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

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

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: D
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: C
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: C
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: B
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

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: CE
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

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

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

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

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:

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:

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

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
```

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

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
```

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