QUESTION 895
An organization has decided to implement biometric controls for improved access management. However, a significant number of authorized users are being denied access to networked resources. Which of the following is the main biometric factor that requires attention?

A. False acceptance
B. False rejection
C. True negative
D. True positive

Answer: C

QUESTION 896
A security administrator is researching ways to improve the security of a manufacturing company's systems within the next three to six months.
Which of the following would provide the security administer with the most diverse perspective?

A. Platform-specific security benchmark for the company's specific systems
B. Manufacturing security auditing requirement
C. Academic security research on emerging technologies
D. Security regulations from other industry verticals

Answer: A

QUESTION 897
After discovering a security incident and removing the affected files, an administrator disabled an unneeded service that led to the breach.

A. Containment
B. Eradication
C. Recovery
D. Identification

Answer: B

QUESTION 898
A company is implementing an authentication system for its wireless network. The system will be for public use and must be able to track how long a person is connected to the WiFi system for billing purposes. Which of the following would be BEST to implement in this situation?

A. Captive portal
B. Pre shared key
C. WPS
D. 802.1x

Answer: A

QUESTION 899
An organization has the following password policies:
- Passwords must be at least 16 characters long.
- A password cannot be the same as any previous 20 passwords.
- Three failed login attempts will lock the account for 5 minutes.
- Passwords must have one uppercase letter, one lowercase letter, and one non-alphanumeric symbol.
A database server was recently breached. and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on a completely separate server.
Which of the following is MOST likely the issue and the best solution?

A. Some users are reusing passwords for different systems: the organization should scan for password reuse across systems.
B. The organization has improperly configured single sign-on; the organization should implement a RADIUS server to control account logins.
C. User passwords are not sufficiently long or complex: the organization should increase the complexity and length requirements for passwords.
D. The trust relationship between the two servers has been compromised: the organization should place each server on a separate VLAN.

Answer: D

QUESTION 900
An attacker is able to capture the payload for the following packet:
- IP 192.168.1.22:2020 10.10.10.5:443
- IP 192.168.1.10:1030 10.10.10.1:21
- IP 192.168.1.57:5217 10.10.10.1:3389
During an investigation. an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.
B. The application server is also running a web server that has been compromised.
C. The attacker is picking off unencrypted credentials and using those to log in to the secure server.
D. User accounts have been improperly configured to allow single sign-on across multiple servers.

Answer: C

QUESTION 901
Which of the following algorithms would be used to provide non-repudiation of a file transmission?

A. AES
B. RSA
C. MD5
D. SHA

Answer: B

QUESTION 902
Which of the following ready resources is a cold site MOST likely to have?

A. Servers
B. Workstations
C. Internet Access.
D. Electricity

Answer: A

QUESTION 903
An organization is considering utilizing a third-party web-hosting service for a human resources application. The organization's Chief Information Officer (CIO) is concerned the web-hosting service may not have a sufficient level of security. The sales representative for the web-hosting service suggests that the CIO use banner grabbing to test the security levels of an existing website hosted by the company (www.example.com).
Which of the following commands should the CIO use? (Select TWO).

A. nc
B. telnet
C. ifconfig
D. tracert
E. netstat
F. nslookup

Answer: AB

QUESTION 904
A user receives a security alert pop-up from the host-based IDS, and a few minutes later notices a document on the desktop has disappeared and in its place is an odd filename with no icon image. When clicking on this icon, the user receives a system notification that it cannot find the correct program to use to open this file.
Which of the following types of malware has MOST likely targeted this workstation?

A. Rootkit
B. Spyware
C. Ransomware
D. Remote-access trojan

Answer: C

QUESTION 905
After a systems administrator installed and configured Kerberos services, several users experienced authentication issues.
Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

Answer: C

QUESTION 906
A mobile application developer wants to secure an application that transmits sensitive information. Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling
B. Chaining
C. Signing
D. Pinning

Answer: D