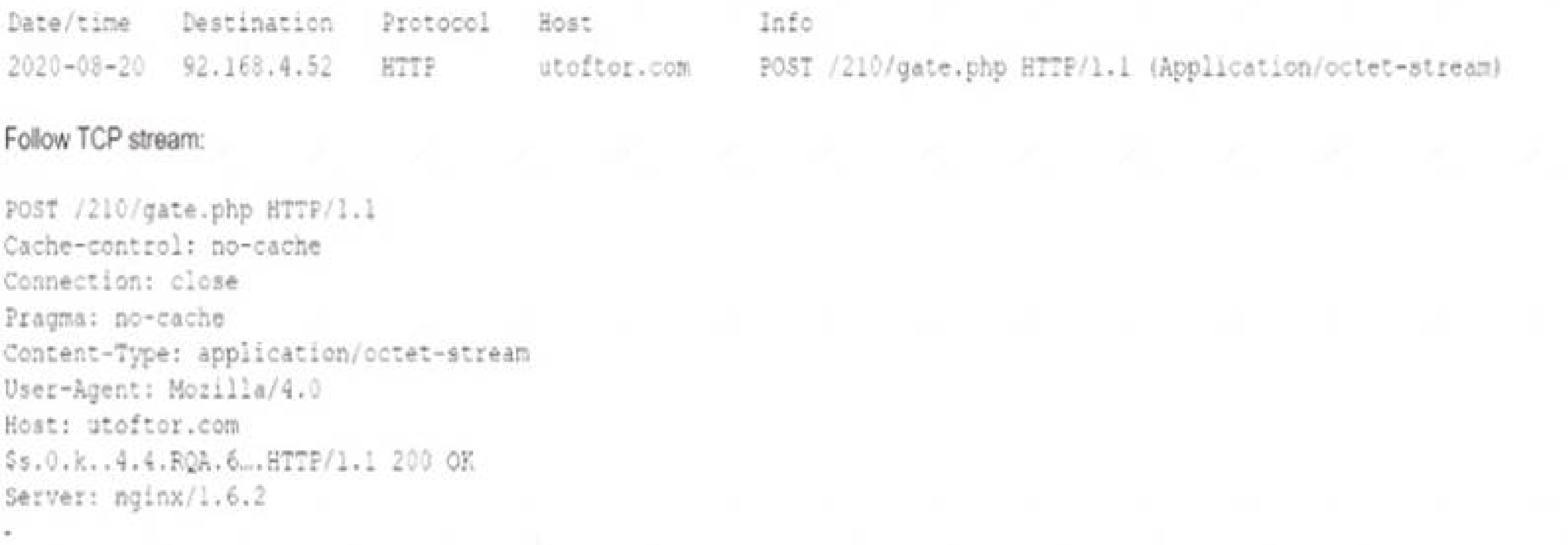
Answer: D

NEW QUESTION 506
- (Exam Topic 3)
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

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

Answer: EF

NEW QUESTION 510
- (Exam Topic 3)
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:



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

Follow TCP stream:

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

Which of the following describes what has occurred?

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

Answer: B

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

NEW QUESTION 514
- (Exam Topic 3)
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

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

Answer: A

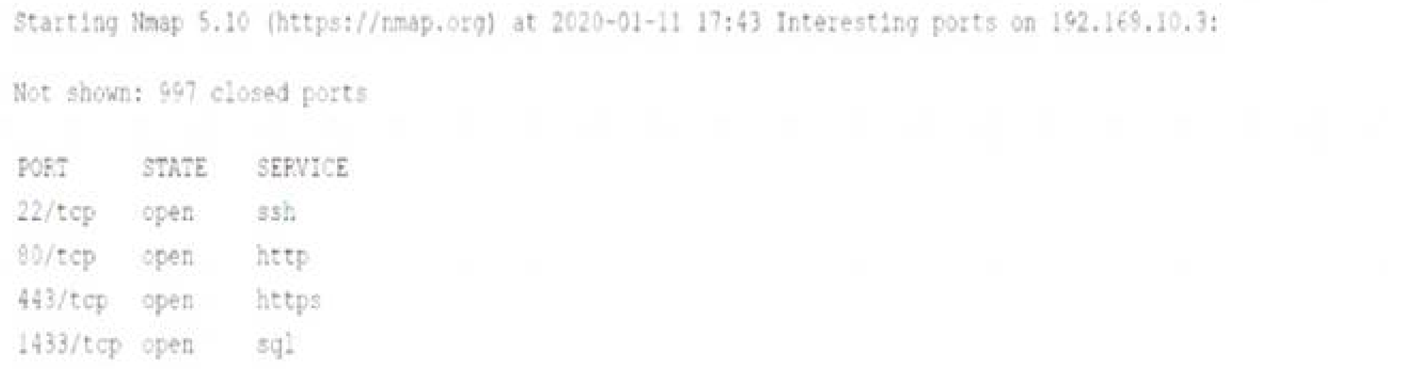
NEW QUESTION 519

- (Exam Topic 3)
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?

A. SIEM
B. IDS
C. MFA
D. TLS

Answer: C

NEW QUESTION 521
- (Exam Topic 3)
An organization has a policy that requires servers to be dedicated to one function and unneeded services to be disabled. Given the following output from an Nmap scan of a web server:



```
Starting Nmap 5.10 (https://nmap.org) at 2020-01-11 17:43 Interesting ports on 192.169.10.3:

Not shown: 997 closed ports

PORT      STATE   SERVICE
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    https
1433/tcp  open    sql
```

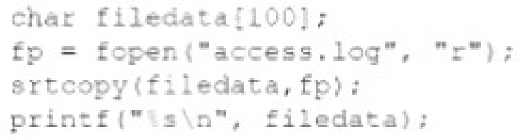
Which of the following ports should be closed?

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

Answer: D

Explanation:
"servers to be dedicated to one function..." http/s and SQL are two functions. I will select D, but agree with folks that the question is horribly written, and the person who wrote it was most likely drunk.

NEW QUESTION 524
- (Exam Topic 3)
An internally developed file-monitoring system identified the following except as causing a program to crash often:



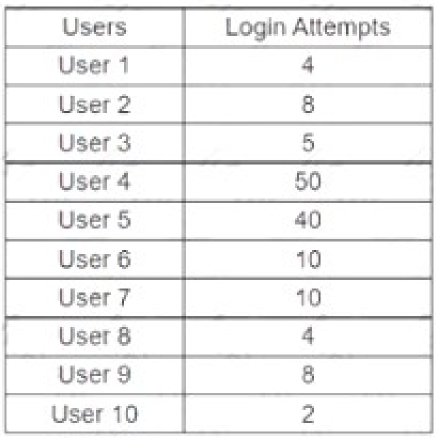
```
char filedata[100];
fp = fopen("access.log", "r");
srtcopy(filedata,fp);
printf("%s\n", filedata);
```

Which of the following should a security analyst recommend to fix the issue?

A. Open the access.log file ri read/write mode.
B. Replace the strcpv function.
C. Perform input samtizaton
D. Increase the size of the file data buffer

Answer: A

NEW QUESTION 526
- (Exam Topic 3)
A cybersecurity analyst routinely checks logs, querying for login attempts. While querying for unsuccessful login attempts during a five-day period, the analyst produces the following report:



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

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

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

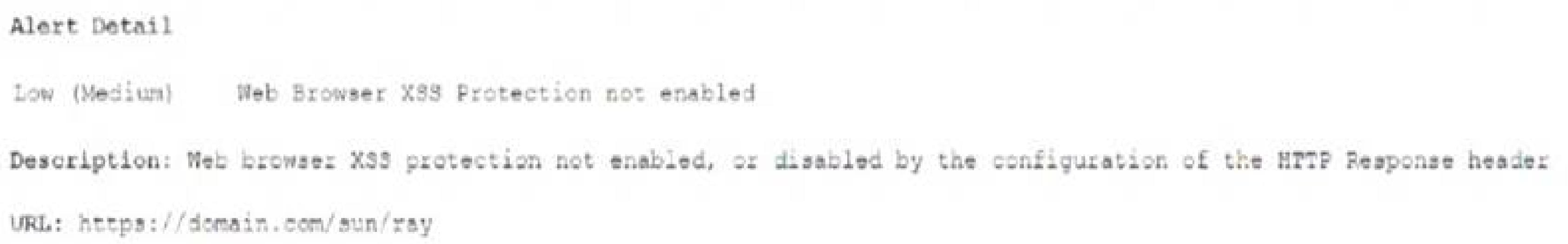
Answer: D

NEW QUESTION 530
- (Exam Topic 3)
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

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

Answer: C

NEW QUESTION 535
- (Exam Topic 3)
A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:



```
Alert Detail

Low (Medium)     Web Browser XSS Protection not enabled

Description: Web browser XSS protection not enabled, or disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray
```

Which of the following is the MOST likely solution to the listed vulnerability?

A. Enable the browser's XSS filter.
B. Enable Windows XSS protection
C. Enable the browser's protected pages mode
D. Enable server-side XSS protection

Answer: D

NEW QUESTION 540
- (Exam Topic 3)
A new vanant of malware is spreading on ihe company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

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

Answer: A

NEW QUESTION 543
- (Exam Topic 3)
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

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

Answer: D

NEW QUESTION 548
- (Exam Topic 3)
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten
B. Panda
C. Tiger
D. Jackal
E. Bear
F. Spider

Answer: CD

NEW QUESTION 550
- (Exam Topic 3)
An organization is adopting loT devices at an increasing rate and will need to account for firmware updates in its vulnerability management programs. Despite the number of devices being deployed, the organization has only focused on software patches so far. leaving hardware-related weaknesses open to compromise. Which of the following best practices will help the organization to track and deploy trusted firmware updates as part of its vulnerability management programs?

A. Utilize threat intelligence to guide risk evaluation activities and implement critical updates after proper testing.
B. Apply all firmware updates as soon as they are released to mitigate the risk of compromise.
C. Determine an annual patch cadence to ensure all patching occurs at the same time.
D. Implement an automated solution that detects when vendors release firmware updates and immediately deploy updates to production.

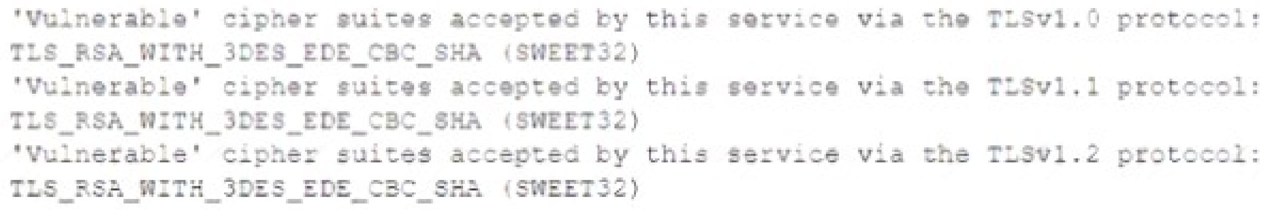
Answer: D

NEW QUESTION 554
- (Exam Topic 3)
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:
• The partners' PCs must not connect directly to the laboratory network.
• The tools the partners need to access while on the laboratory network must be available to all partners
• The partners must be able to run analyses on the laboratory network, which may take hours to complete Which of the following capabilities will MOST likely meet the security objectives of the request?

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

Answer: C

NEW QUESTION 557
- (Exam Topic 3)
During a review of the vulnerability scan results on a server, an information security analyst notices the following:



```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

A. It only accepts TLSvl 2
B. It only accepts cipher suites using AES and SHA
C. It no longer accepts the vulnerable cipher suites
D. SSL/TLS is offloaded to a WAF and load balancer

Answer: C

NEW QUESTION 561
- (Exam Topic 3)
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

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

Answer: B

NEW QUESTION 565
- (Exam Topic 3)
During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Answer: A

NEW QUESTION 570
......