**Database Hardening Screenshots:**

1)

**Graphical user interface, text, application

Description automatically generated**

2)

Text

Description automatically generated

Text

Description automatically generated

3)

Text

Description automatically generated

4)

Text

Description automatically generated

5)

Text

Description automatically generated

6)

Text

Description automatically generatedText

Description automatically generated

7)

Text

Description automatically generated

Database Hardening

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Shape

Description automatically generated

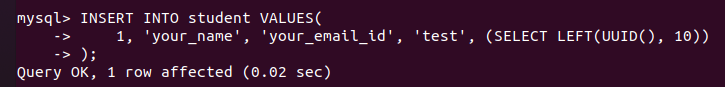


Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence



A screen shot of a computer

Description automatically generated with low confidence

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Timeline

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated



Text

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

A picture containing chart

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

1. What is salting? How does it strengthen password hashing?

Salting is a technique to protect passwords that has been stored in the databases which is done by adding a string of 32 or more characters and hashing them. Salting helps in preventing hackers from breaching an enterprise environment and stopping of stealing it from the database.

1. What is Role Based Access Control? What are the benefits of RBAC? List other authorization models.

RBAC is generally helps in the process of restricting network access based on individual’s role within a team or organization and has become one of the main methods for access control. Benefits of RBAC includes Reducing administrative work and IT support, maximizing operational efficiency, and improving compliance. The other authorization models include Access Control List, Discretionary Access Control, Mandatory Access Control and Attribute Based Access Control.

1. What are some attacks on passwords? How to defend against such attacks?

Some attacks on passwords include phishing, man in the middle attack, brute force attack, dictionary attack, credential stuffing and keyloggers. To defend against such attacks double check with the source check within the IT Team, enable encryption on the router, use of VPN, use of complex passwords, enable and configure remote access, require multi factor authentication, considering of investing in password managers, regularly change passwords and checking of hardware regularly.

1. Write a short description on Bcrypt, Scrypt and Argon2 and PBKDF2.

Bcrypt is a difficult algorithm use to store passwords through one way hashing function.

Scrypt is designed in such a manner that to rely on high memory requirements as opposed to high requirements on computational powers.

Argon2 is a technique used in modern ASIC resistant and GPU resistant secure key derivation function. High chances of password cracking resistance compared to other techniques.

PBKDF2 is a cryptographic derivative function which is resistant to dictionary attacks and rainbow table attacks. It is iteratively deriving HMAC with padding. It allows configure the number of iterations.

1. Explain how passwords are stored in Linux (location, encryption algorithm, salt and file permissions)?

Passwords stored in Linux can be through a user account with a corresponding password for that account. Passwords of all the users in a system must be first saved in a particular file or database which can in turn be verified during a user login. Passwords were generally stored in /etc/passwd. File permissions a user must not be able to change fields. It can also lead to disrupt permissions and authorizations. Salt is generally used for configuration management system, and it can maintain nodes or remote nodes in defined states. Also, distributed remote execution system is generally used to execute commands and query data on remote nodes. Encryption Algorithm involves One way encryption algorithm through DES or Data Encryption Standard to encrypt passwords. Encrypted passwd is then stored in /etc/passwd.