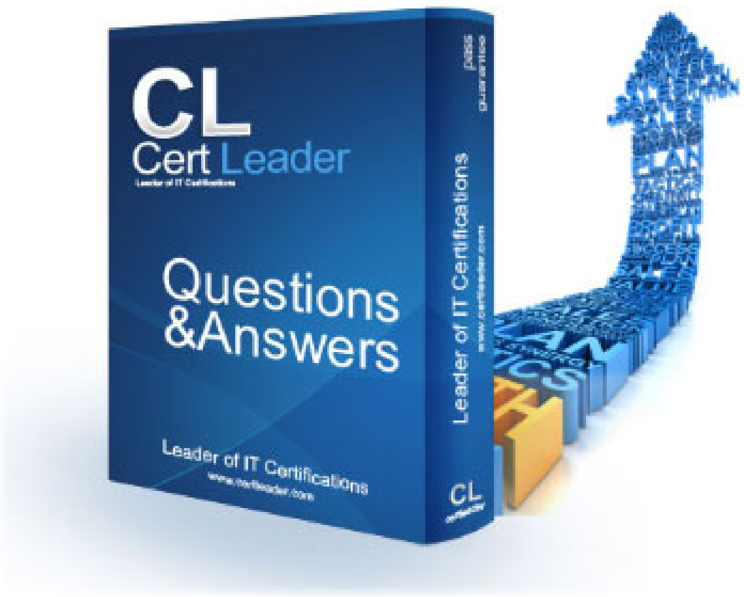
CAS-004 Dumps

CompTIA Advanced Security Practitioner (CASP+) Exam

https://www.certleader.com/CAS-004-dumps.html



NEW QUESTION 1
Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization. Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

A. Align the exploitability metrics to the predetermined system categorization.
B. Align the remediation levels to the predetermined system categorization.
C. Align the impact subscore requirements to the predetermined system categorization.
D. Align the attack vectors to the predetermined system categorization.

Answer: C

Explanation:
Aligning the impact subscore requirements to the predetermined system categorization can help the analyst get a better picture of the risk while adhering to the organization’s policy. The impact subscore is one of the components of the CVSS base score, which reflects the severity of a vulnerability. The impact subscore is calculated based on three metrics: confidentiality, integrity, and availability. These metrics can be adjusted according to the system categorization, which defines the security objectives and requirements for a system based on its potential impact on an organization’s operations and assets. By aligning the impact subscore requirements to the system categorization, the analyst can ensure that the CVSS scores reflect the true impact of a vulnerability on a specific system and prioritize remediation accordingly.

NEW QUESTION 2
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

A. Remote provider BCDR
B. Cloud provider BCDR
C. Alternative provider BCDR
D. Primary provider BCDR

Answer: B

NEW QUESTION 3
A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation m the near future?

A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.
C. Implement a centralized network gateway to bridge network traffic between all VPCs.
D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

Answer: A

Explanation:
The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

NEW QUESTION 4
A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders. Which of the following techniques would the company use to evaluate data confidentiality controls?

A. Eavesdropping
B. On-path
C. Cryptanalysis
D. Code signing
E. RF sidelobe sniffing

Answer: A

NEW QUESTION 5
A company’s employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Select TWO.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Answer: CF

NEW QUESTION 6

Which of the following BEST sets expectation between the security team and business units within an organization?

A. Risk assessment
B. Memorandum of understanding
C. Business impact analysis
D. Business partnership agreement
E. Services level agreement

Answer: E

Explanation:
A service level agreement (SLA) is the best option to set expectations between the security team and business units within an organization. An SLA is a document that defines the scope, quality, roles, responsibilities, and metrics of a service provided by one party to another. An SLA can help align the security team's objectives and activities with the business units' needs and expectations, as well as establish accountability and communication channels. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://searchitchannel.techtarget.com/definition/service-level-agreement

NEW QUESTION 7
An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:
• Some developers can directly publish code to the production environment.
• Static code reviews are performed adequately.
• Vulnerability scanning occurs on a regularly scheduled basis per policy.
Which of the following should be noted as a recommendation within the audit report?

A. Implement short maintenance windows.
B. Perform periodic account reviews.
C. Implement job rotation.
D. Improve separation of duties.

Answer: D

NEW QUESTION 8
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting
B. Permissive
C. Enforcing
D. Mandatory

Answer: C

Explanation:
Reference: https://source.android.com/security/selinux/customize
SELinux (Security-Enhanced Linux) is a security module for Linux systems that provides mandatory access control (MAC) policies for processes and files. SELinux can operate in three modes:
Enforcing: SELinux enforces the MAC policies and denies access based on rules. Permissive: SELinux does not enforce the MAC policies but only logs actions that would
have been denied if running in enforcing mode.
Disabled: SELinux is turned off.
To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse. References: https://access.redhat.com/documentation/en- us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security- enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes https://source.android.com/security/selinux

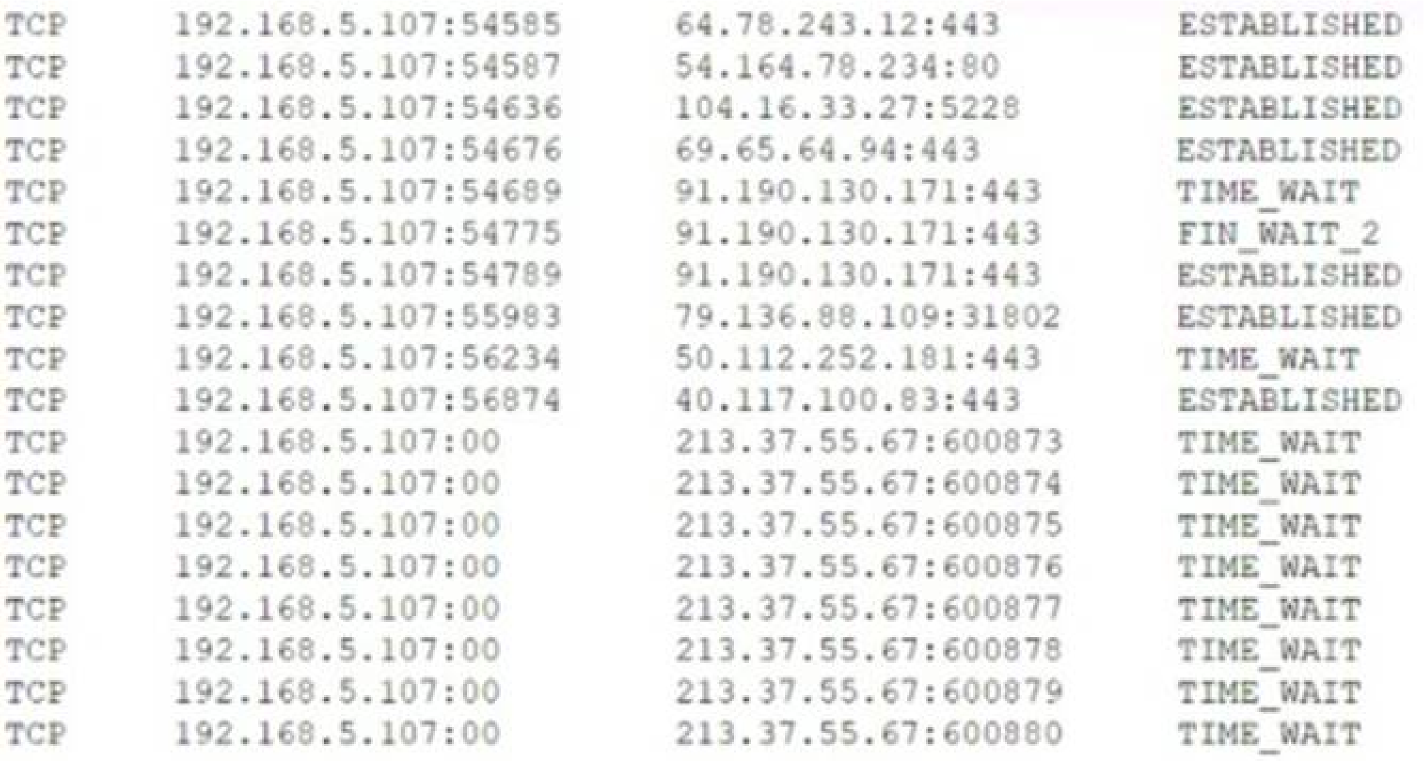
NEW QUESTION 9
A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:
• dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
• A persistent TCP/6667 connection to the external address was established at 7:55 a.m. The connection is still active.
• Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.
• A sample outbound request payload from PCAP showed the ASCII content: "JOIN
#community".
Which of the following is the MOST likely root cause?

A. A SQL injection was used to exfiltrate data from the database server.
B. The system has been hijacked for cryptocurrency mining.
C. A botnet Trojan is installed on the database server.
D. The dbadmin user is consulting the community for help via Internet Relay Chat.

Answer: D

Explanation:
The dbadmin user is consulting the community for help via Internet Relay Chat. The clues in the given information point to the dbadmin user having established an Internet Relay Chat (IRC) connection to an external address at 7:55 a.m. This connection is still active, and only a few kilobytes of data have been transferred since the start of the connection. The sample outbound request payload of "JOIN #community" also suggests that the user is trying to join an IRC chatroom. This suggests that the dbadmin user is using the IRC connection to consult the community for help with a problem. Therefore, the root cause of the anomalous activity is likely the dbadmin user consulting the community for help via IRC. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 10, Investigating Intrusions and Suspicious Activity.

NEW QUESTION 10
Users are claiming that a web server is not accessible. A security engineer logs for the site. The engineer connects to the server and runs netstat -an and receives the following output:



```
TCP       192.168.5.107:54585          64.78.243.12:443             ESTABLISHED
TCP       192.168.5.107:54587          54.164.78.234:80             ESTABLISHED
TCP       192.168.5.107:54636          104.16.33.27:5228            ESTABLISHED
TCP       192.168.5.107:54676          69.65.64.94:443              ESTABLISHED
TCP       192.168.5.107:54689          91.190.130.171:443           TIME_WAIT
TCP       192.168.5.107:54775          91.190.130.171:443           FIN_WAIT_2
TCP       192.168.5.107:54789          91.190.130.171:443           ESTABLISHED
TCP       192.168.5.107:55983          79.136.88.109:31802          ESTABLISHED
TCP       192.168.5.107:56234          50.112.252.181:443           TIME_WAIT
TCP       192.168.5.107:56874          40.117.100.83:443            ESTABLISHED
TCP       192.168.5.107:00             213.37.55.67:600873          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600874          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600875          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600876          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600877          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600878          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600879          TIME_WAIT
TCP       192.168.5.107:00             213.37.55.67:600880          TIME_WAIT
```

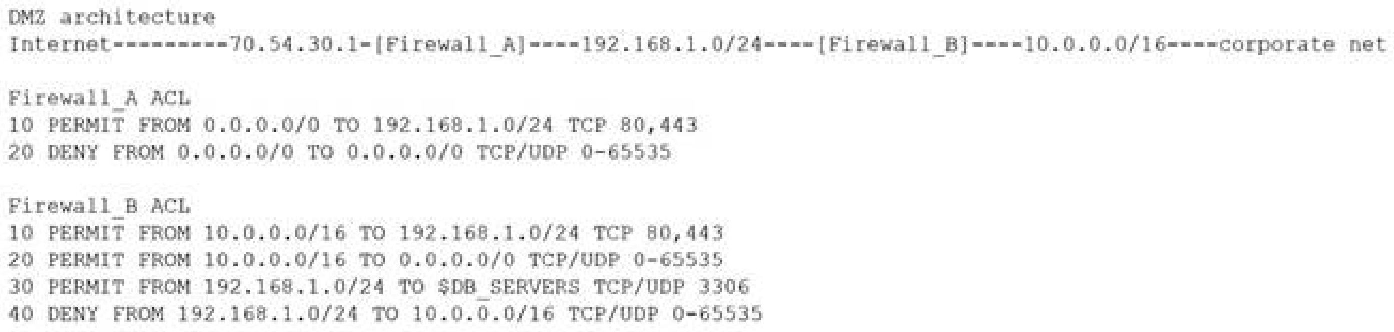
Which of the following is MOST likely happening to the server?

A. Port scanning
B. ARP spoofing
C. Buffer overflow
D. Denial of service

Answer: D

Explanation:
A denial of service (DoS) attack is a malicious attempt to disrupt the normal functioning of a server by overwhelming it with requests or traffic1. One possible indicator of a DoS attack is a large number of connections from a single source IP address1. In this case, the output of netstat -an shows that there are many connections from 213.37.55.67 with different port numbers and in TIME WAIT state23. This suggests that the attacker is sending many SYN packets to initiate connections but not completing them, thus exhausting the server's resources and preventing legitimate users from accessing it1.

NEW QUESTION 10
A security architect is reviewing the following proposed corporate firewall architecture and configuration:



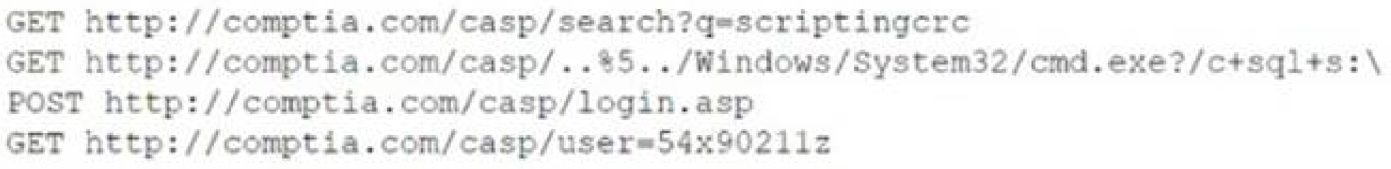
```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network. Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443. Which of the following should the architect recommend to ensure all requirements are met
in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP80,443
C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0- 65535
F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Answer: AD

NEW QUESTION 11
A security analyst needs to recommend a remediation to the following threat:



```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Patch the system.
B. Update the antivirus.
C. Install a host-based firewall.

D. Enable TLS 1.2.

Answer: D

NEW QUESTION 12
A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts. The organization websites are:
* www.mycompany.org
* www.mycompany.com
* campus.mycompany.com
* wiki. mycompany.org
The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the BEST solution?

A. Purchase one SAN certificate.
B. Implement self-signed certificates.
C. Purchase one certificate for each website.
D. Purchase one wildcard certificate.

Answer: D

Explanation:
Purchasing one wildcard certificate is the best solution to protect multiple websites hosted by an organization in a cloud-hosted WAF. A wildcard certificate is a type of SSL/TLS certificate that can secure a domain name and any number of its subdomains with a single certificate. For example, a wildcard certificate for *.mycompany.com can secure www.mycompany.com, campus.mycompany.com, and any other subdomain under mycompany.com. A wildcard certificate can save costs and simplify management compared to purchasing individual certificates for each website.
References: [CompTIA CASP+ Study Guide, Second Edition, page 301]

NEW QUESTION 16
A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability. Which of the following would BEST resolve and mitigate the issue? (Select TWO).

A. Deploying a WAF signature
B. Fixing the PHP code
C. Changing the web server from HTTPS to HTTP
D. UsingSSLv3
E. Changing the code from PHP to ColdFusion
F. Updating the OpenSSL library

Answer: AF

Explanation:
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.
* B. Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
* C. Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
* D. Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
* E. Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server.
https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug https://heartbleed.com/

NEW QUESTION 19
A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.
This is an example of:

A. due intelligence
B. e-discovery.
C. due care.
D. legal hold.

Answer: A

Explanation:
Reference: https://www.ansarada.com/due-diligence/hr

NEW QUESTION 21
An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API. Given this information, which of the following is a noted risk?

A. Feature delay due to extended software development cycles
B. Financial liability from a vendor data breach
C. Technical impact to the API configuration
D. The possibility of the vendor’s business ceasing operations

Answer: A

Explanation:
Reference: https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability

NEW QUESTION 26
A security engineer estimates the company’s popular web application experiences 100 attempted breaches per day. In the past four years, the company’s data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8
C. 50
D. 36,500

Answer: A

Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative- risk-analysis/
The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company’s data has been breached two times in four years, so the ARO is 2 / 4 = 0.5. The other options are incorrect calculations. Verified References: https://www.comptia.org/blog/what-is-risk-management https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 27
A company security engineer arrives at work to face the following scenario:
1) Website defacement
2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
3) A Job offer from the company's competitor
4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data
Which of the following threat actors Is MOST likely involved?

A. Organized crime
B. Script kiddie
C. APT/nation-state
D. Competitor

Answer: C

Explanation:
An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: “Advanced Persistent Threats,” Wiley, 2018.
https://www.wiley.com/en- us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition
-p-9781119396582

NEW QUESTION 30
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users’ trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
+ Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Answer: BF

Explanation:
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks. The other options are either irrelevant or less effective for the given scenario.

NEW QUESTION 34
An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS

and SaaS solutions, and it was designed with the following considerations:
- Protection from DoS attacks against its infrastructure and web applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.
- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive architecture.
With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

A. The public cloud provider is applying QoS to the inbound customer traffic.
B. The API gateway endpoints are being directly targeted.
C. The site is experiencing a brute-force credential attack.
D. A DDoS attack is targeted at the CDN.

Answer: A

NEW QUESTION 39
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

A. Community cloud service model
B. Multinency SaaS
C. Single-tenancy SaaS
D. On-premises cloud service model

Answer: C

Explanation:
A single-tenancy SaaS solution is the best solution for this company. SaaS stands for software as a service, which is a cloud-based model that allows customers to access applications hosted by a provider over the internet. A single-tenancy SaaS solution means that the company has its own dedicated instance of the application and its underlying infrastructure, which offers more control, customization, and security than a multi-tenancy SaaS solution where multiple customers share the same resources. A single- tenancy SaaS solution also eliminates the need for managing a private cloud or an on- premises infrastructure. Verified References: https://www.comptia.org/training/books/casp- cas-004-study-guide , https://www.ibm.com/cloud/learn/saas

NEW QUESTION 44
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

Answer: B

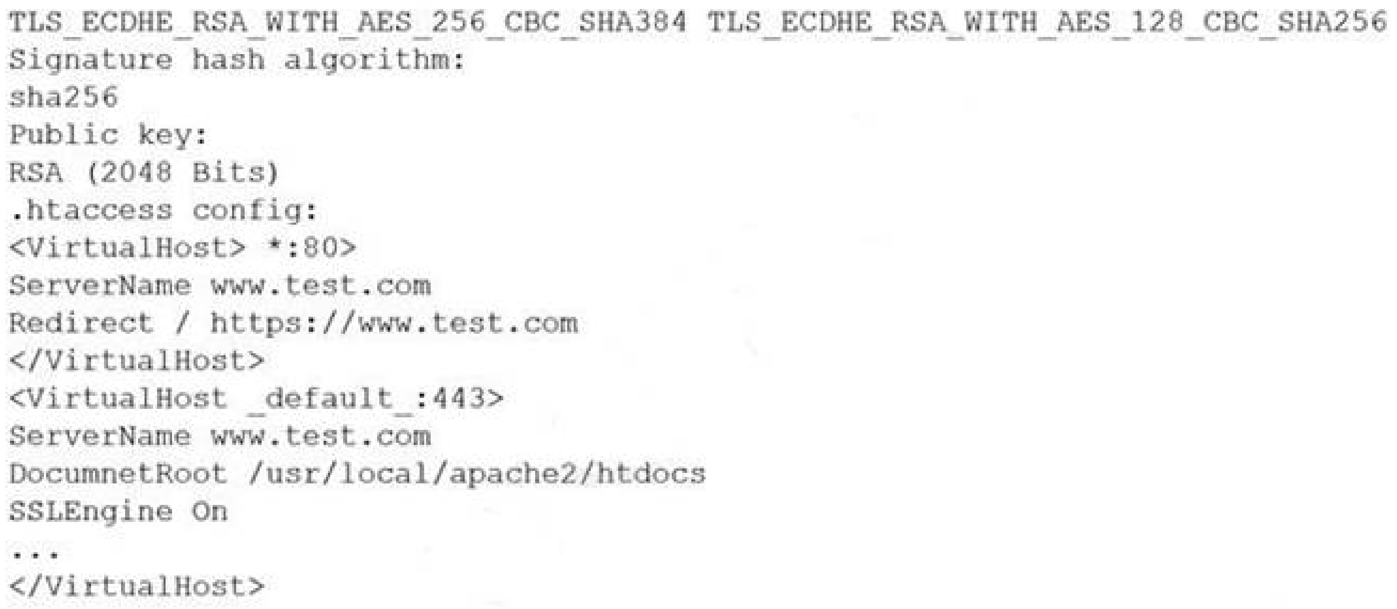
NEW QUESTION 46
A municipal department receives telemetry data from a third-party provider The server collecting telemetry sits in the municipal departments screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to Implement nsk mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
C. Installing and configuring filesystem integrity monitoring service on the telemetry server
D. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM
E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
F. Using the published data schema to monitor and block off nominal telemetry messages

Answer: AC

Explanation:
A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and
configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

NEW QUESTION 47
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:



```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumnetRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer's inability to connect?

A. Weak ciphers are being used.
B. The public key should be using ECDSA.
C. The default should be on port 80.
D. The server name should be test.com.

Answer: A

Explanation:
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa- ecdsa-are-there-easy-answers-for-which-to-choose-when

NEW QUESTION 48
A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then
tries to boot the computer using wake-on-LAN, but the system would not come up. which of the following explains why the computer would not boot?

A. The operating system was corrupted.
B. SElinux was in enforced status.
C. A secure boot violation occurred.
D. The disk was encrypted.

Answer: A

NEW QUESTION 49
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

A. ARF
B. XCCDF
C. CPE
D. CVE
E. CVSS
F. OVAL

Answer: BF

Explanation:
Reference: https://www.govinfo.gov/content/pkg/GOVPUB-C13- 9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)
XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language) are two SCAP (Security Content Automation Protocol) standards that can enable the organization to view each of the configuration
checks in a machine-readable checklist format for full automation. XCCDF is a standard for expressing security checklists and benchmarks, while OVAL is a standard for expressing system configuration information and vulnerabilities. ARF (Asset Reporting Format) is a standard for expressing the transport format of information about assets, not configuration checks. CPE (Common Platform Enumeration) is a standard for identifying and naming hardware, software, and operating systems, not configuration checks. CVE (Common Vulnerabilities and Exposures) is a standard for identifying and naming publicly known cybersecurity vulnerabilities, not configuration checks. CVSS (Common Vulnerability Scoring System) is a standard for assessing the severity of cybersecurity vulnerabilities, not configuration checks. Verified References: https://www.comptia.org/blog/what-is-scap https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 54
A company's Chief Information Officer wants to Implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide Information on attempted attacks, and provide analysis of malicious activities to determine the processes or users Involved. Which of the following would provide this information?

A. HIPS
B. UEBA
C. HIDS
D. NIDS

Answer: B

NEW QUESTION 55
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

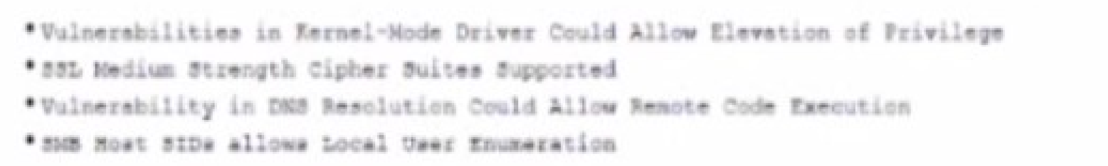
Explanation:
The best option for the security analyst to perform is to contact the security department at the business partner and alert them to the email event. The email appears to be a phishing attempt that tries to trick the employees into revealing their login credentials by impersonating a legitimate sender. The security department at the business partner should be notified so they can investigate the source and scope of the attack and take appropriate actions to protect their systems and users. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-014

NEW QUESTION 58
A pharmaceutical company recently experienced a security breach within its customer- facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.
The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

A. The pharmaceutical company
B. The cloud software provider
C. The web portal software vendor
D. The database software vendor

Answer: A

NEW QUESTION 63
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:



- Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
- SSL Medium Strength Cipher Suites Supported
- Vulnerability in DNS Resolution Could Allow Remote Code Execution
- SMB Host SIDs allows Local User Enumeration

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker
B. Port scanner
C. Account enumerator
D. Exploitation framework

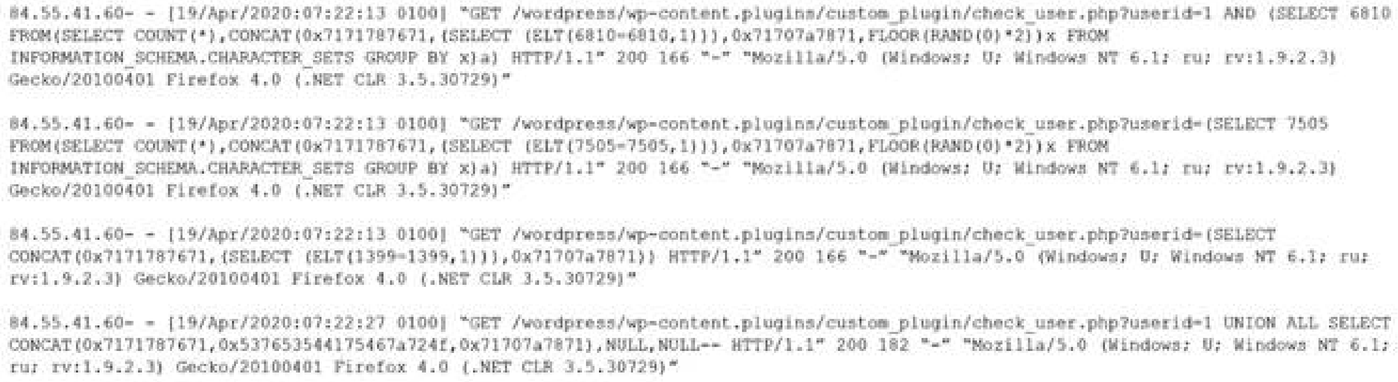
Answer: A

NEW QUESTION 65
A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

A. Distribute the software via a third-party repository.
B. Close the web repository and deliver the software via email.
C. Email the software link to all customers.
D. Display the SHA checksum on the website.

Answer: D

NEW QUESTION 67
Given the following log snippet from a web server:



```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT 7505
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1;
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

A. SQL injection
B. Cross-site scripting
C. Brute-force
D. Cross-site request forgery

Answer: A

NEW QUESTION 72
The Chief Information Security Officer (CISO) is working with a new company and needs a legal “document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?

A. SLA
B. ISA
C. Permissions and access
D. Rules of engagement

Answer: D

Explanation:
Rules of engagement are legal documents that should be signed by all parties involved in an assessment to ensure they understand their roles and responsibilities. Rules of engagement define the scope, objectives, methods, deliverables, limitations, and expectations of an assessment project. They also specify the legal and ethical boundaries, communication channels, escalation procedures, and reporting formats for the assessment. Rules of engagement help to avoid misunderstandings, conflicts, or liabilities during or after an assessment.
References: [CompTIA CASP+ Study Guide, Second Edition, page 34]

NEW QUESTION 77
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

A. Importing the availability of messages
B. Ensuring non-repudiation of messages
C. Enforcing protocol conformance for messages
D. Assuring the integrity of messages

Answer: D

Explanation:
Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service.
Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: https://www.comptia.org/blog/what-is-integrity
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 79
A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:
* Capable of early detection of advanced persistent threats.
* Must be transparent to users and cause no performance degradation.
+ Allow integration with production and development networks seamlessly.
+ Enable the security team to hunt and investigate live exploitation techniques.
Which of the following technologies BEST meets the customer's requirements for security capabilities?

A. Threat Intelligence
B. Deception software
C. Centralized logging
D. Sandbox detonation

Answer: B

Explanation:
Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them. By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools12
. Deception software can also provide valuable insights into the attacker’s tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys 13.
Deception software can meet the customer’s requirements for security capabilities because:
? It is capable of early detection of APTs by creating attractive targets for them and
alerting security teams when they are engaged12.
? It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources13.
? It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration13.
? It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker’s activities on the decoys13.

NEW QUESTION 81
Which of the following terms refers to the delivery of encryption keys to a CASB or a third- party entity?

A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow

Answer: D

Explanation:
Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy. References: https://www.techopedia.com/definition/1772/key-escrow
https://searchsecurity.techtarget.com/definition/key-escrow

NEW QUESTION 86
During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.
Which of the following processes would BEST satisfy this requirement?

A. Monitor camera footage corresponding to a valid access request.
B. Require both security and management to open the door.
C. Require department managers to review denied-access requests.
D. Issue new entry badges on a weekly basis.

Answer: B

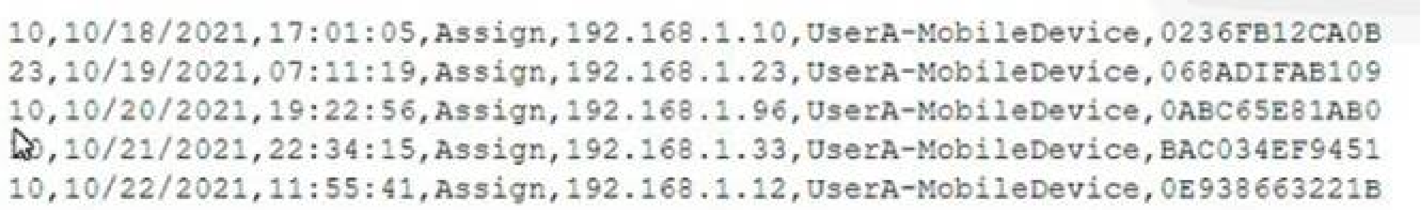
Explanation:
Reference: https://www.getkisi.com/access-control
This solution would implement a two-factor authentication (2FA) process that would prevent unauthorized individuals from entering the storage room by following an authorized employee. The two factors would be the card reader issued by the security team and the presence of a department manager.

NEW QUESTION 88
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

A. when it is passed across a local network.
B. in memory during processing
C. when it is written to a system's solid-state drive.
D. by an enterprise hardware security module.

Answer: B

NEW QUESTION 89
A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices:



```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
10,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

Which of the following mobile configuration settings is the mobile administrator verifying?

A. Service set identifier authentication
B. Wireless network auto joining
C. 802.1X with mutual authentication
D. Association MAC address randomization

Answer: B

Explanation:
Wireless network auto joining is the mobile configuration setting that the mobile administrator is verifying by reviewing the mobile device DHCP logs. Wireless network auto joining is a feature that allows mobile devices to automatically connect to a predefined wireless network without requiring user intervention or authentication. This can be useful for corporate or trusted networks that need frequent access by mobile devices. The DHCP logs show that the mobile devices are assigned IP addresses from the wireless network with SSID "CorpWiFi", which indicates that they are auto joining this network. References: [CompTIA CASP+ Study Guide, Second Edition, page 420]

NEW QUESTION 93
A bank hired a security architect to improve its security measures against the latest threats The solution must meet the following requirements
- Recognize and block fake websites
- Decrypt and scan encrypted traffic on standard and non-standard ports
- Use multiple engines for detection and prevention
- Have central reporting

Which of the following is the BEST solution the security architect can propose?

A. CASB
B. Web filtering

C. NGFW
D. EDR

Answer: C

Explanation:
A next-generation firewall (NGFW) is a device or software that provides advanced network security features beyond the traditional firewall functions. A NGFW can provide the following capabilities:
? Recognize and block fake websites, using URL filtering and reputation-based
analysis
? Decrypt and scan encrypted traffic on standard and non-standard ports, using SSL/TLS inspection and deep packet inspection
? Use multiple engines for detection and prevention, such as antivirus, intrusion prevention system (IPS), application control, and sandboxing
? Have central reporting, using a unified management console and dashboard A cloud access security broker (CASB) is a device or software that acts as an intermediary between cloud service users and cloud service providers. A CASB can provide various security functions such as visibility, compliance, data security, and threat protection, but it does not provide all the capabilities of a NGFW. Web filtering is a technique that blocks or allows web access based on predefined criteria such as categories, keywords, or reputation. Web filtering can help recognize and block fake websites, but it does not provide all the capabilities of a NGFW. Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints such as computers or mobile devices. EDR can help detect and respond to advanced threats, but it does not provide all the capabilities of a NGFW. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise
Security Architecture, Objective 2.2: Select appropriate hardware and software solutions

NEW QUESTION 96
Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

A. MOU
B. NDA
C. SLA
D. ISA

Answer: A

NEW QUESTION 99
A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53
B. MITRE ATT&CK
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: B

Explanation:
MITRE ATT&CK is a threat management framework that provides a comprehensive and detailed knowledge base of adversary tactics and techniques based on real-world observations. It can help threat hunting teams to identify, understand, and prioritize potential threats, as well as to develop effective detection and response strategies. MITRE ATT&CK covers the entire lifecycle of a cyberattack, from initial access to impact, and provides information on how to mitigate, detect, and hunt for each technique. It also includes threat actor profiles, software descriptions, and data sources that can be used for threat intelligence and analysis.
Verified References:
? https://attack.mitre.org/
? https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride- owasp-top-10-mitre-attck-framework/
? https://www.ibm.com/topics/threat-management

NEW QUESTION 101
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency
B. Data exposure
C. Data loss
D. Data dispersion

Answer: B

Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified References: https://www.comptia.org/blog/what-is-data-exposure
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 104
An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately. many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

A. Regression testing
B. SAST
C. Third-party dependency management

D. IDE SAST
E. Fuzz testing
F. IAST

Answer: DE

NEW QUESTION 106
The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewal
B. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit claus
C. Regularly assess the supplier’s post-contract renewal with a dedicated risk management team.
D. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all supplier
E. Store findings from the reviews in a database for all other business units and risk teams to reference.
F. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
G. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed andmanaged based on the supplier’s ratin
H. Report finding units that rely on the suppliers and the various risk teams.

Answer: D

Explanation:
A governance program that rates suppliers based on their access to data, the type of data, and how they access the data is the best way to manage the risk of handling and security of customer data by third parties. This allows the company to assign key controls that are reviewed and managed based on the supplier’s rating and report findings to the relevant units and risk teams. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/third-party-risk- management

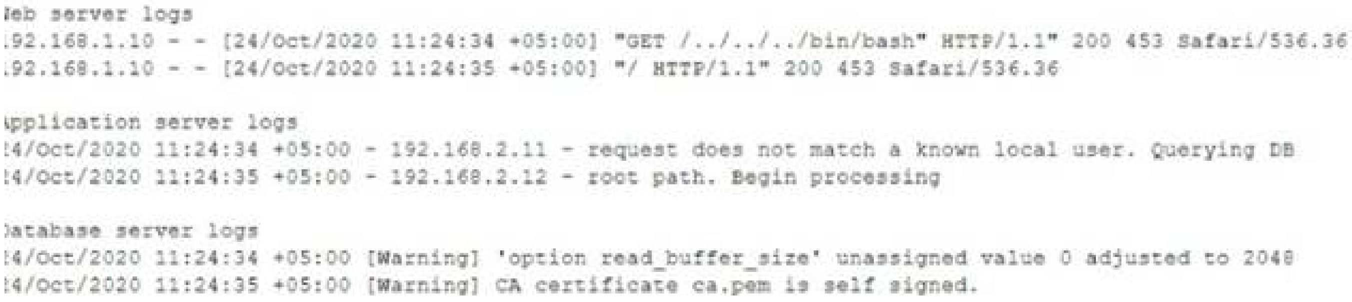
NEW QUESTION 111
Correct Answer: (Answer option in bold)
Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources)
Verified References: (Related URLs AND Make sure Links are working and verified references)
================
A security administrator wants to detect a potential forged sender claim in tt-e envelope of an email. Which of the following should the security administrator implement? (Select TWO).

A. MX record
B. DMARC
C. SPF
D. DNSSEC
E. S/MIME
F. TLS

Answer: BC

Explanation:
DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework) are two mechanisms that can help detect and prevent email spoofing, which is the creation of email messages with a forged sender address. DMARC allows a domain owner to publish a policy that specifies how receivers should handle messages that fail authentication tests, such as SPF or DKIM (DomainKeys Identified Mail). SPF allows a domain owner to specify which mail servers are authorized to send email on behalf of their domain. By checking the DMARC and SPF records of the sender’s domain, a receiver can verify if the email is from a legitimate source or not. Verified References:
? https://en.wikipedia.org/wiki/Email_spoofing
? https://en.wikipedia.org/wiki/DMARC
? https://en.wikipedia.org/wiki/Sender_Policy_Framework

NEW QUESTION 116
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:



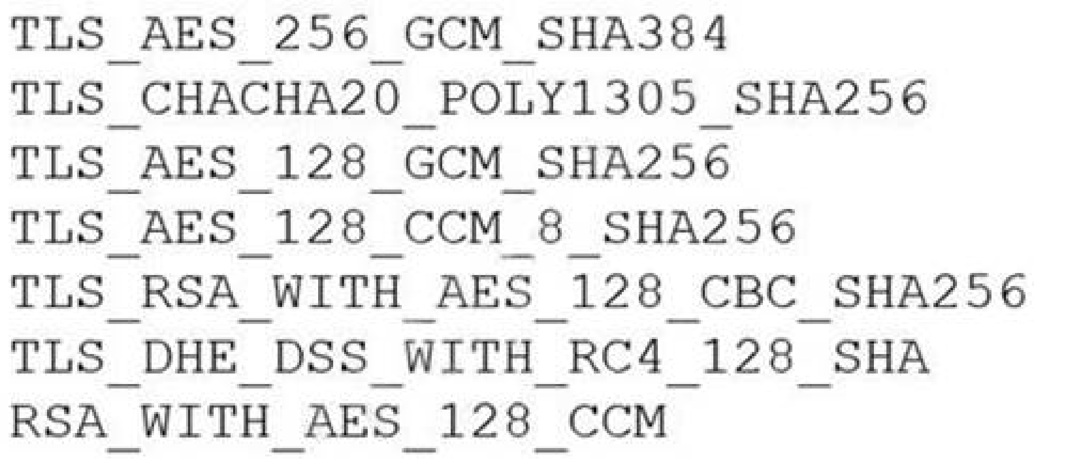
```
Web server logs
.92.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
.92.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_server (‘ REMOTE_ADDR '] received by the web servers.

Answer: C

NEW QUESTION 121
A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:



```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

A. TLS_AES_128_CCM_8_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA
C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_AES_128_GCM_SHA256

Answer: B

Explanation:
The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: https://www.comptia.org/blog/what-is-a-cipher https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 125
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator’s discovery?

A. A vulnerability
B. A threat
C. A breach
D. A risk

Answer: A

Explanation:
Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-
explained

NEW QUESTION 126
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. CRL
C. CSRs
D. OCSP

Answer: C

Explanation:
Reference: https://www.ssl.com/faqs/compromised-private-keys/

NEW QUESTION 128
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Answer: C

Explanation:
The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 1:

Network Security Architecture and Design, Section 1.3: Cloud Security.

NEW QUESTION 132
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B

Explanation:
PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified References: https://www.comptia.org/blog/what-is-pam https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 135
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.
B. Isolate the servers to prevent the spread.
C. Notify law enforcement.
D. Request that the affected servers be restored immediately.

Answer: B

Explanation:
Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that the affected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified References:
https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself https://www.comptia.org/certifications/comptia-advanced-security-practitioner

NEW QUESTION 140
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

A. Conduct input sanitization.
B. Deploy a SIEM.
C. Use containers.
D. Patch the OS
E. Deploy a WAF.
F. Deploy a reverse proxy
G. Deploy an IDS.

Answer: AE

Explanation:
A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.
According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization.
LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.45

NEW QUESTION 143
A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

A. Loss of governance
B. Vendor lockout
C. Compliance risk
D. Vendor lock-in

Answer: C

NEW QUESTION 147

FILL IN THE BLANK

SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

The company's hardening guidelines indicate the following: There should be one primary server or service per device. Only default ports should be used. Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

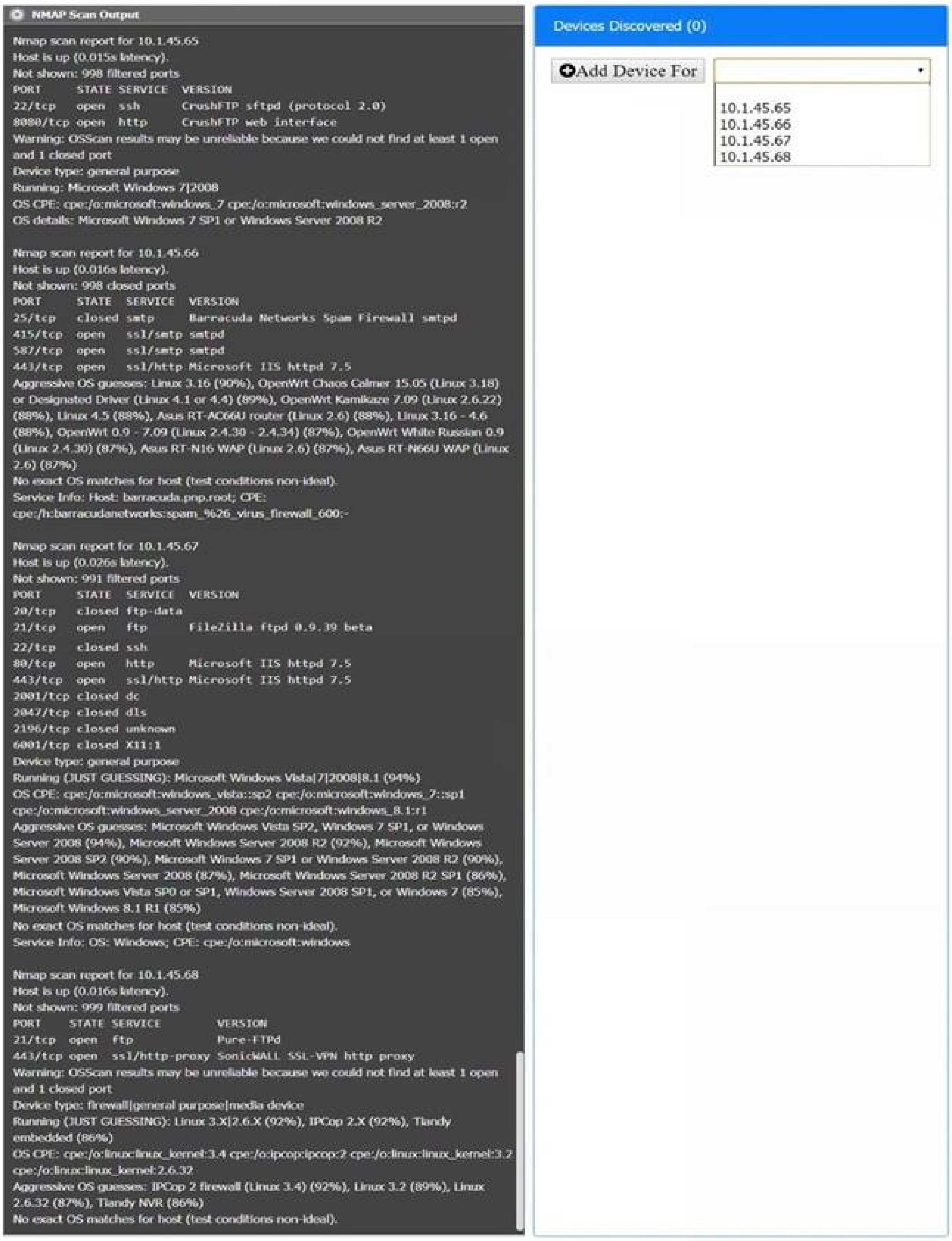
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

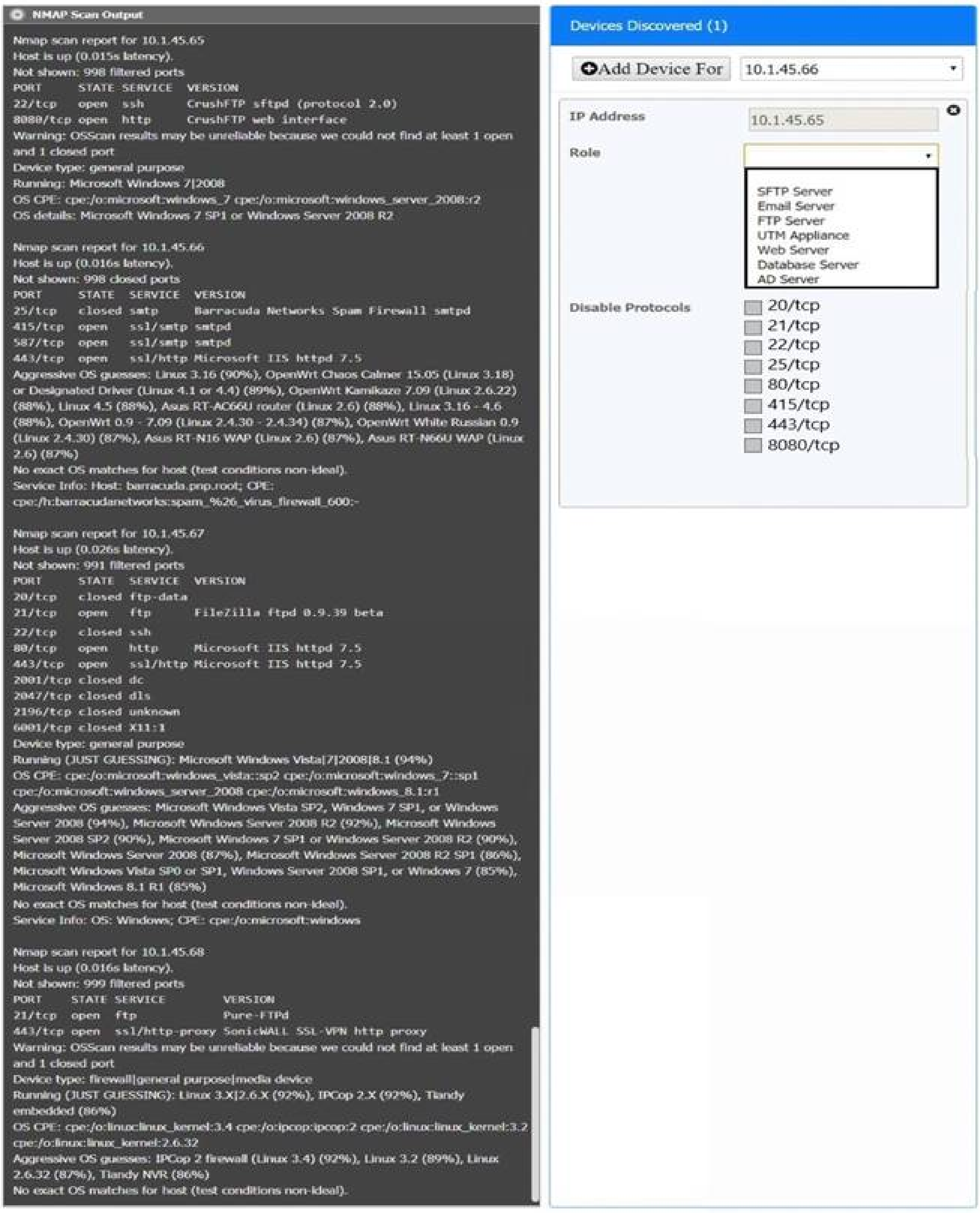
The primary server or service of the device (Note that each IP should by associated with one service/port only)

The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)

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



```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE   SERVICE  VERSION
25/tcp    closed smtp      Barracuda Networks Spam Firewall smtpd
415/tcp   open    ssl/smtp smtpd
587/tcp   open    ssl/smtp smtpd
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE   SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open    ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open    http     Microsoft IIS httpd 7.5
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Pure-FTPd
443/tcp open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```



NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE   VERSION
22/tcp    open  ssh       CrushFTP sftpd (protocol 2.0)
8080/tcp open   http      CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE   SERVICE   VERSION
25/tcp    closed smtp       Barracuda Networks Spam Firewall smtpd
415/tcp   open    ssl/smtp smtpd
587/tcp   open    ssl/smtp smtpd
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE   SERVICE   VERSION
20/tcp    closed ftp-data
21/tcp    open    ftp       FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open    http      Microsoft IIS httpd 7.5
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE          VERSION
21/tcp   open  ftp              Pure-FTPd
443/tcp open   ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

Devices Discovered (1)

Add Device For: 10.1.45.66

IP Address: 10.1.45.65

Role:

Disable Protocols
□ 20/tcp
□ 21/tcp
□ 22/tcp
□ 25/tcp
□ 80/tcp
□ 415/tcp
□ 443/tcp
□ 8080/tcp

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 10.1.45.65 SFTP Server Disable 8080
* 10.1.45.66 Email Server Disable 415 and 443
* 10.1.45.67 Web Server Disable 21, 80
* 10.1.45.68 UTM Appliance Disable 21

NEW QUESTION 151
A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.
Which of the following will allow the inspection of the data without multiple certificate deployments?

A. Include all available cipher suites.
B. Create a wildcard certificate.
C. Use a third-party CA.
D. Implement certificate pinning.

Answer: B

Explanation:
A wildcard certificate is a certificate that can be used for multiple subdomains of a domain, such as *.example.com. This would allow the inspection of the data without multiple certificate deployments, as one wildcard certificate can cover all the subdomains that will be separated out with subdomains. Including all available cipher suites may not help with inspecting the data without multiple certificate deployments, as cipher suites are used for negotiating encryption and authentication algorithms, not for verifying certificates. Using a third-party CA (certificate authority) may not help with inspecting the data without multiple certificate deployments, as a third-party CA is an entity that issues and validates certificates, not a type of certificate. Implementing certificate pinning may not help with inspecting the data without multiple certificate deployments, as certificate pinning is a technique that hardcodes the expected certificate or public key in the application code, not a type of certificate. Verified References: https://www.comptia.org/blog/what-is-a-wildcard- certificate https://partners.comptia.org/docs/default-source/resources/casp-

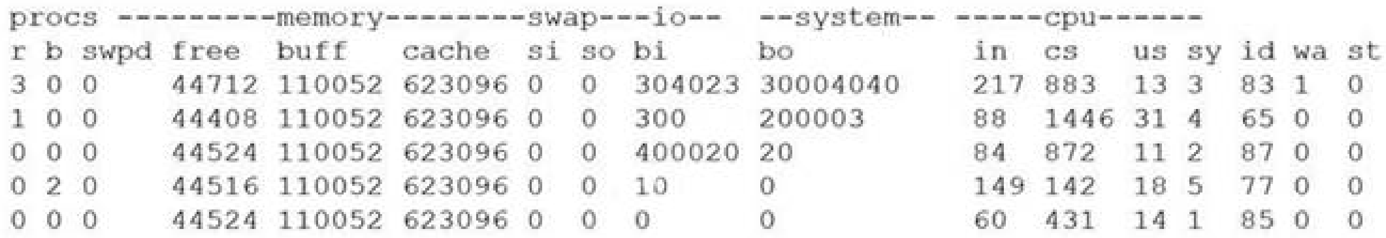
content-guide

NEW QUESTION 156
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 161
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.



```
procs ---------memory--------swap---io--   --system-- -----cpu------
r b swpd free  buff   cache  si so bi      bo          in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040    217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003      88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20          84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0           149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0           60  431  14 1  85 0  0
```

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65
B. 77
C. 83
D. 87

Answer: D

Explanation:
The process ID 87 can be the starting point for an investigation of a possible buffer overflow attack, as it shows a high percentage of CPU utilization (99.7%) and a suspicious command name (graphic.linux_randomization.prg). A buffer overflow attack is a type of attack that exploits a vulnerability in an application or system that allows an attacker to write data beyond the allocated buffer size, potentially overwriting memory segments and executing malicious code. A high CPU utilization could indicate that the process is performing intensive or abnormal operations, such as a buffer overflow attack. A suspicious command name could indicate that the process is trying to disguise itself or evade detection, such as by mimicking a legitimate program or using random characters. The other process IDs do not show signs of a buffer overflow attack, as they have low CPU utilization and normal command names. Verified References: https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 163
A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

A. Mirror the blobs at a local data center.
B. Enable fast recovery on the storage account.
C. Implement soft delete for blobs.
D. Make the blob immutable.

Answer: C

Explanation:
Soft delete allows blobs to be deleted, but the data remains accessible for a period of time before it is permanently deleted. This allows the company to delete blobs as needed, while still affording enough time for the backup process to complete. After the backup process is complete, the blobs can be permanently deleted.

NEW QUESTION 167
A network administrator who manages a Linux web server notices the following traffic: http://corr.ptia.org/.../.../.../... /etc./shadow
Which of the following Is the BEST action for the network administrator to take to defend against this type of web attack?

A. Validate the server certificate and trust chain.
B. Validate the server input and append the input to the base directory path.
C. Validate that the server is not deployed with default account credentials.
D. Validate that multifactor authentication is enabled on the server for all user accounts.

Answer: B

Explanation:
The network administrator is noticing a web attack that attempts to access the /etc/shadow file on a Linux web server. The /etc/shadow file contains the encrypted passwords of all users on the system and is a common target for attackers. The attack uses a technique called directory traversal, which exploits a vulnerability in the web application that allows an attacker to access files or directories outside of the intended scope by manipulating the file path.
Validating the server input and appending the input to the base directory path would be the best action for the network administrator to take to defend against this type of web attack, because it would:
? Check the user input for any errors, malicious data, or unexpected values before

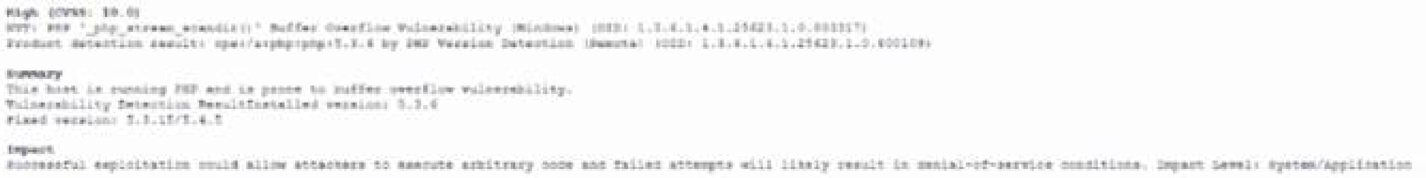
processing it by the web application.
? Prevent directory traversal by ensuring that the user input is always relative to the base directory path of the web application, and not absolute to the root directory of the web server.
? Deny access to any files or directories that are not part of the web application’s scope or functionality.

NEW QUESTION 170
A company Is adopting a new artificial-intelligence-based analytics SaaS solution. This Is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk In adopting this solution?

A. The inability to assign access controls to comply with company policy
B. The inability to require the service provider process data in a specific country
C. The inability to obtain company data when migrating to another service
D. The inability to conduct security assessments against a service provider

Answer: C

NEW QUESTION 175
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:



```
High (CVSS: 10.0)
NVT: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803317)
Product detection result: cpe:/a:php:php:5.3.6 by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to buffer overflow vulnerability.
Vulnerability Detection ResultInstalled version: 5.3.6
Fixed version: 5.3.15/5.4.5

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application
```

Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Answer: A

NEW QUESTION 177
A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

A. The principle of lawful, fair, and transparent processing
B. The right to be forgotten principle of personal data erasure requests
C. The non-repudiation and deniability principle
D. The principle of encryption, obfuscation, and data masking

Answer: A

NEW QUESTION 179
city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:
+ Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
+ All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
+ Ransomware threats and zero-day vulnerabilities must be quickly identified. Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection
B. Log aggregator
C. Zero trust network access
D. PAM
E. Cloud sandbox
F. SIEM
G. NGFW

Answer: BDF

Explanation:
B. Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1 .
* D. PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .
* F. SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero- day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

NEW QUESTION 184
A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

A. Business impact rating
B. CVE dates
C. CVSS scores

D. OVAL

Answer: A

NEW QUESTION 185
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

A. Accept
B. Avoid
C. Transfer
D. Mitigate

Answer: D

NEW QUESTION 186
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: A

NEW QUESTION 187
A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of
web-application security Which of the following is the BEST option?

A. ICANN
B. PCI DSS
C. OWASP
D. CSA
E. NIST

Answer: C

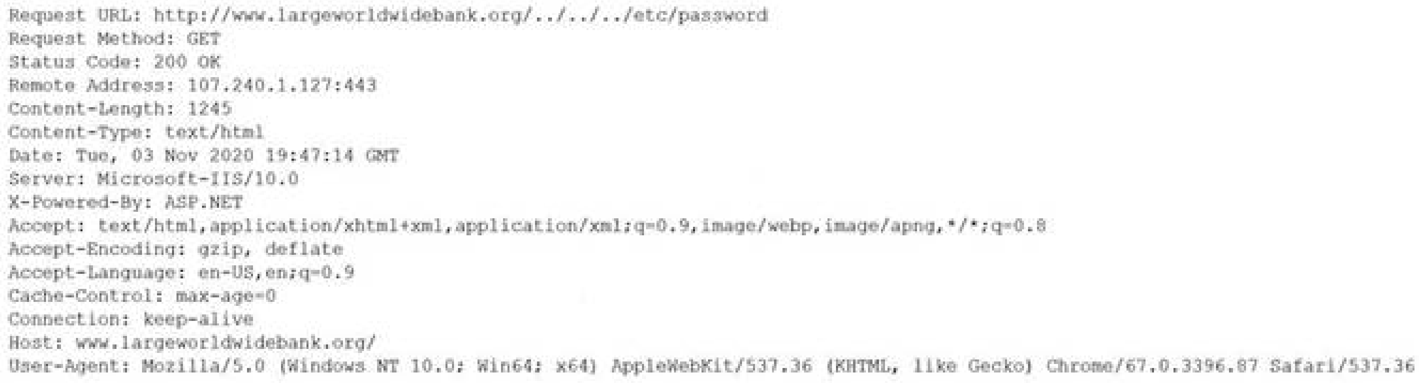
NEW QUESTION 189
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager
B. Performing DAST on a weekly basis
C. Introducing the use of container orchestration
D. Deploying instance tagging

Answer: A

Explanation:
Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/
A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. References: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

NEW QUESTION 191
A security analyst is reviewing the following output:



```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

A. Installing a network firewall
B. Placing a WAF inline
C. Implementing an IDS

D. Deploying a honeypot

Answer: B

Explanation:
The output shows a SQL injection attack that is trying to exploit a web application. A WAF (Web Application Firewall) is a security solution that can detect and block malicious web requests, such as SQL injection, XSS, CSRF, etc. Placing a WAF inline would prevent the attack from reaching the web server and database.
References: https://owasp.org/www-community/attacks/SQL_Injection https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

NEW QUESTION 194
A company wants to improve the security of its web applications that are running on in- house servers A risk assessment has been performed and the following capabilities are desired:
• Terminate SSL connections at a central location
• Manage both authentication and authorization for incoming and outgoing web service calls
• Advertise the web service API
• Implement DLP and anti-malware features
Which of the following technologies will be the BEST option?

A. WAF
B. XML gateway
C. ESB gateway
D. API gateway

Answer: D

Explanation:
An API gateway is a device or software that acts as an intermediary between clients and servers that provide web services through application programming interfaces (APIs). An API gateway can provide various functions such as:
? Terminating SSL connections at a central location, reducing the overhead on the backend servers and simplifying certificate management
? Managing both authentication and authorization for incoming and outgoing web service calls, enforcing security policies and access control
? Advertising the web service API, providing documentation and discovery features for developers and consumers
? Implementing DLP and anti-malware features, preventing data leakage and malicious code injection A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can provide some protection for web services, but it does not provide all the functions of an API gateway. An XML gateway is a device or software that validates, transforms, and routes XML messages between clients and servers that provide web services. An XML gateway can provide some functions of an API gateway, but it is limited to XML-based web services and does not support other formats such as JSON. An enterprise service bus (ESB) gateway is a device or software that integrates and orchestrates multiple web services into a single service or application. An ESB gateway can provide some functions of an API gateway, but it is more focused on business logic and workflow rather than security and performance.
References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION 198
FILL IN THE BLANK
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

A. Accept
B. Avoid
C. Transfer
D. Mitigate

Answer: D

NEW QUESTION 202
An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.
Which of the following side-channel attacks did the team use?

A. Differential power analysis
B. Differential fault analysis
C. Differential temperature analysis
D. Differential timing analysis

Answer: B

Explanation:
"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults—unexpected environmental conditions—into cryptographic operations, to reveal their internal states."

NEW QUESTION 206
A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization.
Which of the following should be the analyst's FIRST action?

A. Create a full inventory of information and data assets.
B. Ascertain the impact of an attack on the availability of crucial resources.
C. Determine which security compliance standards should be followed.
D. Perform a full system penetration test to determine the vulnerabilities.

Answer: A

Explanation:
This is because a risk assessment requires identifying the assets that are valuable to the organization and could be targeted by attackers. A full inventory of information and data assets can help the analyst prioritize the most critical assets and determine their potential exposure to threats. Without knowing what assets are at stake, the analyst cannot effectively assess the risk level or the impact of an attack. Creating an inventory of assets is also a prerequisite for performing other actions, such as following compliance standards, measuring availability, or conducting penetration tests.

NEW QUESTION 210
The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.
Which of the following testing methods would be BEST for the engineer to utilize in this situation?

A. Software composition analysis
B. Code obfuscation
C. Static analysis
D. Dynamic analysis

Answer: C

NEW QUESTION 215
A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.
* Transactions being required by unauthorized individual
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attacker using email to distribute malware and ransom ware.
* Exfiltration of sensitivity company information.
The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

Explanation:
Data loss prevention (DLP) is the best option to resolve the board's concerns for this email migration. DLP is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block email messages based on predefined rules and criteria, such as content, sender, recipient, attachment, etc. DLP can help protect transactions, customer data, and company information from being compromised by malicious actors or accidental leaks. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how- does-it-work.html

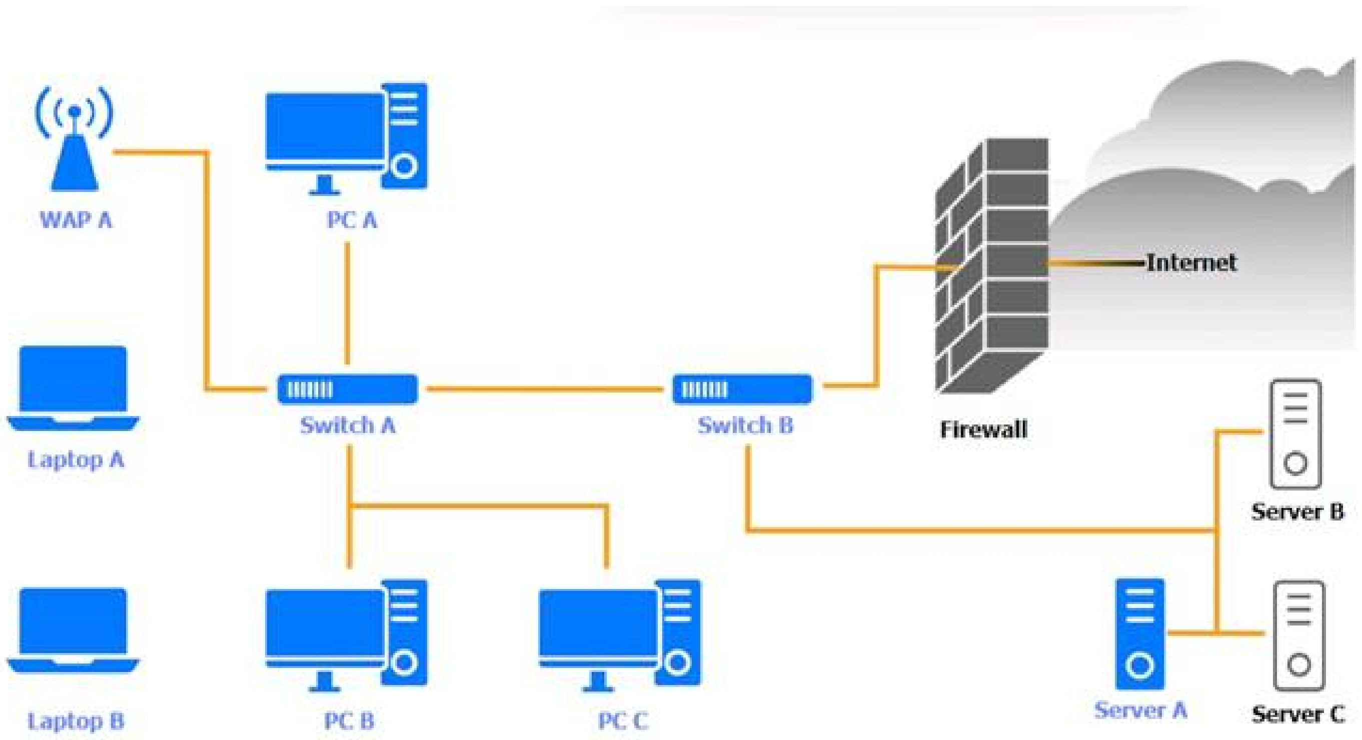
NEW QUESTION 217
A security architect Is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been Implemented to prevent these types of risks?

A. Code reviews
B. Supply chain visibility
C. Software audits
D. Source code escrows

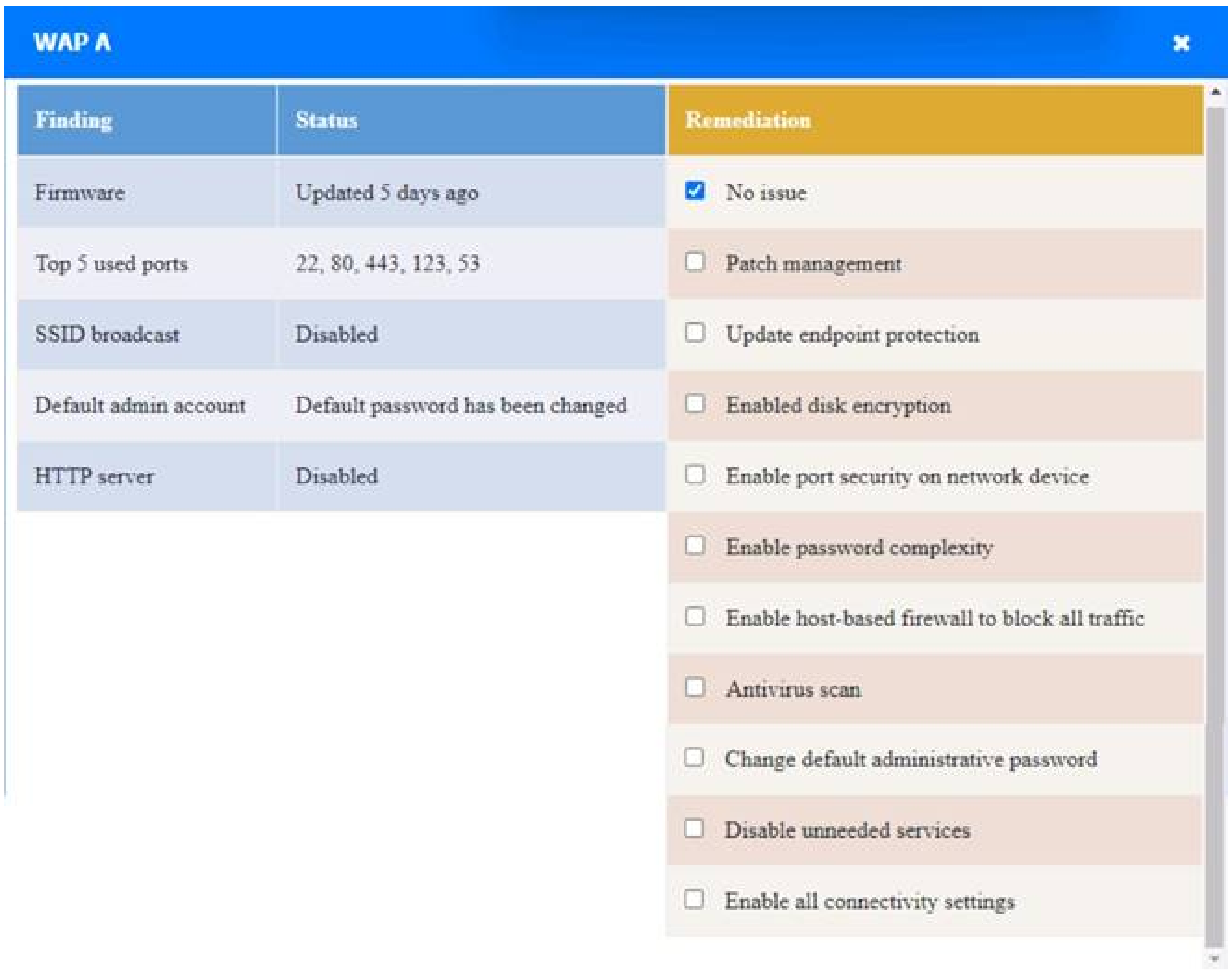
Answer: D

Explanation:
A source code escrow is a legal agreement that involves a third party holding the source code of a software application on behalf of the software vendor and the software licensee. The source code escrow ensures that the licensee can access the source code in case the vendor goes out of business, fails to provide maintenance or support, or breaches the contract terms.
A source code escrow would have prevented the risk of having an old application that is not covered for maintenance anymore because the software company is no longer in business, because it would:
? Allow the licensee to obtain the source code and continue to update, fix, or modify
the application according to their needs.
? Protect the vendor's intellectual property rights and prevent unauthorized disclosure or use of the source code.
? Provide a legal framework and a trusted mediator for resolving any disputes or issues between the vendor and the licensee.

NEW QUESTION 218
SIMULATION
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:
• The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
• The SSH daemon on the database server must be configured to listen to port 4022.
• The SSH daemon must only accept connections from a Single workstation.
• All host-based firewalls must be disabled on all workstations.
• All devices must have the latest updates from within the past eight days.
• All HDDs must be configured to secure data at rest.
• Cleartext services are not allowed.
• All devices must be hardened when possible.
Instructions:
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



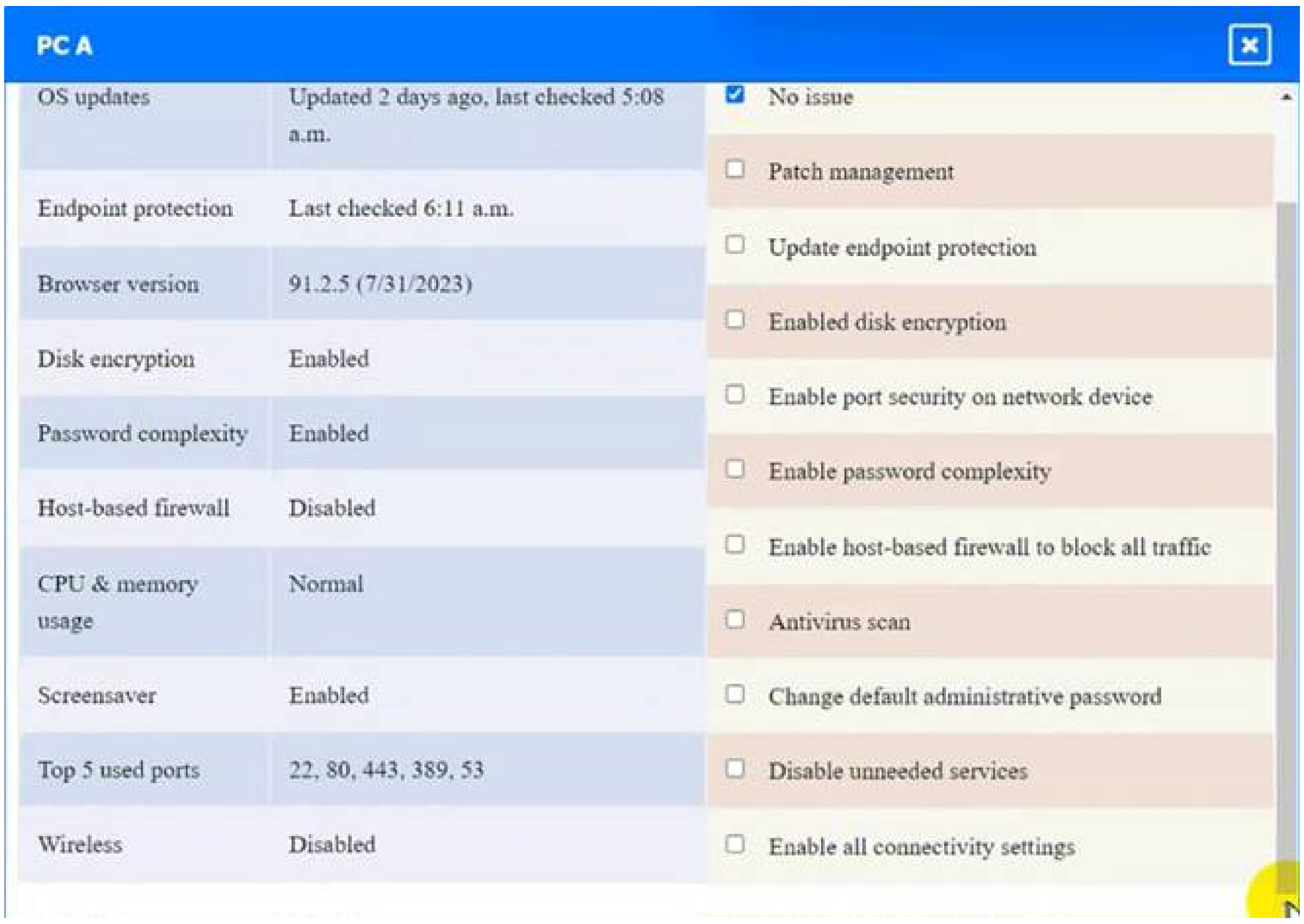
WAP A



WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	□ Patch management
SSID broadcast	Disabled	□ Update endpoint protection
Default admin account	Default password has been changed	□ Enabled disk encryption
HTTP server	Disabled	□ Enable port security on network device
		□ Enable password complexity
		□ Enable host-based firewall to block all traffic
		□ Antivirus scan
		□ Change default administrative password
		□ Disable unneeded services
		□ Enable all connectivity settings

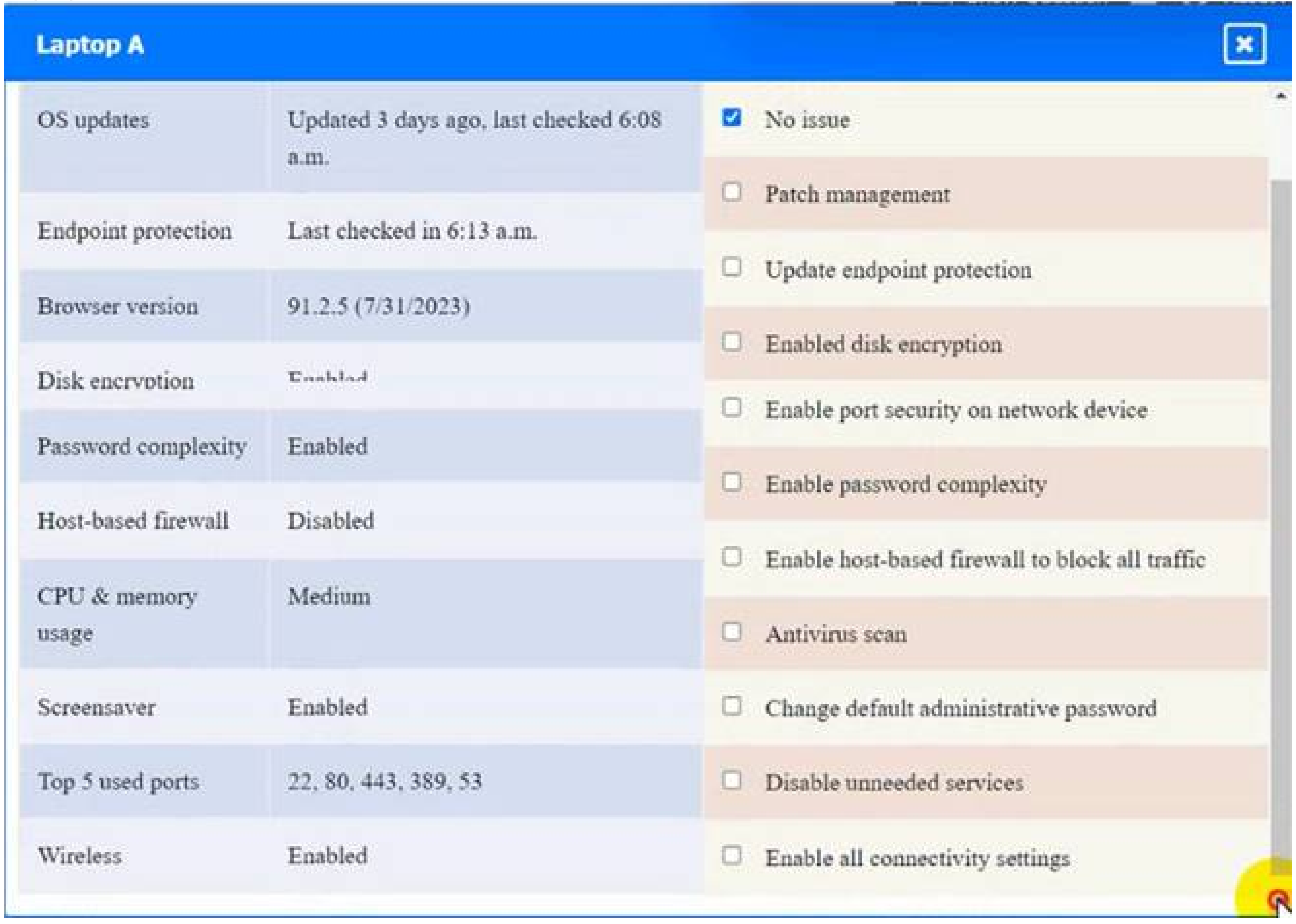
PC A



OS updates	Updated 2 days ago, last checked 5:08 a.m.
Endpoint protection	Last checked 6:11 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

- ☑ No issue
- □ Patch management
- □ Update endpoint protection
- □ Enabled disk encryption
- □ Enable port security on network device
- □ Enable password complexity
- □ Enable host-based firewall to block all traffic
- □ Antivirus scan
- □ Change default administrative password
- □ Disable unneeded services
- □ Enable all connectivity settings

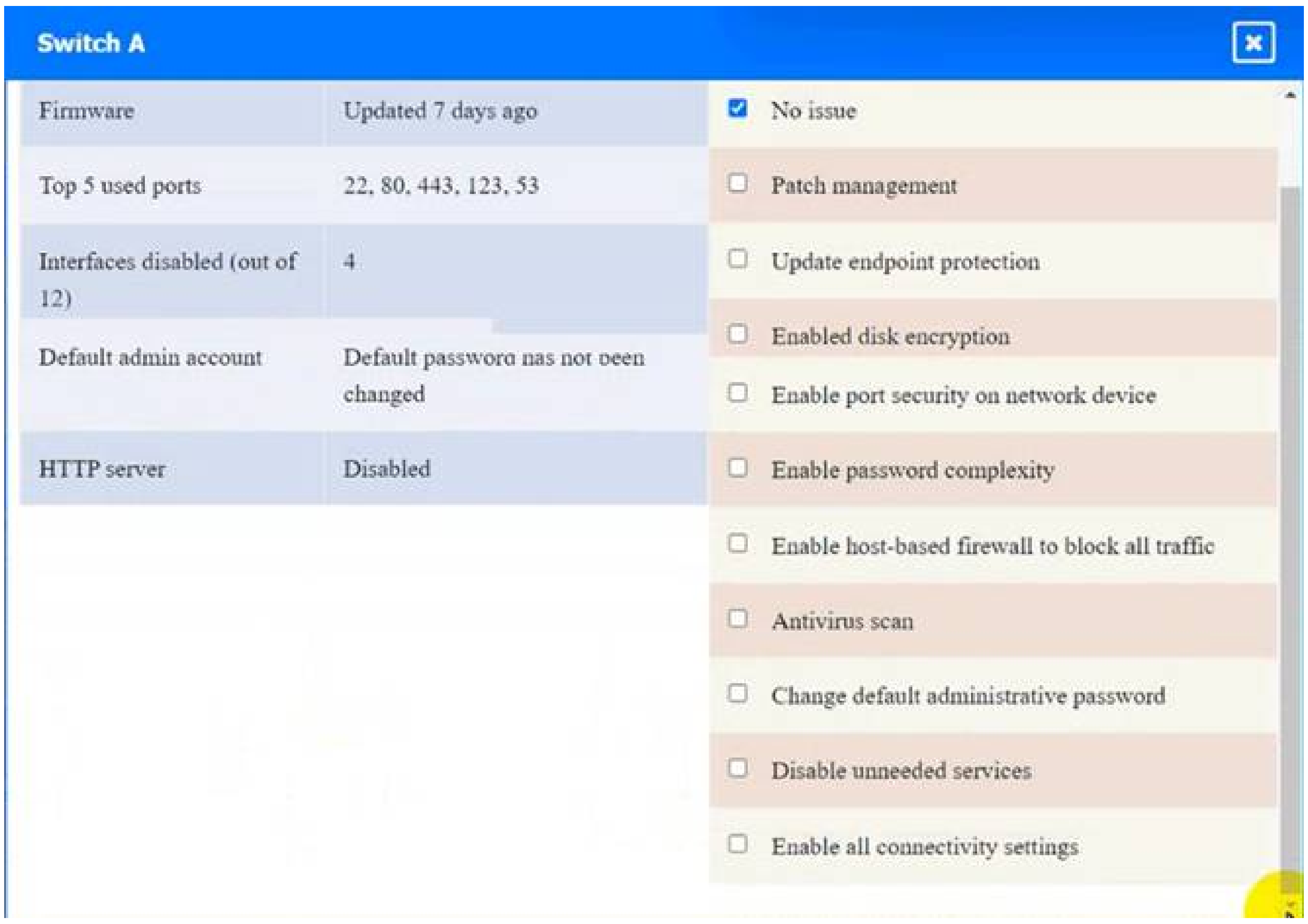
Laptop A



OS updates	Updated 3 days ago, last checked 6:08 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Enabled

- ☑ No issue
- □ Patch management
- □ Update endpoint protection
- □ Enabled disk encryption
- □ Enable port security on network device
- □ Enable password complexity
- □ Enable host-based firewall to block all traffic
- □ Antivirus scan
- □ Change default administrative password
- □ Disable unneeded services
- □ Enable all connectivity settings

Switch A

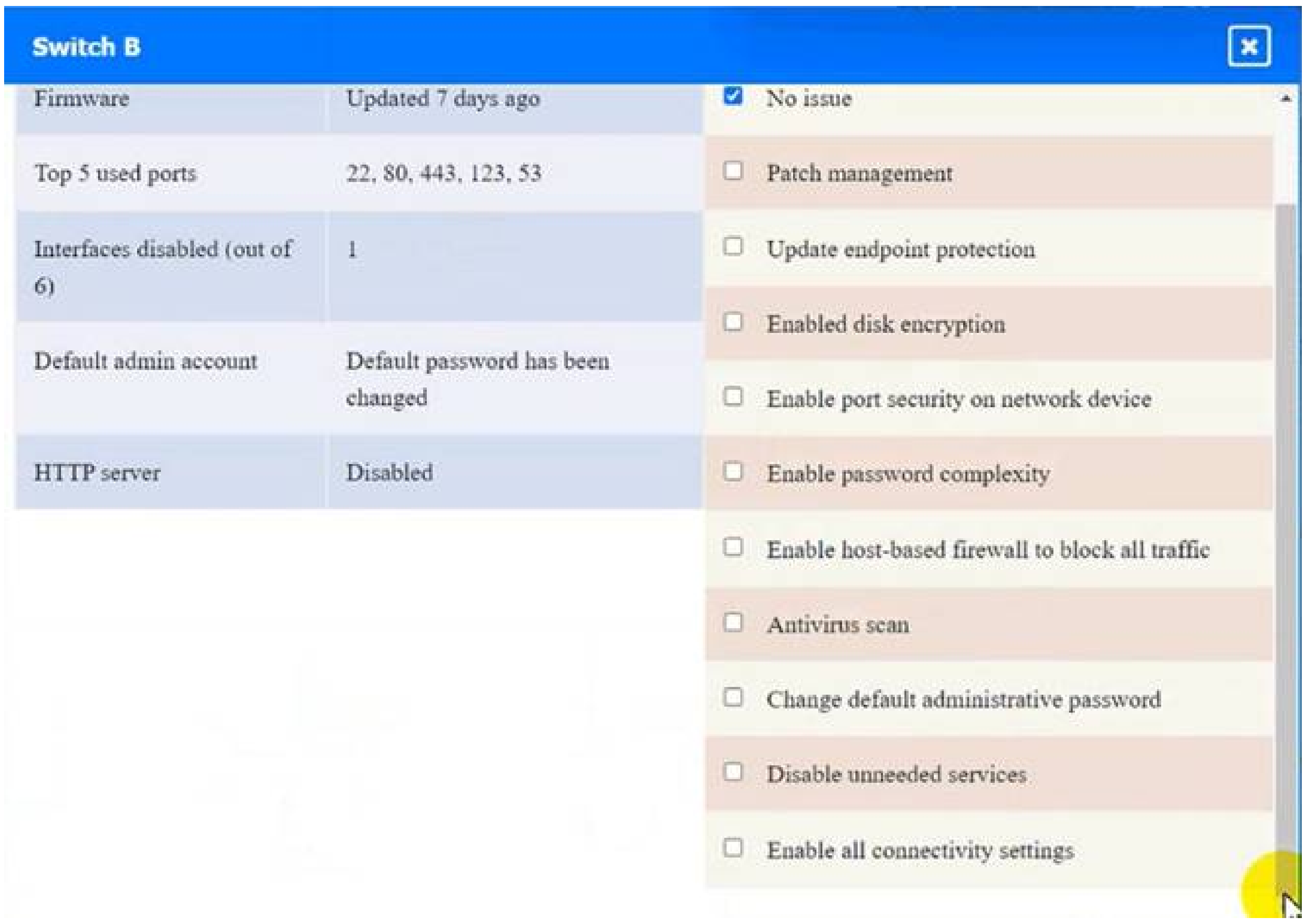


Switch A

Firmware	Updated 7 days ago
Top 5 used ports	22, 80, 443, 123, 53
Interfaces disabled (out of 12)	4
Default admin account	Default password has not been changed
HTTP server	Disabled

- ☑ No issue
- □ Patch management
- □ Update endpoint protection
- □ Enabled disk encryption
- □ Enable port security on network device
- □ Enable password complexity
- □ Enable host-based firewall to block all traffic
- □ Antivirus scan
- □ Change default administrative password
- □ Disable unneeded services
- □ Enable all connectivity settings

Switch B:

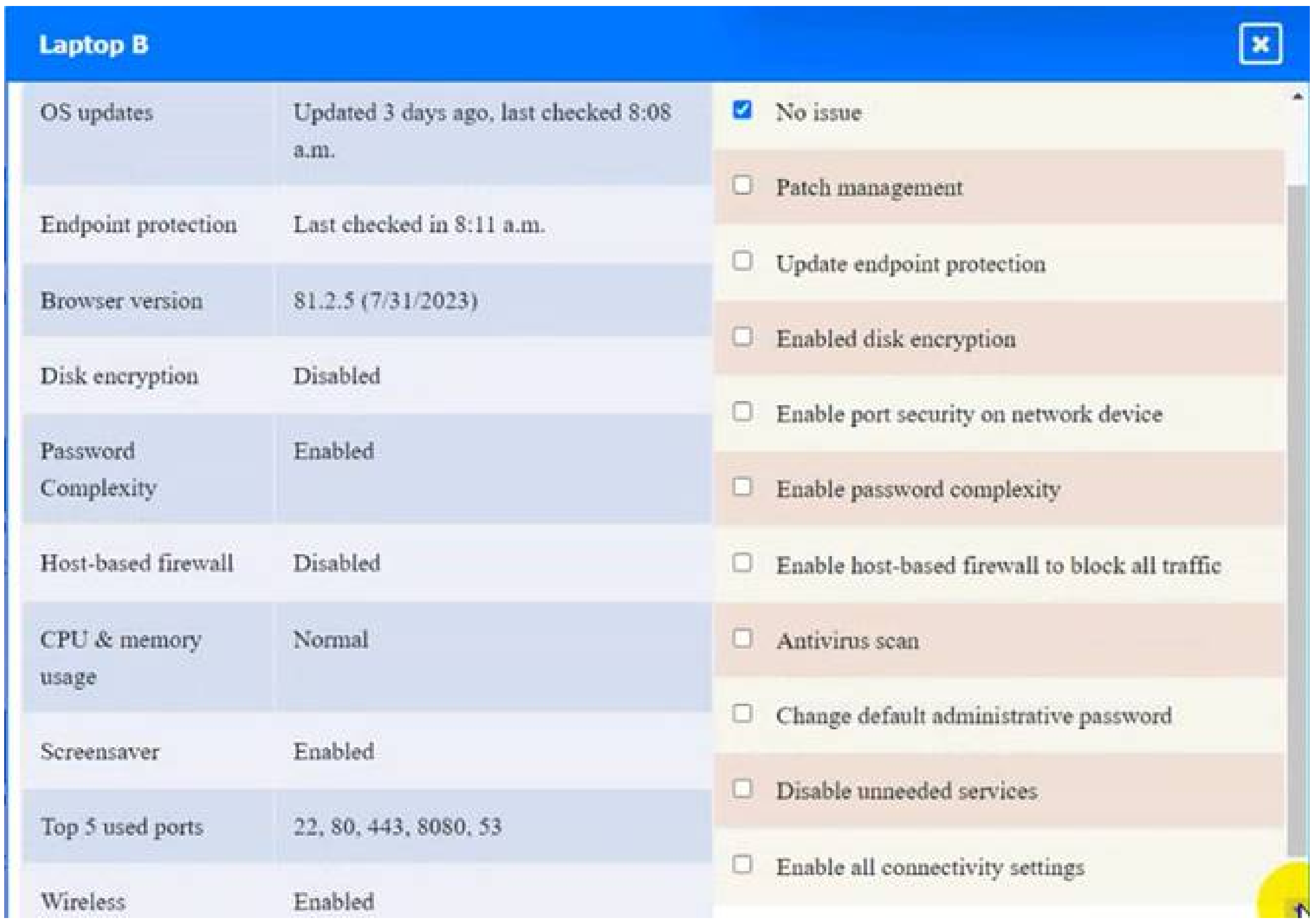


Switch B

Firmware	Updated 7 days ago
Top 5 used ports	22, 80, 443, 123, 53
Interfaces disabled (out of 6)	1
Default admin account	Default password has been changed
HTTP server	Disabled

- ☑ No issue
- □ Patch management
- □ Update endpoint protection
- □ Enabled disk encryption
- □ Enable port security on network device
- □ Enable password complexity
- □ Enable host-based firewall to block all traffic
- □ Antivirus scan
- □ Change default administrative password
- □ Disable unneeded services
- □ Enable all connectivity settings

Laptop B

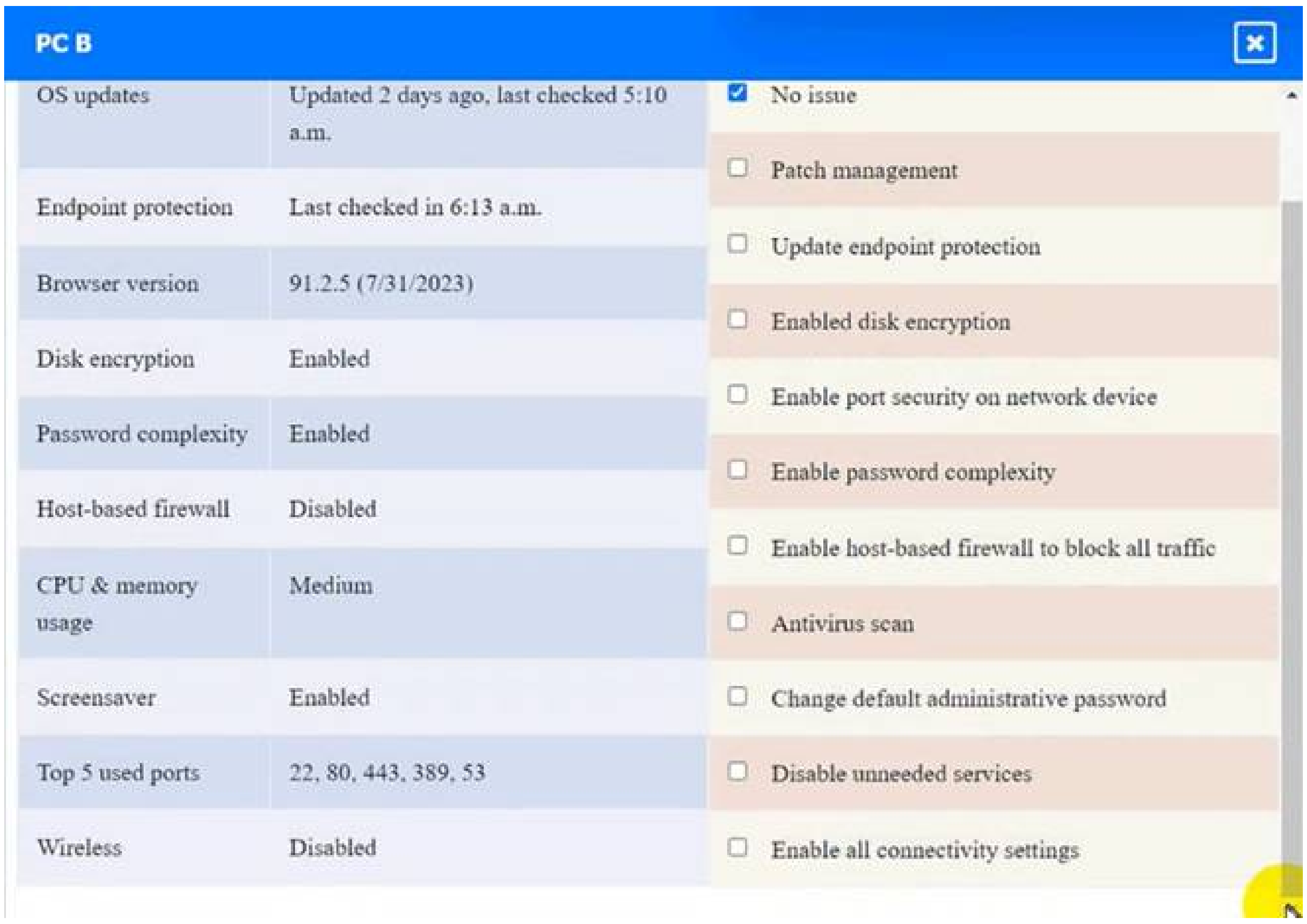


Laptop B

OS updates	Updated 3 days ago, last checked 8:08 a.m.
Endpoint protection	Last checked in 8:11 a.m.
Browser version	81.2.5 (7/31/2023)
Disk encryption	Disabled
Password Complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 8080, 53
Wireless	Enabled

☑ No issue
☐ Patch management
☐ Update endpoint protection
☐ Enabled disk encryption
☐ Enable port security on network device
☐ Enable password complexity
☐ Enable host-based firewall to block all traffic
☐ Antivirus scan
☐ Change default administrative password
☐ Disable unneeded services
☐ Enable all connectivity settings

PC B

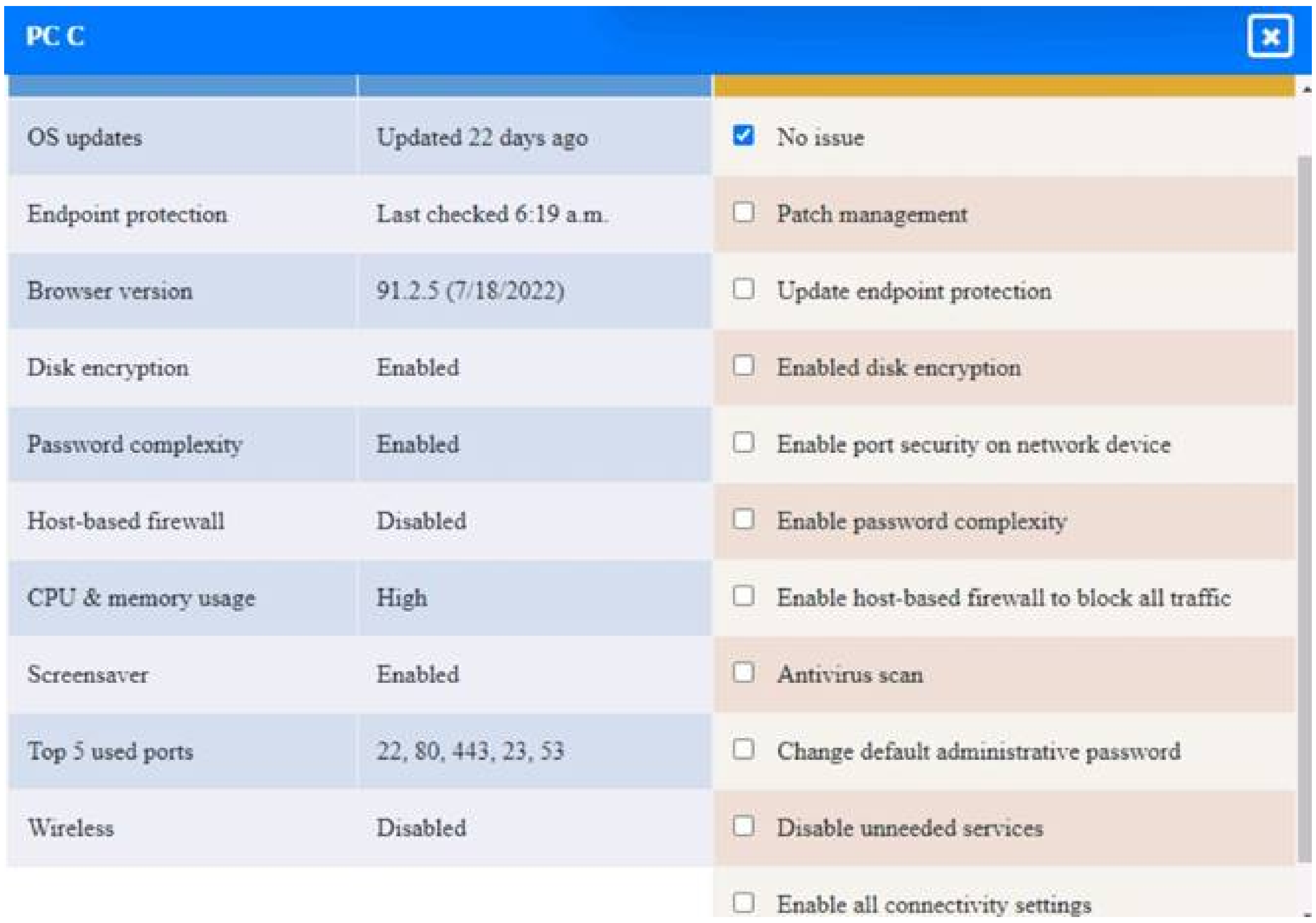


PC B

OS updates	Updated 2 days ago, last checked 5:10 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

☑ No issue
☐ Patch management
☐ Update endpoint protection
☐ Enabled disk encryption
☐ Enable port security on network device
☐ Enable password complexity
☐ Enable host-based firewall to block all traffic
☐ Antivirus scan
☐ Change default administrative password
☐ Disable unneeded services
☐ Enable all connectivity settings

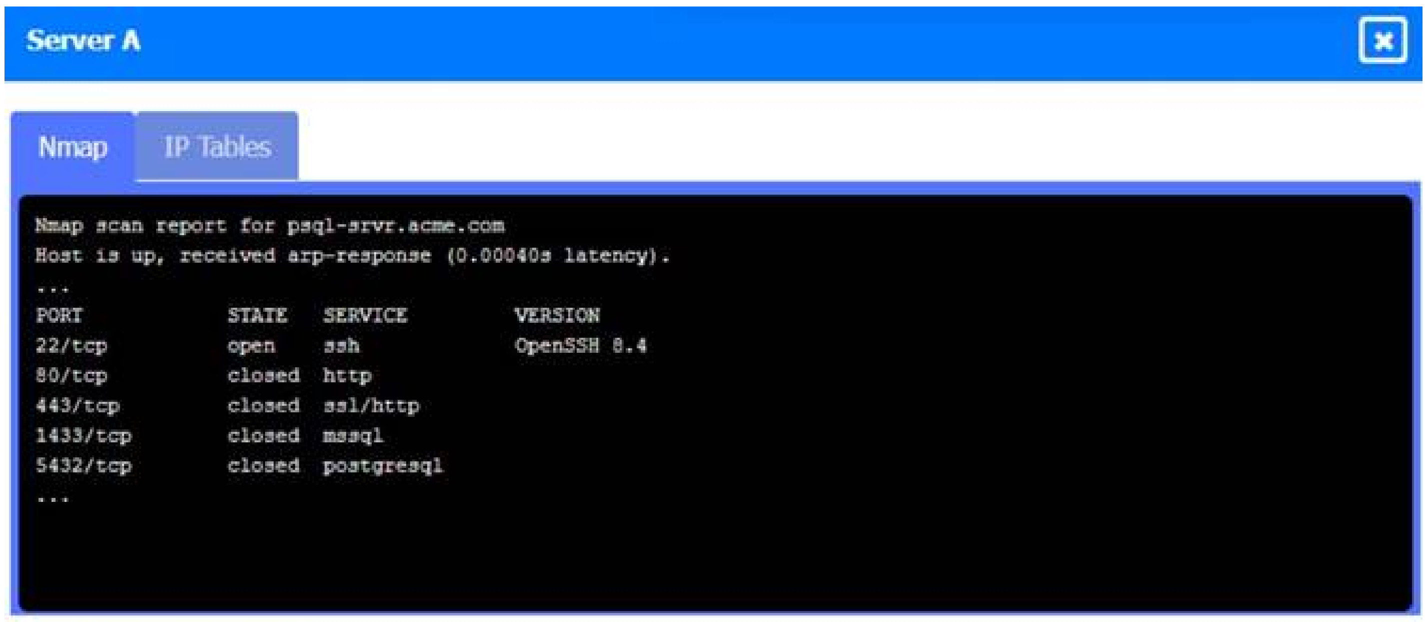
PC C



PC C

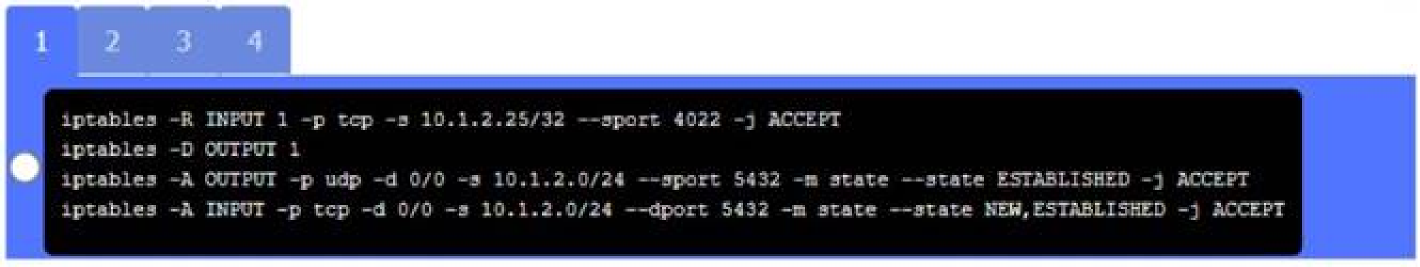
OS updates	Updated 22 days ago	☑ No issue
Endpoint protection	Last checked 6:19 a.m.	□ Patch management
Browser version	91.2.5 (7/18/2022)	□ Update endpoint protection
Disk encryption	Enabled	□ Enabled disk encryption
Password complexity	Enabled	□ Enable port security on network device
Host-based firewall	Disabled	□ Enable password complexity
CPU & memory usage	High	□ Enable host-based firewall to block all traffic
Screensaver	Enabled	□ Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	□ Change default administrative password
Wireless	Disabled	□ Disable unneeded services
		□ Enable all connectivity settings

Server A



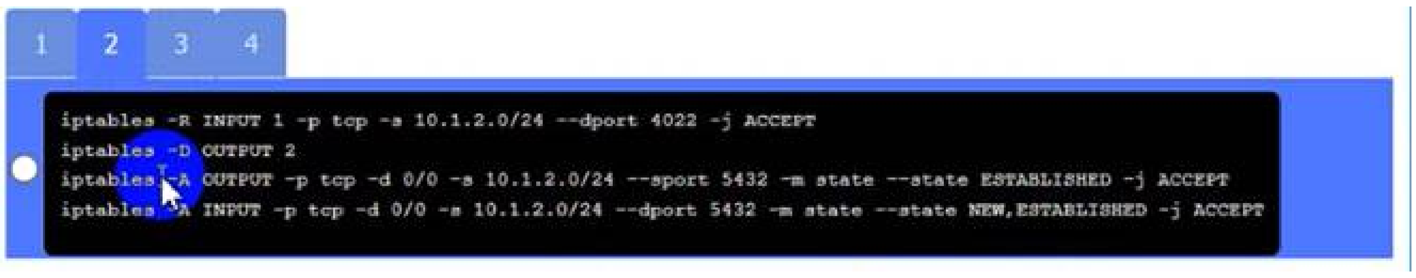
Server A

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT         STATE    SERVICE       VERSION
22/tcp       open     ssh           OpenSSH 8.4
80/tcp       closed   http
443/tcp      closed   ssl/http
1433/tcp     closed   mssql
5432/tcp     closed   postgresql
...
```



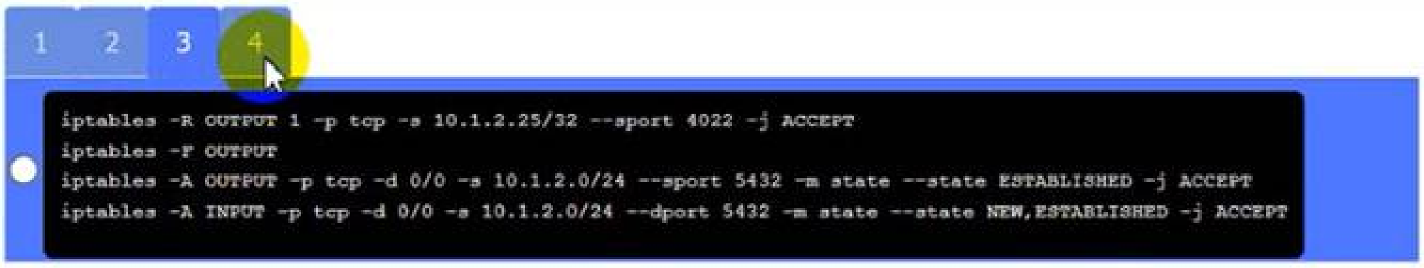
○

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



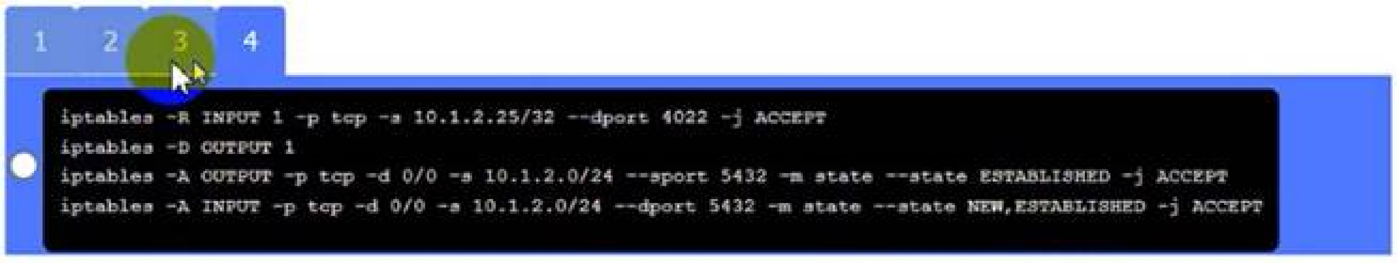
○

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



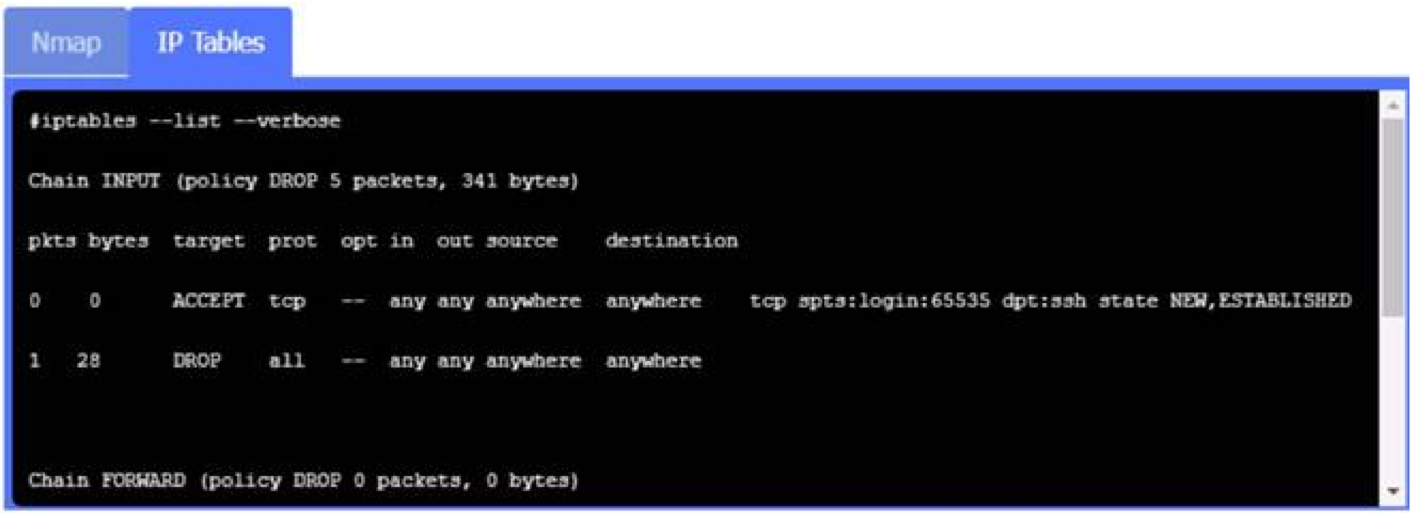
○

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



○

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

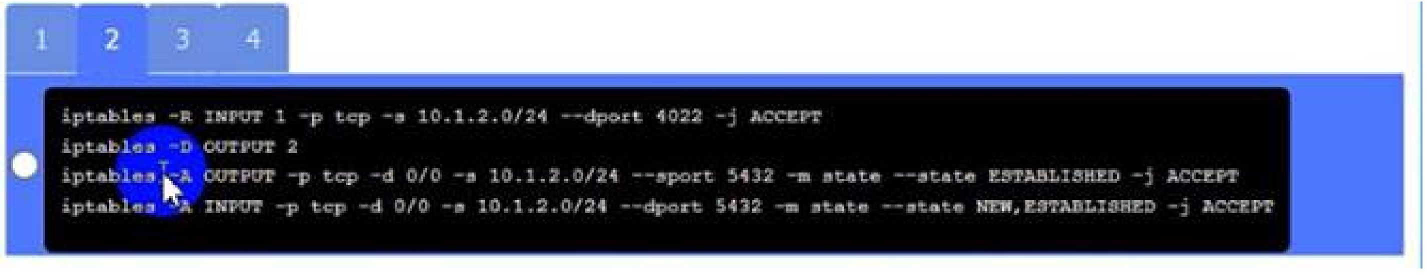


```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED

1    28     DROP    all   --  any any anywhere  anywhere


Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
WAP A: No issue found. The WAP A is configured correctly and meets the requirements. PC A = Enable host-based firewall to block all traffic
This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.
Laptop A: Patch management
This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
Laptop B: Disable unneeded services
This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet
is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.
PC B: Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.
PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config
Server A. Need to select the following:



```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

A black and white screen with white text
Description automatically generated

NEW QUESTION 222
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

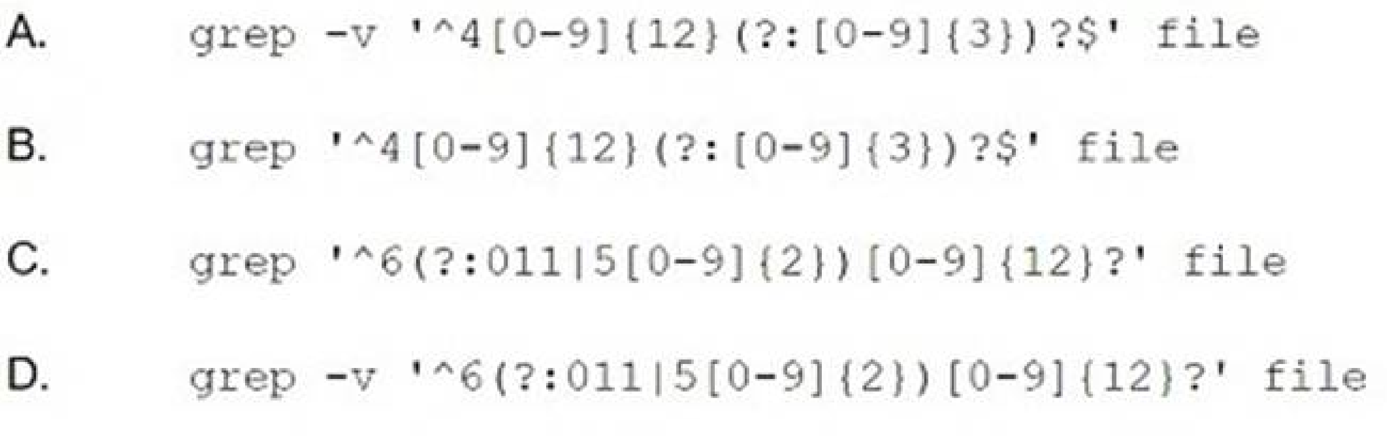
Answer: A

Explanation:
Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality

problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost- effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified References: https://www.comptia.org/blog/what-is-cloud-computing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 227

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card data.
Which of the following commands should the analyst run to BEST determine whether financial data was lost?



```
A.    grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file

B.    grep '^4[0-9]{12}(?:[0-9]{3})?$' file

C.    grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file

D.    grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file
```

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

Answer: C

NEW QUESTION 231

A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company’s Linux servers. While the software version is no longer supported by the OSS community, the company’s Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.
Based on this agreement, this finding is BEST categorized as a:

A. true positive.
B. true negative.
C. false positive.
D. false negative.

Answer: C

NEW QUESTION 236

The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:
* Transaction being requested by unauthorized individuals.
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attackers using email to malware and ransomeware.
* Exfiltration of sensitive company information.
The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the boar’s concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

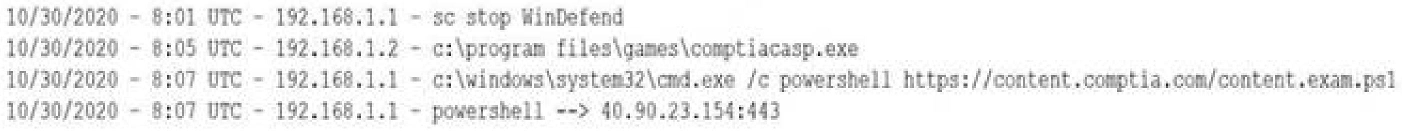
Answer: A

Explanation:

Data loss prevention (DLP) is the best option to resolve the board’s concerns for this email migration. DLP is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block email messages based on predefined rules and criteria, such as content, sender, recipient, attachment, etc. DLP can help protect transactions, customer data, and company information from being compromised by malicious actors or accidental leaks. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how- does-it-work.html

NEW QUESTION 241

A security analyst notices a number of SIEM events that show the following activity:



```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

Which of the following response actions should the analyst take FIRST?

A. Disable powershell.exe on all Microsoft Windows endpoints.
B. Restart Microsoft Windows Defender.
C. Configure the forward proxy to block 40.90.23.154.

D. Disable local administrator privileges on the endpoints.

Answer: C

Explanation:
The SIEM events show that powershell.exe was executed on multiple endpoints with an outbound connection to 40.90.23.154, which is an IP address associated with malicious activity. This could indicate a malware infection or a command-and-control channel. The best response action is to configure the forward proxy to block 40.90.23.154, which would prevent further communication with the malicious IP address. Disabling powershell.exe on all endpoints may not be feasible or effective, as it could affect legitimate operations and not remove the malware. Restarting Microsoft Windows Defender may not detect or stop the malware, as it could have bypassed or disabled it. Disabling local administrator privileges on the endpoints may not prevent the malware from running or communicating, as it could have escalated privileges or used other methods. Verified References: https://www.comptia.org/blog/what-is-a-forward-proxy https://partners.comptia.org/docs/default-source/resources/casp-content-guide

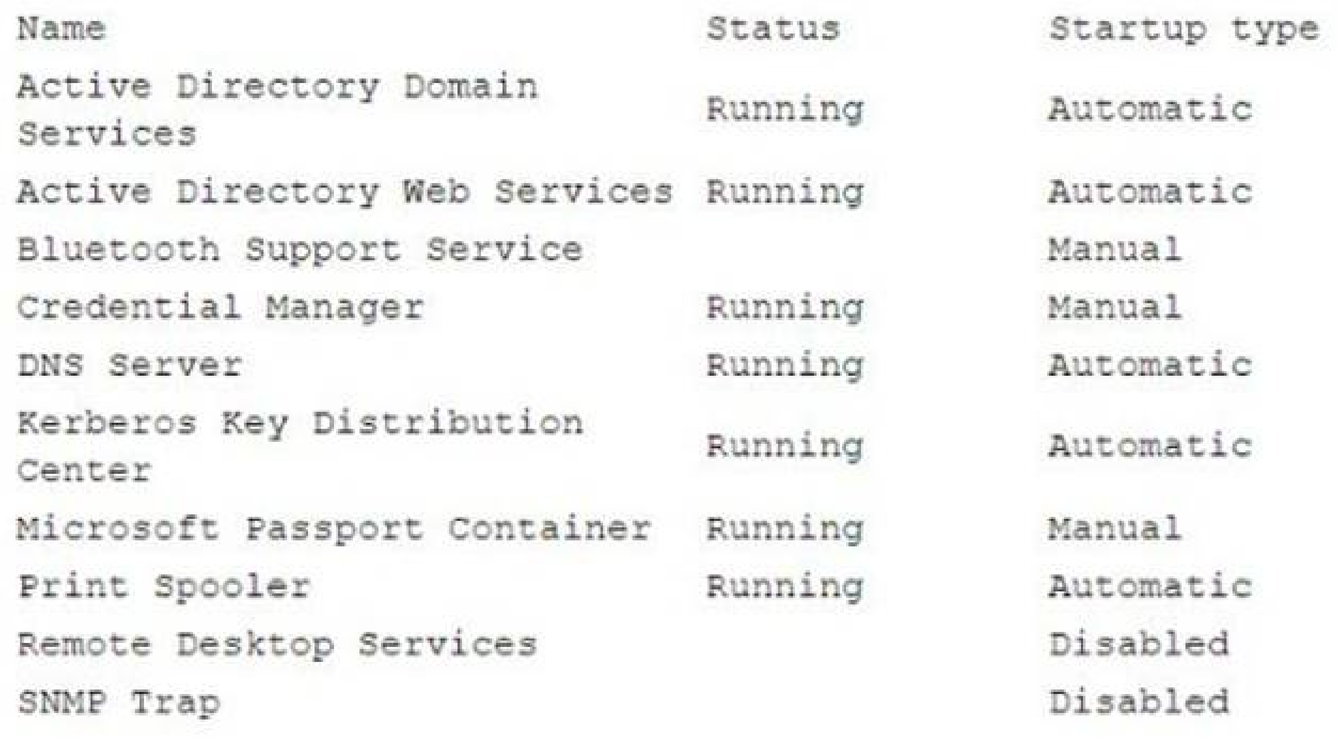
NEW QUESTION 245
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based

Answer: B

Explanation:
We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage. https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

NEW QUESTION 250
A security administrator has been tasked with hardening a domain controller against lateral movement attacks. Below is an output of running services:



Name	Status	Startup type
Active Directory Domain Services	Running	Automatic
Active Directory Web Services	Running	Automatic
Bluetooth Support Service		Manual
Credential Manager	Running	Manual
DNS Server	Running	Automatic
Kerberos Key Distribution Center	Running	Automatic
Microsoft Passport Container	Running	Manual
Print Spooler	Running	Automatic
Remote Desktop Services		Disabled
SNMP Trap		Disabled

Which of the following configuration changes must be made to complete this task?

A. Stop the Print Spooler service and set the startup type to disabled.
B. Stop the DNS Server service and set the startup type to disabled.
C. Stop the Active Directory Web Services service and set the startup type to disabled.
D. Stop Credential Manager service and leave the startup type to disabled.

Answer: A

Explanation:
Stopping the Print Spooler service and setting the startup type to disabled is the best configuration change to harden a domain controller against lateral movement attacks. The Print Spooler service has been known to be vulnerable to remote code execution exploits that can allow attackers to gain access to domain controllers and other sensitive machines. Disabling this service can reduce the attack surface and prevent exploitation attempts.

NEW QUESTION 253
A consultant needs access to a customer's cloud environment. The customer wants to enforce the following engagement requirements:
• All customer data must remain under the control of the customer at all times.
• Third-party access to the customer environment must be controlled by the customer.
• Authentication credentials and access control must be under the customer's control.
Which of the following should the consultant do to ensure all customer requirements are satisfied when accessing the cloud environment?

A. use the customer's SSO with read-only credentials and share data using the customer's provisioned secure network storage
B. use the customer-provided VDI solution to perform work on the customer's environment.

C. Provide code snippets to the customer and have the customer run code and securely deliver its output
D. Request API credentials from the customer and only use API calls to access the customer's environmen

Answer: B

Explanation:
The consultant should use the customer-provided VDI solution to perform work on the customer's environment. VDI stands for virtual desktop infrastructure, which is a technology that allows users to access a virtual desktop hosted on a remote server. VDI can help meet the customer's requirements by ensuring that all customer data remains under the customer's control at all times, that third-party access to the customer environment is controlled by the customer, and that authentication credentials and access control are under the customer's control. Verified References:

- https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engin
- https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

NEW QUESTION 254
A security analyst is reviewing SIEM events and is uncertain how to handle a particular event. The file is reviewed with the security vendor who is aware that this type of file routinely triggers this alert.
Based on this information, the security analyst acknowledges this alert Which of the following event classifications is MOST likely the reason for this action?

A. True negative
B. False negative
C. False positive
D. Non-automated response

Answer: C

Explanation:
The security analyst acknowledges this alert because it is a false positive. A false positive is an event classification that indicates a benign or normal activity is mistakenly flagged as malicious or suspicious by the SIEM system. A false positive can occur due to misconfigured rules, outdated signatures, or faulty algorithms. A false positive can waste the security analyst's time and resources, so it is important to acknowledge and dismiss it after verifying that it is not a real threat. Verified References:

- https://www.ibm.com/topics/siem
- https://www.microsoft.com/en-us/security/business/security-101/what-is-siem
- https://www.splunk.com/en_us/data-insider/what-is-siem.html

NEW QUESTION 259
An administrator at a software development company would like to protect the integrity of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers
B. The CA has included the certificate in its CR
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate

Answer: C

Explanation:
The most likely cause of the signature failing is that the certificate is set for the wrong key usage. Key usage is an extension of a certificate that defines the purpose and functionality of the public key contained in the certificate. Key usage can include digital signature, key encipherment, data encipherment, certificate signing, and others. If the certificate is set for a different key usage than digital signature, it will not be able to sign the applications properly. The administrator should check the key usage extension of the certificate and make sure it matches the intended purpose. Verified References:

- https://www.wintips.org/how-to-fix-windows-cannot-verify-the-digital-signature-for-this-file-error-in-win
- https://softwaretested.com/mac/how-to-fix-a-digital-signature-error-on-windows-10/
- https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-2

NEW QUESTION 261
The analyst should implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics. This approach would allow the analyst to test each solution individually and measure its effectiveness against the attack, without affecting the other solutions or the production environment. This would also minimize the downtime required to implement the best solution, as only one change would be needed. The other options would either involve implementing multiple solutions at once, which could cause conflicts or errors, or collecting metrics before running the attack simulation, which would not reflect the actual impact of the solutions.
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

A. E-discovery
B. Review analysis
C. Information governance
D. Chain of custody

Answer: A

Explanation:
The process that involves searching and collecting evidence during an investigation or lawsuit is e-discovery. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can be used for civil litigation, criminal prosecution, regulatory compliance, internal investigations, and other purposes. E-discovery can help parties obtain evidence from various sources, such as emails, documents, databases, social media, cloud services, mobile devices, and others. Verified References:

- https://www.techtarget.com/searchsecurity/definition/electronic-discovery
- https://www.edrm.net/frameworks-and-standards/edrm-model/
- https://www.law.cornell.edu/wex/electronic_discovery_(federal)

NEW QUESTION 266
A security analyst has been tasked with providing key information in the risk register. Which of the following outputs or results would be used to BEST provide the information needed to determine the security posture for a risk decision? (Select TWO).

A. Password cracker
B. SCAP scanner
C. Network traffic analyzer
D. Vulnerability scanner
E. Port scanner
F. Protocol analyzer

Answer: BD

Explanation:
The tools that can be used to provide key information in the risk register are SCAP scanner and vulnerability scanner. SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications for automating the management of security configuration, vulnerability assessment, and compliance evaluation. SCAP scanner is a tool that can scan systems and networks for security issues based on SCAP content. Vulnerability scanner is a tool that can scan systems and networks for known vulnerabilities and weaknesses. These tools can help the security analyst identify and prioritize the risks associated with the systems and networks, as well as provide possible remediation actions. Verified References:

- https://www.techtarget.com/searchsecurity/definition/Security-Content-Automation-Protocol
- https://learn.microsoft.com/en-us/azure/security/fundamentals/vulnerability-management
- https://www.techtarget.com/searchsecurity/definition/vulnerability-scanner

NEW QUESTION 268
In comparison with traditional on-premises infrastructure configurations, defining ACLs in a CSP relies on:

A. cloud-native applications.
B. containerization.
C. serverless configurations.
D. software-defined netWorkin
E. secure access service edge.

Answer: D

Explanation:
Defining ACLs in a CSP relies on software-defined networking. Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane, allowing for centralized and programmable network management. SDN can enable dynamic and flexible network configuration and optimization, as well as improved security and performance. In a CSP, SDN can be used to define ACLs that can apply to virtual networks, subnets, or interfaces, regardless of the physical infrastructure. SDN can also allow for granular and consistent ACL enforcement across different cloud services and regions. Verified References:

- https://www.techtarget.com/searchsdn/definition/software-defined-networking-SDN
- https://learn.microsoft.com/en-us/azure/architecture/guide/networking/network-security
- https://www.techtarget.com/searchcloudcomputing/definition/cloud-networking

NEW QUESTION 272
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
• Mobile clients should verify the identity of all social media servers locally.
• Social media servers should improve TLS performance of their certificate status
• Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Answer: BF

Explanation:
The company should implement OCSP stapling and HSTS to improve TLS performance and enforce HTTPS. OCSP stapling is a technique that allows a server to provide a signed proof of the validity of its certificate along with the TLS handshake, instead of relying on the client to contact the certificate authority (CA) for verification. This can reduce the latency and bandwidth of the TLS handshake, as well as improve the privacy and security of the certificate status. HSTS stands for HTTP Strict Transport Security, which is a mechanism that instructs browsers to only use HTTPS when connecting to a website, and to reject any unencrypted or invalid connections. This can prevent downgrade attacks, man-in-the-middle attacks, and mixed content errors, as well as improve the performance of HTTPS connections by avoiding unnecessary redirects. Verified References:

- https://www.techtarget.com/searchsecurity/definition/OCSP-stapling
- https://www.techtarget.com/searchsecurity/definition/HTTP-Strict-Transport-Security
- https://www.cloudflare.com/learning/ssl/what-is-hsts/

NEW QUESTION 273
An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?

A. Properly configure a secure file transfer system to ensure file integrity.
B. Have the external parties sign non-disclosure agreements before sending any image
C. Only share images with external parties that have worked with the firm previousl
D. Utilize watermarks in the images that are specific to each external party.

Answer: D

Explanation:
Watermarking is a technique of adding an identifying image or pattern to an original image to protect its ownership and authenticity. Watermarks can be customized to include specific information about the external party, such as their name, logo, or date of receipt. This way, if any draft images are leaked to the public, the firm can trace back the source of the leak and take appropriate actions. Verified References:

- https://en.wikipedia.org/wiki/Watermark
- https://www.canva.com/features/watermark-photos/
- https://www.mdpi.com/2078-2489/11/2/110

NEW QUESTION 276
A local university that has a global footprint is undertaking a complete overhaul of its website and associated systems. Some of the requirements are:
• Handle an increase in customer demand of resources
• Provide quick and easy access to information
• Provide high-quality streaming media
• Create a user-friendly interface
Which of the following actions should be taken FIRST?

A. Deploy high-availability web server
B. Enhance network access controls.
C. Implement a content delivery networ
D. Migrate to a virtualized environment.

Answer: C

Explanation:
A content delivery network (CDN) is a geographically distributed network of servers that can cache content close to end users, allowing for faster and more efficient delivery of web content, such as images, videos, and streaming media. A CDN can also handle an increase in customer demand of resources, provide high-quality streaming media, and create a user-friendly interface by reducing latency and bandwidth consumption. A CDN can also improve the security and availability of the website by mitigating DDoS attacks and providing redundancy. Verified References:

- https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
- https://learn.microsoft.com/en-us/azure/cdn/cdn-overview
- https://en.wikipedia.org/wiki/Content_delivery_network

NEW QUESTION 279
The CI/CD pipeline requires code to have close to zero defects and zero vulnerabilities. The current process for any code releases into production uses two-week Agile sprints. Which of the following would BEST meet the requirement?

A. An open-source automation server
B. A static code analyzer
C. Trusted open-source libraries
D. A single code repository for all developers

Answer: B

Explanation:
A static code analyzer is a tool that analyzes computer software without actually running the software. A static code analyzer can help developers find and fix vulnerabilities, bugs, and security risks in their new applications while the source code is in its 'static' state. A static code analyzer can help ensure that the code has close to zero defects and zero vulnerabilities by checking the code against a set of coding rules, standards, and best practices. A static code analyzer can also help improve the code quality, performance, and maintainability.
* A. An open-source automation server is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. An open-source automation server is a tool that automates various tasks related to software development and delivery, such as building, testing, deploying, and monitoring. An open-source automation server can help speed up the CI/CD pipeline, but it does not analyze or improve the code itself.
* C. Trusted open-source libraries are not tools that can help ensure that the code has close to zero defects and zero vulnerabilities. Trusted open-source libraries are collections of reusable code that developers can use to implement common or complex functionalities in their applications. Trusted open-source libraries can help save time and effort for developers, but they do not guarantee that the code is free of defects or vulnerabilities.
* D. A single code repository for all developers is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. A single code repository for all developers is a centralized storage location where developers can access and manage their source code files. A single code repository for all developers can help facilitate collaboration and version control, but it does not analyze or improve the code itself.
https://www.comparitech.com/net-admin/best-static-code-analysis-tools/ https://www.perforce.com/blog/sca/what-static-analysis

NEW QUESTION 280
Which of the following describes the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely?

A. Key escrow
B. TPM
C. Trust models
D. Code signing

Answer: A

Explanation:
Key escrow is the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow by a trusted third party that can release them under certain conditions. Key escrow can be useful for backup or recovery purposes, or for complying with legal or regulatory requirements that may demand access to encrypted data.
* B. TPM is not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. TPM stands for Trusted Platform Module, which is a hardware device that provides secure storage and generation of cryptographic keys on a computer. TPM does not involve any third party or escrow service.
* C. Trust models are not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Trust models are frameworks that define how entities can establish and maintain trust relationships in a network or system. Trust models do not necessarily involve any third party or escrow service.
* D. Code signing is not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Code signing is a process of using digital signatures to verify the authenticity and integrity of software code. Code signing does not involve any third party or escrow service.

NEW QUESTION 285
An organization is looking to establish more robust security measures by implementing PKI. Which of the following should the security analyst implement when considering mutual authentication?

A. Perfect forward secrecy on both endpoints
B. Shared secret for both endpoints
C. Public keys on both endpoints
D. A common public key on each endpoint
E. A common private key on each endpoint

Answer: C

Explanation:
Public keys on both endpoints are required for implementing PKI-based mutual authentication. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates are issued by trusted authorities called Certificate Authorities (CAs), and can be used to prove the identity and authenticity of the certificate holders. Mutual authentication is a process in which two parties authenticate each other at the same time using certificates. Mutual authentication can provide stronger security and privacy than one-way authentication, where only one party is authenticated. In PKI-based mutual authentication, each party has a certificate that contains its public key and identity information, and a private key that corresponds to its public key. The private key is kept secret and never shared with anyone, while the public key is shared and used to verify the identity and signature of the certificate holder. The basic steps of PKI-based mutual authentication are as follows:

- Party A sends its certificate to Party B.
- Party B verifies Party A's certificate by checking its validity, signature, and trust chain. If the certificate is valid and trusted, Party B extracts Party A's public key from the certificate.
- Party B generates a random challenge (such as a nonce or a timestamp) and encrypts it with Party A's public key. Party B sends the encrypted challenge to Party A.
- Party A decrypts the challenge with its private key and sends it back to Party B.
- Party B compares the received challenge with the original one. If they match, Party B confirms that Party A is the legitimate owner of the certificate and has possession of the private key.
- The same steps are repeated in reverse, with Party A verifying Party B's certificate and sending a challenge encrypted with Party B's public key.

* A. Perfect forward secrecy on both endpoints is not required for implementing PKI-based mutual authentication. Perfect forward secrecy (PFS) is a property of encryption protocols that ensures that the compromise of a long-term secret key (such as a private key) does not affect the security of past or future session keys (such as symmetric keys). PFS can enhance the security and privacy of encrypted communications, but it does not provide authentication by itself.
* B. Shared secret for both endpoints is not required for implementing PKI-based mutual authentication. Shared secret is a method of authentication that relies on a pre-shared piece of information (such as a password or a passphrase) that is known only to both parties. Shared secret can provide simple and fast authentication, but it does not provide non-repudiation or identity verification.
* D. A common public key on each endpoint is not required for implementing PKI-based mutual authentication. A common public key on each endpoint would imply that both parties share the same certificate and private key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.
* E. A common private key on each endpoint is not required for implementing PKI-based mutual authentication. A common private key on each endpoint would imply that both parties share the same certificate and public key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.

NEW QUESTION 290
......