ISLEVER

# CAS-001

CompTIA Advanced Security Practitioner

DEMO

https://www.islever.com/cas-001.html

https://www.islever.com/comptia.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

**Topic 1, Volume A**

**QUESTION NO: 1**

Which of the following attacks does Unicast Reverse Path Forwarding prevent?

**A.** Man in the Middle
**B.** ARP poisoning
**C.** Broadcast storm
**D.** IP Spoofing

**Answer: D**
**Explanation:**

**QUESTION NO: 2**

Which of the following authentication types is used primarily to authenticate users through the use of tickets?

**A.** LDAP
**B.** RADIUS
**C.** TACACS+
**D.** Kerberos

**Answer: D**
**Explanation:**

**QUESTION NO: 3**

A security consultant is evaluating forms which will be used on a company website. Which of the following techniques or terms is MOST effective at preventing malicious individuals from successfully exploiting programming flaws in the website?

**A.** Anti-spam software
**B.** Application sandboxing
**C.** Data loss prevention
**D.** Input validation

**Answer: D**
**Explanation:**

**QUESTION NO: 4**

A security audit has uncovered that some of the encryption keys used to secure the company B2B financial transactions with its partners may be too weak. The security administrator needs to implement a process to ensure that financial transactions will not be compromised if a weak encryption key is found. Which of the following should the security administrator implement?

**A.** Entropy should be enabled on all SSLv2 transactions.
**B.** AES256-CBC should be implemented for all encrypted data.
**C.** PFS should be implemented on all VPN tunnels.
**D.** PFS should be implemented on all SSH connections.

**Answer: C**
**Explanation:**

**QUESTION NO: 5**

A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data was found on a hidden directory within the hypervisor. Which of the following has MOST likely occurred?

**A.** A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.
**B.** An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.
**C.** A host server was left un-patched and an attacker was able to use a VMEscape attack to gain unauthorized access.
**D.** A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.

**Answer: C**
**Explanation:**

**QUESTION NO: 6**

Company XYZ provides residential television cable service across a large region.

The company's board of directors is in the process of approving a deal with the following three companies:

- A National landline telephone provider
- A Regional wireless telephone provider
- An international Internet service provider

The board of directors at Company XYZ wants to keep the companies and billing separated.

While the Chief Information Officer (CIO) at Company XYZ is concerned about the confidentiality of Company XYZ's customer data and wants to share only minimal information about its customers for the purpose of accounting, billing, and customer authentication.

The proposed solution must use open standards and must make it simple and seamless for Company XYZ's customers to receive all four services.

Which of the following solutions is BEST suited for this scenario?

**A.** All four companies must implement a TACACS+ web based single sign-on solution with associated captive portal technology.
**B.** Company XYZ must implement VPN and strict access control to allow the other three companies to access the internal LDAP.
**C.** Company XYZ needs to install the SP, while the partner companies need to install the WAYF portion of a Federated identity solution.
**D.** Company XYZ needs to install the IdP, while the partner companies need to install the SP portion of a Federated identity solution.

**Answer: D**
**Explanation:**

**QUESTION NO: 7**

The security administrator at a bank is receiving numerous reports that customers are unable to login to the bank website. Upon further investigation, the security administrator discovers that the name associated with the bank website points to an unauthorized IP address.

Which of the following solutions will MOST likely mitigate this type of attack?

**A.** Security awareness and user training
**B.** Recursive DNS from the root servers
**C.** Configuring and deploying TSIG
**D.** Firewalls and IDS technologies