- **Vendor:** CompTIA
- **Exam Code:** CAS-003
- **Exam Name:** CompTIA Advanced Security Practitioner (CASP)
- **New Updated Questions from Braindump2go (Updated in Dec./2020)**

QUESTION 630
A security administrator is concerned about employees connecting their personal devices to the company network. Doing so is against company policy.
The network does not have a NAC solution.
The company uses a GPO that disables the firewall on all company-owned devices while they are connected to the internal network.
Additionally, all company-owned devices implement a standard naming convention that uses the device's serial number.
The security administrator wants to identify active personal devices and write a custom script to disconnect them from the network.
Which of the following should the script use to BEST accomplish this task?

A. Recursive DNS logs
B. DHCP logs
C. AD authentication logs
D. RADIUS logs
E. Switch and router ARP tables

Answer: E

QUESTION 631
An organization designs and develops safety-critical embedded firmware (inclusive of embedded OS and services) for the automotive industry.
The organization has taken great care to exercise secure software development practices for the firmware Of paramount importance is the ability to defeat attacks aimed at replacing or corrupting running firmware once the vehicle leaves production and is in the field Integrating, which of the following host and OS controls would BEST protect against this threat?

A. Configure the host to require measured boot with attestation using platform configuration registers extended through the OS and into application space.
B. Implement out-of-band monitoring to analyze the state of running memory and persistent storage and, in a failure mode, signal a check-engine light condition for the operator.
C. Perform reverse engineering of the hardware to assess for any implanted logic or other supply chain integrity violations
D. Ensure the firmware includes anti-malware services that will monitor and respond to any introduction of malicious logic.
E. Require software engineers to adhere to a coding standard, leverage static and dynamic analysis within the development environment, and perform exhaustive state space analysis before deployment

Answer: D

QUESTION 632
A consultant is planning an assessment of a customer-developed system.
The system consists of a custom-engineered board with modified open-source drivers and a one-off management GUI.
The system relies on two- factor authentication for interactive sessions, employs strong certificate-based data-in-transit encryption, and randomly switches ports for each session.
Which of the following would yield the MOST useful information'?

A. Password cracker
B. Wireless network analyzer
C. Fuzzing tools
D. Reverse engineering principles

Answer: D

QUESTION 633
An organization's mobile device inventory recently provided notification that a zero-day vulnerability was identified in the code used to control the baseband of the devices.
The device manufacturer is expediting a patch, but the rollout will take several months.
Additionally several mobile users recently returned from an overseas trip and report their phones now contain unknown applications, slowing device performance.
Users have been unable to uninstall these applications, which persist after wiping the devices.
Which of the following MOST likely occurred and provides mitigation until the patches are released?

A. Unauthentic firmware was installed, disable OTA updates and carrier roaming via MDM.
B. Users opened a spear-phishing email: disable third-party application stores and validate all signed code prior to execution.
C. An attacker downloaded monitoring applications; perform a full factory reset of the affected devices.
D. Users received an improperly encoded emergency broadcast message, leading to an integrity loss condition; disable emergency broadcast messages

Answer: A

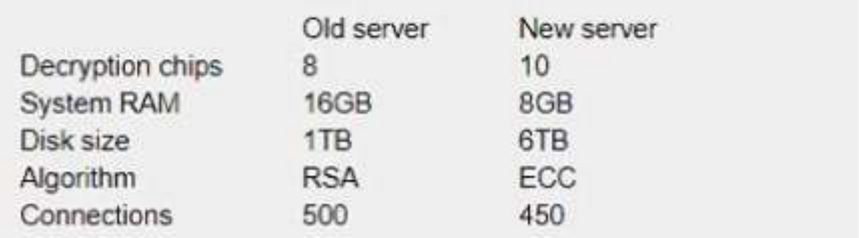
QUESTION 634
Several recent ransomware outbreaks at a company have cost a significant amount of lost revenue.
The security team needs to find a technical control mechanism that will meet the following requirements and aid in preventing these outbreaks:
- Stop malicious software that does not match a signature
- Report on instances of suspicious behavior
- Protect from previously unknown threats
- Augment existing security capabilities
Which of the following tools would BEST meet these requirements?

A. Host-based firewall
B. EDR
C. HIPS
D. Patch management

Answer: C

QUESTION 635
A technician uses an old SSL server due to budget constraints and discovers performance degrades dramatically after enabling PFS.
The technician cannot determine why performance degraded so dramatically.
A newer version of the SSL server does not suffer the same performance degradation.

Performance rather than security is the main priority for the technician
The system specifications and configuration of each system are listed below:



	Old server	New server
Decryption chips	8	10
System RAM	16GB	8GB
Disk size	1TB	6TB
Algorithm	RSA	ECC
Connections	500	450

Which of the following is MOST likely the cause of the degradation in performance and should be changed?

A. Using ECC
B. Using RSA
C. Disk size
D. Memory size
E. Decryption chips
F. Connection requests

Answer: B

QUESTION 636
A company's human resources department recently had its own shadow IT department spin up ten VMs that host a mixture of differently labeled data types (confidential and restricted) on the same VMs。
Which of the following cloud and visualization considerations would BEST address the issue presented in this scenario?

A. Vulnerabilities associated with a single platform hosting multiple data types on VMs should have been considered
B. Vulnerabilities associated with a single server hosting multiple data types should have been considered.
C. Type 1vs Type 2 hypervisor approaches should have been considered
D. Vulnerabilities associated with shared hosting services provided by the IT department should have been considered.

Answer: B

QUESTION 637
An electric car company hires an IT consulting company to improve the cybersecurity of us vehicles.
Which of the following should achieve the BEST long-term result for the company?

A. Designing Developing add-on security components for fielded vehicles
B. Reviewing proposed designs and prototypes for cybersecurity vulnerabilities
C. Performing a cyber-risk assessment on production vehicles
D. Reviewing and influencing requirements for an early development vehicle

Answer: B

QUESTION 638
An enterprise is configuring an SSL client-based VPN for certificate authentication.
The trusted root certificate from the CA is imported into the firewall, and the VPN configuration in the firewall is configured for certificate authentication.
Signed certificates from the trusted CA are distributed to user devices. The CA certificate is set as trusted on the end-user devices, and the VPN client is configured on the end-user devices.
When the end users attempt to connect however, the firewall rejects the connection after a brief period.
Which of the following is the MOST likely reason the firewall rejects the connection?

A. In the firewall, compatible cipher suites must be enabled
B. In the VPN client, the CA CRL address needs to be specified manually
C. In the router, IPSec traffic needs to be allowed in bridged mode
D. In the CA. the SAN field must be set for the root CA certificate and then reissued

Answer: A

QUESTION 639
A software development firm wants to validate the use of standard libraries as part of the software development process.
Each developer performs unit testing prior to committing changes to the code repository.
Which of the following activities would be BEST to perform after a commit but before the creation of a branch?

A. Static analysis
B. Heuristic analysis
C. Dynamic analysis
D. Web application vulnerability scanning
E. Penetration testing

Answer: A

QUESTION 640
A creative services firm has a limited security budget and staff.
Due to its business model, the company sends and receives a high volume of files every day through the preferred method defined by its customers.
These include email, secure file transfers, and various cloud service providers.
Which of the following would BEST reduce the risk of malware infection while meeting the company's resource requirements and maintaining its current workflow?

A. Configure a network-based intrusion prevention system
B. Contract a cloud-based sandbox security service.
C. Enable customers to send and receive files via SFTP
D. Implement appropriate DLP systems with strict policies.

Answer: B

QUESTION 641
During an audit, it was determined from a sample that four out of 20 former employees were still accessing their email accounts.
An information security analyst is reviewing the access to determine if the audit was valid.
Which of the following would assist with the validation and provide the necessary documentation to audit?

A. Examining the termination notification process from human resources and employee account access logs
B. Checking social media platforms for disclosure of company sensitive and proprietary information
C. Sending a test email to the former employees to document an undeliverable email and review the ERP access
D. Reviewing the email global account list and the collaboration platform for recent activity

Answer: A

QUESTION 642
A healthcare company wants to increase the value of the data it collects on its patients by making the data available to third-party researchers for a fee.
Which of the following BEST mitigates the risk to the company?

A. Log all access to the data and correlate with the researcher
B. Anonymize identifiable information using keyed strings
C. Ensure all data is encrypted in transit to the researcher
D. Ensure all researchers sign and abide by non-disclosure agreements
E. Sanitize date and time stamp information in the records.

Answer: B

QUESTION 643
The Chief Executive Officer)CEO) of a small company decides to use cloud computing to host critical corporate data for protection from natural disasters.
The recommended solution is to adopt the public cloud for its cost savings If the CEO insists on adopting the public cloud model, which of the following would be the BEST advice?

A. Ensure the cloud provider supports a secure virtual desktop infrastructure
B. Ensure the colocation facility implements a robust DRP to help with business continuity planning.
C. Ensure the on-premises datacenter employs fault tolerance and load balancing capabilities.
D. Ensure the ISP is using a standard help-desk ticketing system to respond to any system outages

Answer: B

QUESTION 644
A development team releases updates to an application regularly.
The application is compiled with several standard open-source security products that require a minimum version for compatibility.
During the security review portion of the development cycle, which of the following should be done to minimize possible application vulnerabilities?

A. The developers should require an exact version of the open-source security products, preventing the introduction of new vulnerabilities.
B. The application development team should move to an Agile development approach to identify security concerns faster
C. The change logs for the third-party libraries should be reviewed for security patches, which may need to be included in the release.
D. The application should eliminate the use of open-source libraries and products to prevent known vulnerabilities from being included.

Answer: C

QUESTION 645
A penetration tester is given an assignment lo gain physical access to a secure facility with perimeter cameras.
The secure facility does not accept visitors and entry is available only through a door protected by an RFID key and a guard stationed inside the door.
Which of the following would be BEST for the penetration tester to attempt?

A. Gam entry into the building by posing as a contractor who is performing routine building maintenance
B. Tailgate into the facility with an employee who has a valid RFID badge to enter
C. Duplicate an employees RFID badge and use an IR camera to see when the guard leaves the post
D. Look for an open window that can be used to gain unauthorized entry into the facility

Answer: C