SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

IV SEMESTER

1923402 – Database Security

Regulation – 2019

Academic Year 2021 – 2022 (EVEN SEMESTER)

Prepared by

Ms.V.Prema, Assistant Professor (Sr. G) / CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

SUBJECT : DATABASE SECURITY

SEM / YEAR : VI Sem / III Year

UNIT I -INTRODUCTION

Harden your database environment- Patch your database- Audit the database- Define an access policy as the center of your database security and auditing initiative

PART – A

Q.No	Questions	BT Level	Competence
1.	Express the term hardening of database	BTL2	Understanding
2.	Analyze the use of hardening is required.	BTL4	Analyzing
3.	Define hardening in SQL server	BTL1	Remembering
4.	List the types of data auditing tool.	BTL1	Remembering
5.	Discuss about patching in Oracle database	BTL2	Understanding
6.	Interpret why do database hardening	BTL2	Understanding
7.	Differentiate between hardening in SQL server and Oracle database	BTL4	Analyzing
8.	Give the detail How do I know if my database is patched?	BTL2	Understanding
9.	What is Oracle DB hardening?	BTL1	Remembering
10.	Demonstrate the functions of SQL Server	BTL3	Applying
11.	What is the difference between access policy in Azure and Azure security policies	BTL6	Creating
12.	Explain the purpose of patching.	BTL5	Evaluating
13.	Formulate how security policy in the security Center ?	BTL6	Creating
14.	State how do you audit a database.	BTL1	Remembering
15.	Show the essentials and characteristics Oracle DB hardening.	BTL3	Applying
16.	Define patching in Oracle database.	BTL1	Remembering
17.	What are hardening guidelines?	BTL1	Remembering
18.	Analyze the meaning of database audit..	BTL4	Analyzing
19.	Illustrate when did database auditing is important?	BTL3	Applying
20.	Summarize the purpose of security policies?	BTL5	Evaluating
	PART – B		
1.	(i) Explain the database hardening with illustrations (6) (ii) Summarize the motivation to Hardening an Oracle environment. (7)	BTL5	Evaluating
2.	(i) Describe in detail basic concepts SQL Server. (7) (ii) Explain in detail notes on SQL Server environment. (6)	BTL1	Remembering
3.	(i) Describe the Sybase environment. (7) (ii) Write Short notes on the DB2 UDB (LUW) environment. (6)	BTL1	Remembering

4.	**Explain** the Use configuration scanners or audit checklists. (13)	BTL1	Remembering
5.	**i) Explain** the Hardening a MySQL environment. (6) **ii)Describe** Anatomy of buffer overflow vulnerabilities. (7)	BTL2	Understanding
6.	**i)Explain** Audit the database. (6) **ii)Write** a database access policy is the core of any implementation. (7)	BTL4	Analyzing
7.	**(i)Illustrate** login names, which may exist as part of installations of other Sybase servers. (6) **(ii)Explain the issues found by the SQL server**. (7)	BTL3	Applying
8.	**Describe** How to Contact Oracle with Security Vulnerabilities. (13)	BTL2	Understanding
9.	**(i) Formulate** Memory layout for an operating system process. (5) **(ii)Outline** about the Oracle in detail. (8)	BTL6	Creating
10	**Illustrate** SYS system privileges with example. (13)	BTL3	Applying
11.	**Describe** the following in detail (i) Stack grows down (from high memory to low memory). (7) (ii) simplest buffer overflow problem with example. (6)	BTL1	Remembering
12.	**Analyze** and elaborate the role of Database Administrator. (13)	BTL4	Analyzing
13.	**Explain** the basic key concept of database security. (13)	BTL4	Analyzing
14.	**Discuss** A good starting point for MySQL hardening. (13)	BTL2	Understanding
	PART C		
1.	How to create a database in SQL Server? (15)	BTL4	Analyzing
2.	Explain the nature and scope of maintenance level Database security**. (15)**	BTL5	Evaluating
3.	i)What is the meaning and importance database security? (7) ii)Explain the database security based on Access Control. (8)	BTL5	Evaluating
4.	Generalize your **view** about 9 Best Practices for Systems Hardening. (15)	BTL6	Creating

UNIT II – DATABASE SECURITY AND DEFENSE STRATEGY

Defense–in–depth, The security software landscape-Perimeter security- firewalls- intrusion detection- and intrusion prevention- Securing the core- Application security-Public key infrastructure (PKI)- Vulnerability management and Patch management

PART – A

Q.No	Questions	BT Level	Competence
1	Show the characteristics of defense in depth concept.	BTL3	Applying
2	Explain practical aspects of DiD defense-in-depth	BTL5	Evaluating
3	Analyze an defense in depth is important?.	BTL4	Analyzing
4	Examine the security landscape.	BTL3	Applying
5	Define cybercrime	BTL1	Remembering
6	State Cyber Security a threat.	BTL1	Remembering
7	Discuss the three elements of cybersecurity	BTL2	Understanding
8	Illustrate the 3 types of firewalls	BTL3	Applying
9	Classify the 3 key layers of the defense in depth security strategy	BTL4	Analyzing
10	Give definition for cyber security landscape	BTL2	Understanding
11	Generalize on CIA in terms of information security	BTL6	Creating
12	Tabulate the essentials and characteristics of an firewall.	BTL1	Remembering
13	Formulate on what is a perimeter security systems?	BTL6	Creating
14	Why are firewall important?	BTL5	Evaluating
15	List out the seven layers in layered security	BTL1	Remembering
16	Differentiate on intrusion detection and intrusion prevention	BTL2	Understanding
17	What are the six components of PKI?	BTL1	Remembering
18	Summarize application security analyst	BTL2	Understanding
19	Point out the difference between firewall and antivirus	BTL4	Analyzing
20	Define SCCM patch management.	BTL1	Remembering

PART – B

1	i)Discuss in detail about the Defense-in-depth (6) ii)Describe the Intrusion detection and prevention in detail. (7)	BTL2	Understanding
2	Illustrate the following i)Firewalls. (7) ii)Virtual private networks (6)	BTL3	Applying
3	Describe in detail about the security software landscape . (13)	BTL1	Remembering
4	i)Generalize on the Vulnerability assessment and patch management (7) ii)How do Security management perform in the database?. (6)	BTL6	Creating

5	i) Examine on Perimeter security, firewalls. (7) ii)Identify and explain Intrusion detection systems Intrusion prevention systems . (6)	BTL1	Remembering
6	Describe the following. i)IDS monitor in detail. (6) ii)False positives in IDS. (7)	BTL2	Understanding
7	Explain in detail about Securing the core. (13)	BTL2	Understanding
8	**i)** Define removing false positives through more specific signatures. .(8) **ii)** Tabulate the types of intrusion prevention. (5)	BTL1	Remembering
9	Describe in detail about the types of firewalls. (13)	BTL1	Remembering
10	(i) Discuss in detail Web application request-response paradigm. (7) (ii) Summarize the Application security in detail. (6)	BTL2	Understanding
11	Explain the following in detail. i) Public key infrastucture. (7) ii) Importance of Vulnerability management. (6)	BTL5	Evaluating
12	i)Explain in detail Vulnerability management process and technologies. (7) ii)Write notes on Why are there so many vulnerabilities?. (6)	BTL4	Analyzing
13	Summarize the concept of Vulnerability scanners. (13)	BTL4	Analyzing
14	Analyze the following with example i) Incident management. (7) ii) Patch management. (6)	BTL3	Applying
	PART C		
1.	Analyze the Firewall Authentication Types	BTL4	Analyzing
2.	Evaluate the components of Public key infrastuctures..	BTL5	Evaluating

3.	Summarize the various **Classification of Intrusion Detection System**	BTL5	Evaluating
4.	Generalize about steps involved in patch management in details	BTL6	Creating

UNIT III THE DATABASE AS A NETWORKED SERVER			
Leave your database in the core-Understand the network access map for your database environment-Track tools and applications- Remove unnecessary network libraries-Use port scanners—so will the hackers-Secure services from known network attacks- Use firewalls and Named Pipes and SMB/CIFS			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1.	Express the term TNS in database?	BTL2	Understanding
2.	How to you manage tools and equipment?	BTL2	Understanding
3.	Write a full form of Netca in Oracle	BTL1	Remembering
4.	Define Net Manager in Oracle	BTL1	Remembering
5.	Discuss about the TNS file in SQL Developer.	BTL2	Understanding
6.	Give the different types of port scanners	BTL2	Understanding
7.	What is a TNS entries in Oracle	BTL1	Remembering
8.	Assess tool is used for network port scanning.	BTL5	Evaluating
9.	State disabling unnecessary services	BTL1	Remembering
10.	Write a Generalize note on tracker tools.	BTL6	Creating
11.	Classify the different types of security services.	BTL4	Analyzing
12.	Illustrate about security services in network security.	BTL3	Applying
13.	Assess on some of the ways you can secure a network from attack?	BTL5	Evaluating
14.	What is the the best network security?	BTL1	Remembering
15.	Show the TNS file in SQL Developer	BTL3	Applying
16.	Explain the term What is the best port scanner??	BTL4	Analyzing

17.	What are some examples of network security?	BTL1	Remembering
18.	Show the 5 safeguards against Internet and network attacks	BTL3	Applying
19.	Analyze the hackers scan ports.	BTL4	Analyzing
20.	Generalize about Which software is best for tracking?	BTL6	Creating
	PART – B		
1	i)Discuss the criteria don't expose your database to the public Internet.(6) ii)Explain in detail about the Three-tier application architecture using a DMZ.(7)	BTL2	Understanding
2	i. Give the detail about Virtual LAN in detail.(3) ii. Describe in detail about Data access diagram showing database connection endpoints..(10)	BTL1	Remembering
3	i. Describe the reasons for adoption include the following.(7) ii. Explain retrieving network connection information in SQL Server..(6)	BTL1	Remembering
4	Generalize on SQL server and Sybase. (13)	BTL6	Creating
5	**i.** Explain about the steps are required to support desired monitoring.(7) **ii.** Discuss Remove unnecessary network libraries.(6)	BTL1	Remembering
6	(i) Summarize on SQL Server networking architecture..(7) (ii) Discuss about the SQL Server Network Utility to enable or disable protocol support.(6)	BTL2	Understanding
7	Explain briefly the following *i.* DB2 networking layers. (7) *ii.* Oracle networking layers.(6)	BTL4	Analyzing
8	**i.** Summarize Selecting a network protocol for a service name..(7) **ii.** Assess on Oracle Listener Ports (6)	BTL5	Evaluating
9	Demonstrate briefly about SQL Server (and Sybase) networking layers.(13)	BTL3	Applying
10	Explain the following in detail i. Anatomy of a vulnerability .(7) ii. Uses of firewalls.(6)	BTL4	Analyzing
11	Discuss Secure services from known network attacks.(13)	BTL2	Understanding
12	Analyze the Named Pipes and SMB/CIFS . Explain in detail.(13)	BTL4	Analyzing
13	Describe in detail about SMB Commands . (13)	BTL1	Remembering
14	i)Write in detail about Default Oracle 11i Ports.(6) ii) Explain in detail about Internet-based VPN	BTL3	Applying
	PART C		
1.	i. Explain the following in detail Tool tracking system. (8) ii. Analyze the main features of network access map. (7)	BTL4	Analyzing
2.	Write an types network security attacks in detail. .(15)	BTL5	Evaluating
3.	(i) Explain in detail notes on type of hackers. (8) (ii) Discuss in detail notes on port scanning attack. (7)	BTL5	Evaluating
4.	Write a detail notes on CIFS in detail. (15)	BTL6	Creating

UNIT IV – AUTHENTICATION AND PASSWORD SECURITY			
Choose an appropriate authentication option-Understand who gets system administration privileges- Choose strong passwords- Implement account lockout after failed login attempts- Create and enforce password profiles-Use passwords for all database components-and Understand and secure authentication back doors.			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1.	How to you choose a strong password?	BTL2	Understanding
2.	Illustrate the the 3 types of authentication.	BTL3	Applying
3.	What is the most commonly used form of authentication??	BTL1	Remembering
4.	Analyze system administration	BTL4	Analyzing
5.	Define backdoor security.	BTL1	Remembering
6.	Discuss the duties and responsibilities of system administrator	BTL1	Remembering
7.	How many good character for creating of the password?	BTL2	Understanding
8.	Define the best practice for account lockout duration.	BTL1	Remembering
9.	Differentiate types of authentication.	BTL2	Understanding
10.	Show the some examples of strong passwords	BTL3	Applying
11.	Compare the authentication method	BTL5	Evaluating
12.	What the 4 types of administrators?	BTL1	Remembering
13.	Write the advantages of system administrator	BTL6	Creating
14.	Discriminate How do you choose a strong password?	BTL5	Evaluating
15.	Definitions of digital authentication methods	BTL1	Remembering
16.	Express the Character of the strong passwords.	BTL2	Understanding
17.	Formulate the How do you implement account lockout policy	BTL6	Creating
18.	Categorize the features of types of system admin.	BTL4	Analyzing
19.	Compare types of system admin	BTL4	Analyzing
20.	Demonstrate the use of a system administrator.	BTL3	Applying
PART – B			
1	(i) What is authentication? Write a detail notes on authentication security ? (7) (ii) How to use Weak authentication options? (6)	BTL1	Remembering
2	**i)** Give the A Windows user is created when installing DB2 in Windows, because DB2 UDB uses the operating system to authenticate users. (7) **ii)** Explain cyber security in detail. (6)	BTL2	Understanding
3	Discuss on Other authentication options supported by DB2 UDB 8.2 (13)	BTL2	Understanding
4	Describe in detail about Guessing and cracking passwords. (13)	BTL1	Remembering
5	i) Formulate the When doing a review, and it 's uses : (6) ii) Describe in detail about procedure to enable and set a password for the guest account. (7)	BTL6	Creating
6	Illustrate in detail about port scan and DoS protection?. (13).	BTL3	Applying

7	i) Analyze the Promote and verify the use of strong passwords. (7) ii) Explain in detail Do's and Don'ts for setting the password (6)	BTL4	Analyzing
8	i)Explain in detail about the Implement account lockout after failed login attempts (7) ii)Explain in detail denial-of-service attack. (6)	BTL5	Evaluating
9	Analyze the Create and enforce password profiles . (13)	BTL4	Analyzing
0	Describe in detail about Use passwords for all database components (13)	BTL1	Remembering
11	i) Explain the Hijacking the Oracle listener. (7) ii) What is listener password? How to set the listener password? (6)	BTL4	Analyzing
12	i) Describe the detail notes of secure authentication back doors. (6) ii) Discuss the Conceptual steps in Kerberos distributed authentication. (7)	BTL1	Remembering
13	i) List the denial rule in database firewall to shut down connections based on failed logins.. (3) ii) Illustrate in detail about . (10)	BTL3	Applying
14	**i)** Discuss the Report showing failed login information.. (6) **ii)** Discuss the Using SQLdict to run a dictionary attack on the sa account in SQL Server. (7)	BTL2	Understanding
	PART C		
1	(i) Write about the purpose of administration privileges. (8) (ii) What are the remedies for the misuse of password profiles (7)	BTL4	Analyzing
2	(i)Define authentication backdoor and explain its significance. (8) (ii)Briefly describe the advantage of secure authentication. (7)	BTL5	Creating
3.	(i) What are the salient features of system administration privileges? (8) (ii) Explain the concepts of Kerberos . (7)	BTL5	Creating
4.	What are the variousdatabase security? Explain in detail with suitable example (15)	BTL6	Creating

UNIT V – APPLICATION SECURITY			
Reviewing where and how database users and passwords are maintained- Obfuscate application code- Secure the database from SQL injection attacks- Beware of double 86 whammies: Combination of SQL injection and buffer overflow vulnerability-Don't consider eliminating the application server layer- Address packaged application suites- Work toward alignment between the application user model and the database user model			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1.	Give the examples of SQL injection attacks	BTL2	Understanding
2.	Mention the various types of databases are more vulnerable to SQL injections	BTL2	Understanding
3.	Illustrate the password verifiers	BTL1	Remembering
4.	What is an example of obfuscation?	BTL1	Remembering
5.	Show the disadvantages of layered architecture	BTL4	Analyzing
6.	Define obfuscation in coding.	BTL1	Remembering

7.	What are the 2 types of security being applied to a database	BTL2	Understanding
8.	Compare the **In-band SQLi with Out-of-band SQLi**	BTL4	Analyzing
9.	What are the methods used to protect against SQL injection attack?	BTL1	Remembering
10.	State the importance of encrypted password is used in Oracle's command	BTL6	Evaluating
11.	Why layering your application is important?	BTL2	Understanding
12.	List the solution for injection attacks	BTL1	Remembering
13.	How SQL injection attacks work?	BTL6	Evaluating
14.	Mention any two features of obfuscation?	BTL3	Applying
15.	List the example of application integration	BTL3	Applying
16.	Explain integrating packaged applications?	BTL4	Analyzing
17.	Mention the importance of eschewed.	BTL5	Creating

18.	What is the difference between application user model and the database user model	BTL1	Remembering
19.	List the example of obfuscation.	BTL3	Applying
20.	Summarize the strongly typed languages suffer from buffer overflow.	BTL5	Creating
	PART-B		
1	Explain the The application includes the schema. (13)	BTL5	Creating
2	Discuss the Knowing and controlling how database logins are used (13)	BTL2	Understanding
3	Illustrate some a firewall between applications and the database in detail. (13)	BTL3	Applying
4	Describe about the Obfuscate application code (13)	BTL2	Understanding
5	i) What are the Source code and psuedo-code (3) ii) Explain Precompilation and obfuscation. (10)	BTL1	Remembering
6	Explain in detail Secure the database from SQL injection attacks. (13)	BTL3	Applying
7	Demonstrate the working of SQL injection attacks(13)	BTL6	Analyzing
8	Generalize the some good SQL injection guidelines for application developers (13)	BTL4	Creating
9	Explain in detail about Injecting long strings into procedures with buffer overflow vulnerabilities (13)	BTL1	Remembering
10	Discuss the Oracle security alerts for Oracle Applications. (13)	BTL2	Understanding
11	Summarize Patch and monitor with suitable example (13)	BTL6	Analyzing
12	Analyze Work toward alignment between the application user model and the database user model.	BTL4	Analyzing
13	Compare and contrast the Oracle security alerts for Oracle Applications and Oracle ports for Oracle Applications servers. (13)	BTL4	Creating
14	Explain in detail about The key elements in protecting yourself against SQL injection attack. (13)	BTL1	Remembering
	PART C		
1.	Discuss the various SQL injection attacks. (15)	BTL6	Creating

2.	Describe user management system database design	(15)	BTL5	Evaluating
3.	Discuss the Don’t consider eliminating the application server layer.	(15)	BTL4	Creating
4.	Evaluate user roles and permissions database design.	(15)	BTL6	Evaluating

VALLIAMMAI ENGINEERING COLLEGE
SRM