IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **SY0-701**

Title : CompTIA Security+

Version: DEMO

1.Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?
A. Hacktivist
B. Whistleblower
C. Organized crime
D. Unskilled attacker
Answer: C
Explanation:
Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption12.
Reference = 1: Threat Actors - CompTIA Security+ SY0-701 - 2.1 2: CompTIA Security+ SY0-701 Certification Study Guide

2.Which of the following is used to add extra complexity before using a one-way data transformation algorithm?
A. Key stretching
B. Data masking
C. Steganography
D. Salting
Answer: D
Explanation:
Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks.
Reference =
Passwords technical overview
Encryption, hashing, salting – what’s the difference?
Salt (cryptography)

3.An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message.
Which of the following types of social engineering attacks occurred?
A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing

Answer: D
Explanation:
Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one. The employee entered the log-in information, but received a “page not found” error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee’s credentials for the payment website.
Reference = Other Social Engineering Attacks – CompTIA Security+ SY0-701 – 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack … - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

4.An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25.
Which of the following firewall ACLs will accomplish this goal?
A. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53
D. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0/0 port 53
Answer: D
Explanation:
The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B).
Reference = You can learn more about firewall ACLs and DNS in the following resources:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security1
Professor Messer’s CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules2
TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules3

5.A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications.
Which of the following methods would allow this functionality?
A. SSO
B. LEAP

C. MFA
D. PEAP
Answer: A
Explanation:
SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123.
B. LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials4.
C. MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.
D. PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.
Reference = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia: What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com: Protected Extensible Authentication Protocol - Wikipedia