

Безопасность СУБД

СУБД имеет свои собственные:

- Пользовательские бюджеты
- Механизм ведения аудита
- Механизм разграничения доступа
- Язык программирования
- Механизм управления паролями



Microsoft SQL Server **(організація системи безпеки)**

Службы SQL Server



Local System Account



Domain User Account

Режимы доступа к серверу

**Стандартный
(Standard Security)**

**Интегрированный
(Integrated Security)**

Системные таблицы

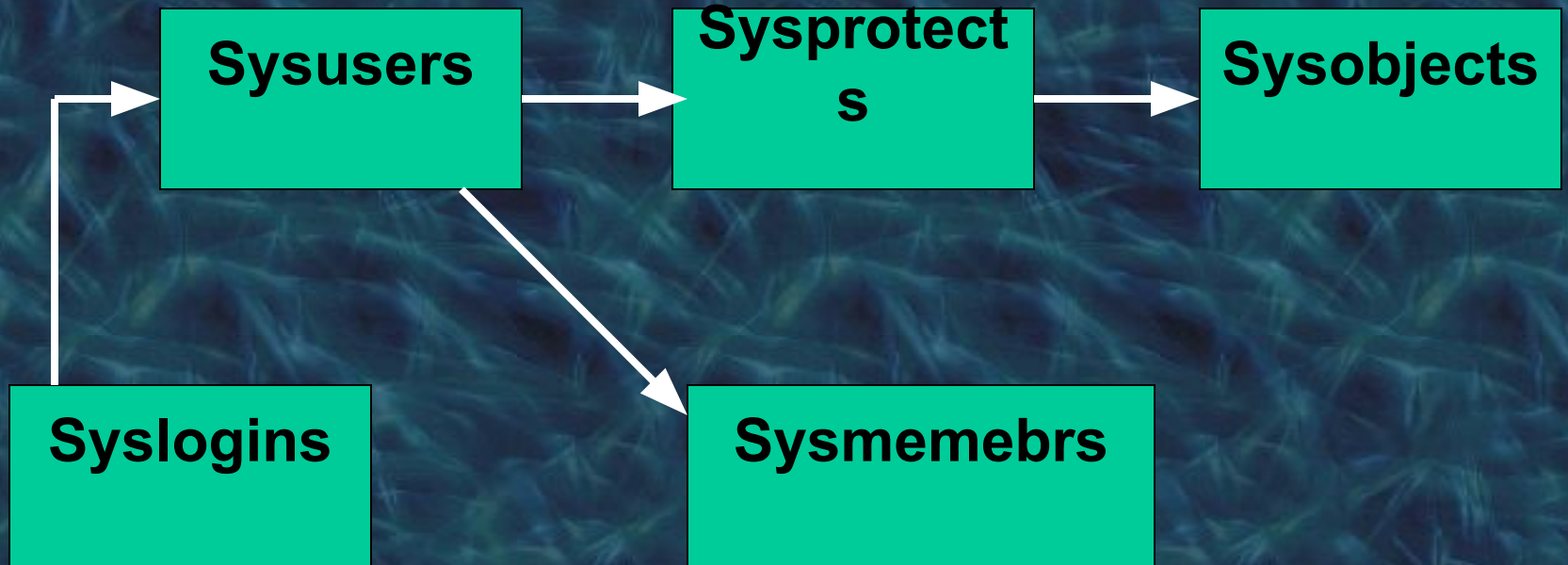
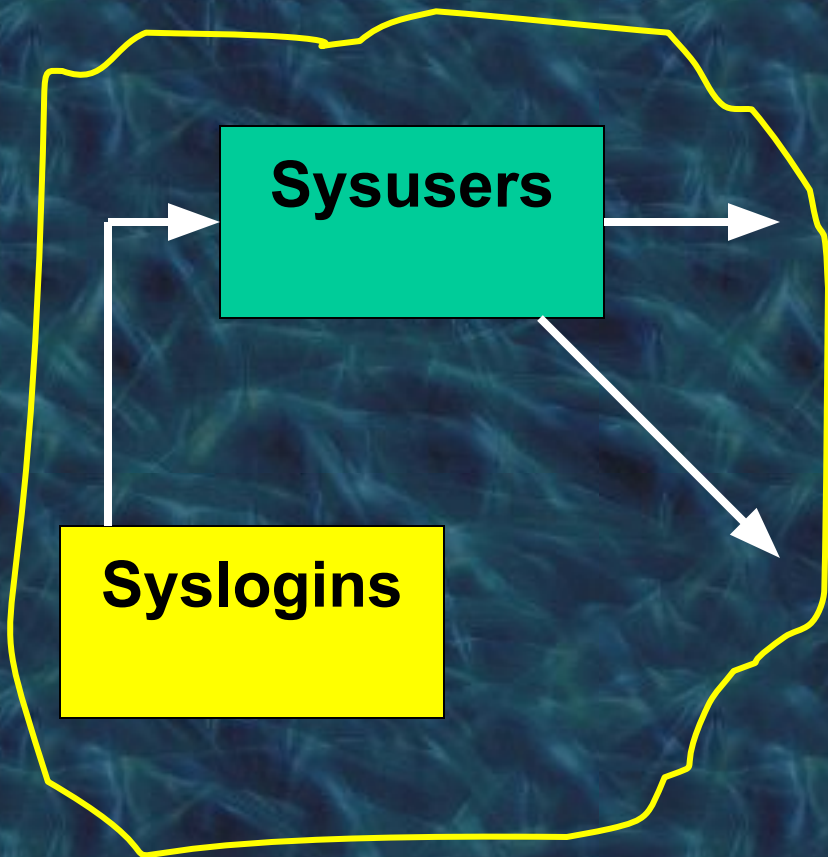


Таблица Syslogins

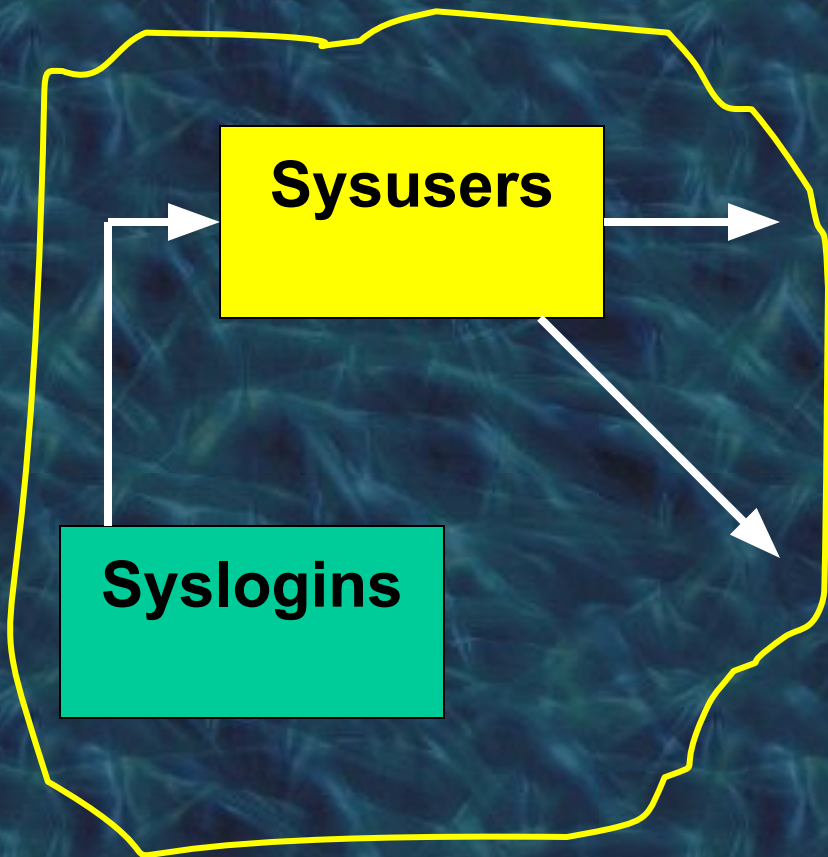


Одна на сервер

Идентификаторы и пароли
пользователей SQL Server

Информация о пользователях
и группах Windows NT

Таблица Sysusers

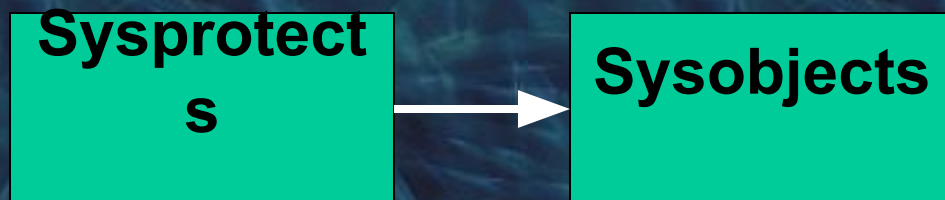


Есть в каждой БД

Права доступа к БД

Права доступа к объектам БД

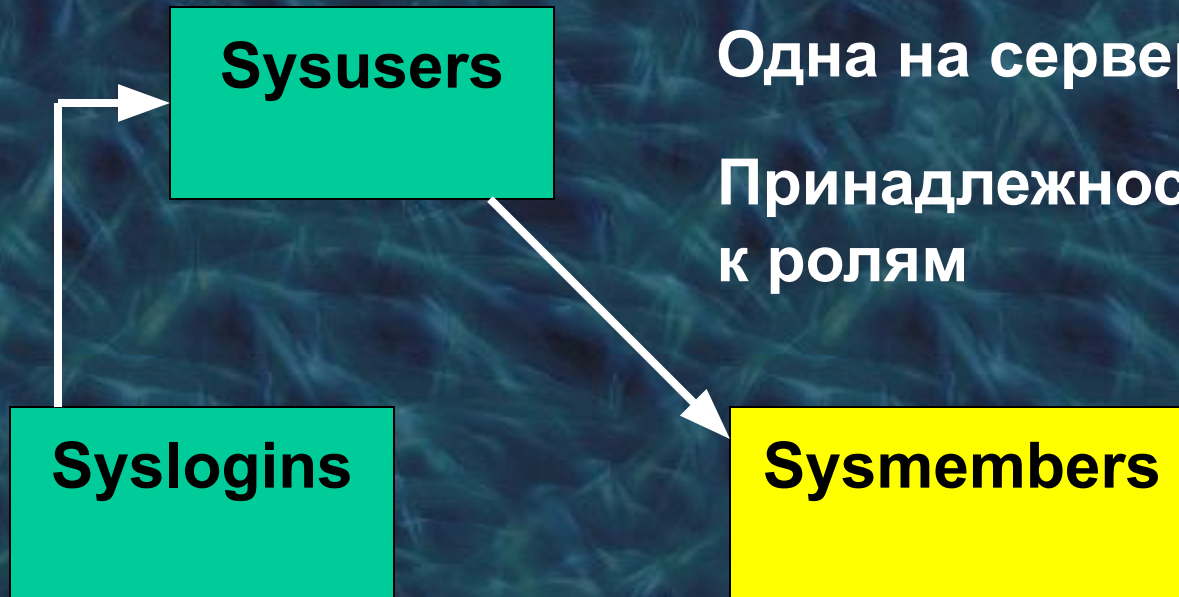
Таблицы Sysprotects и Sysobjects



Есть в каждой БД

Информация об объектах БД

Таблица Sysmembers



Одна на сервер

Принадлежность пользователей
к ролям

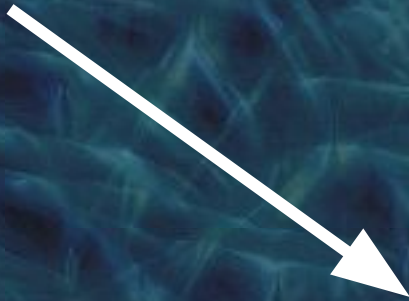
Стандартные идентификаторы пользователей

SA

BULTIN/Administrators

Доступ к БД

Идентификатор
пользователя
(Login)



Учётное имя в БД
(User account)

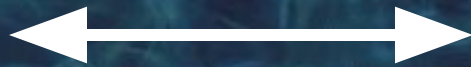
Стандартные учётные имена

Dbp



**Системный
администратор**

guest



**Пользователь,
не имеющий
учётного имени**

Роли

Именованный набор прав



Уровень сервера

Уровень БД

Доступ без учётного имени



Учётная запись guest

роль Public

Разрешения (Permissions)

Выполнение SQL-выражений

Действия с объектами

Предопределённые (стандартные)

Разрешения (Permissions)

Выполнение SQL-выражений

оператор CREATE DATABASE

операторы создания объектов БД

Разрешения (Permissions)

Действия с объектами

Исполнение хранимых процедур

Работа с таблицами и видами

Доступ к определённым полям

Разрешения (Permissions)

Предопределённые (стандартные)

На основе принадлежности к роли

Разрешения владельца объекта

Database Scanner

- Взгляд на СУБД с точки зрения безопасности
- Поддержка MS SQL, Oracle, Sybase
- Интеграция с Internet Scanner

Уязвимости СУБД

	Microsoft SQL Server	Sybase Adaptive Server	Oracle
Default Admin	sa	sa	sys, system
Default Admin passwords	blank	blank	sys - "change_on_install" system - "manager"
Default OS accounts	"Local System" for NT	"sybase" for Unix "Local System" for NT	"oracle" for Unix "Local System" for NT

Бюджеты по умолчанию

Уязвимости СУБД

ELEMENT		MS SQL Server	Sybase AS	Oracle
Login / Account Management				
Stale Logins/ Accts		No Control	No Control	No Control in 7
Off Hours Usage				
Attacks				
Password Management				
Strength				
Aging				
Trojan Horses				
Rights / Permissions				

Бюджет, неиспользуемый в течение долгого времени

Уязвимости СУБД

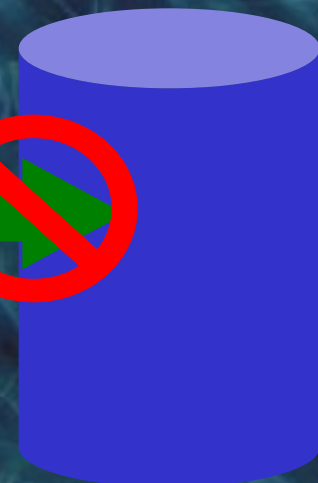
ELEMENT	MS SQL Server	Sybase AS	Oracle
Login / Account Management			
Stale Logins/ Accounts			
Off Hours Usage	No Control	No Control	No Control
Attacks			
Password Management			
Strength			
Aging			
Trojan Horses			
Rights / Permissions			

Отсутствие средств разграничения доступа по времени работы
Контроль соединений в запрещённые часы работы

Уязвимости СУБД

ELEMENT	MS SQL Server	Sybase AS	Oracle
Login / Account Management			
Stale Logins/ Accts			
Off Hours Usage			
Attacks	No Protection	No Protection	No Protection
Password Management			
Strength			
Aging			
Trojan Horses			
Rights / Permissions			

Login Attempt

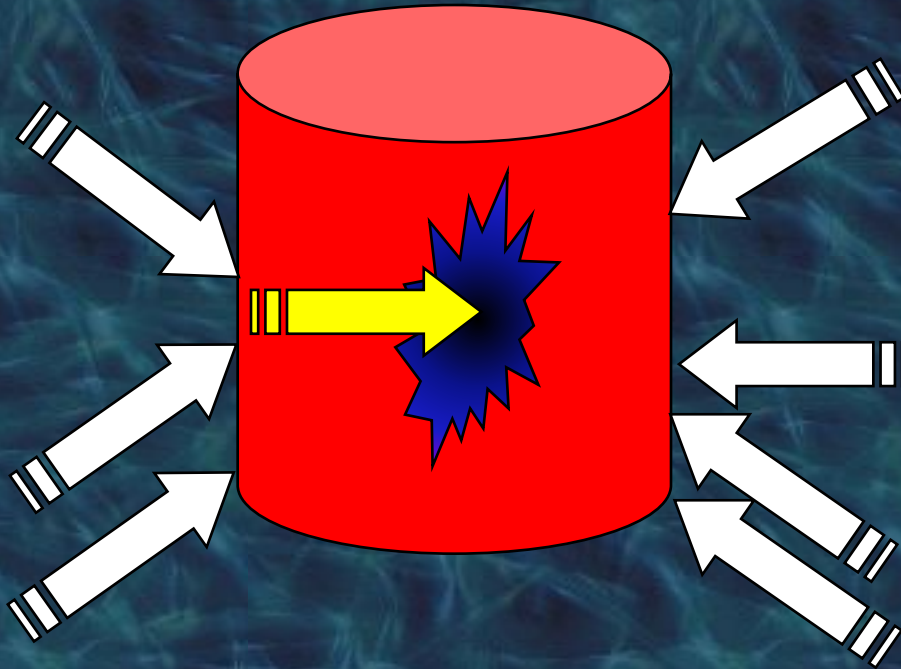


Серия неудачных попыток входа за короткий промежуток времени

Microsoft SQL Server, Sybase, Oracle 7 не блокируют бюджеты
Oracle 8

FAILED_LOGIN_ATTEMPT parameter

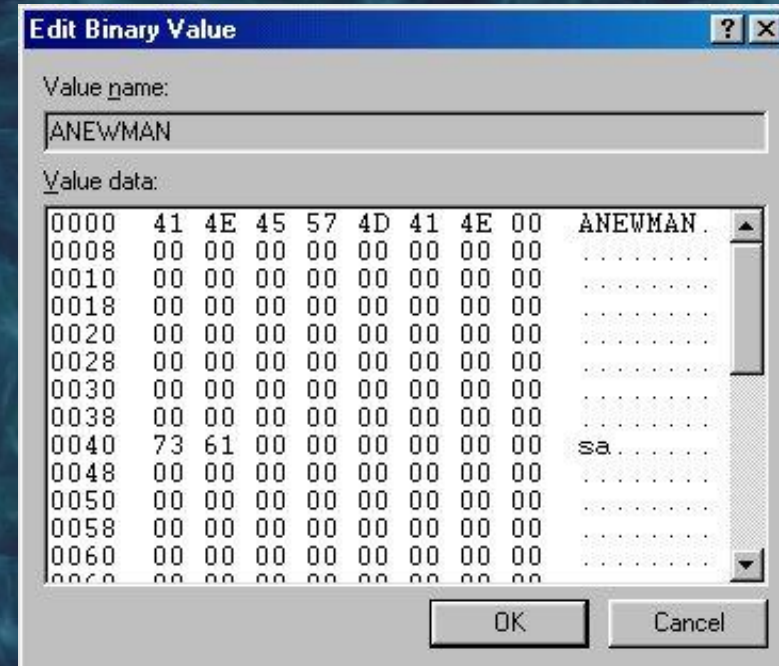
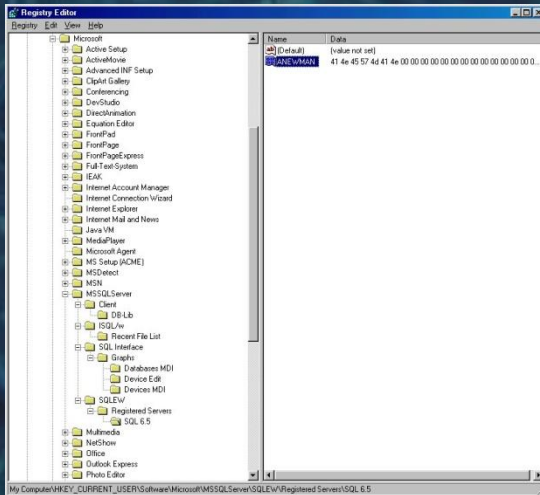
Уязвимости СУБД



Атака по словарю

Уязвимости СУБД

- Регистрация сервера с использованием Standard Security сохраняет пароль SA в реестре
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Microsoft SQL Server\SQLLEW\Registered Server\SQL 6.5.



Открытый пароль SA

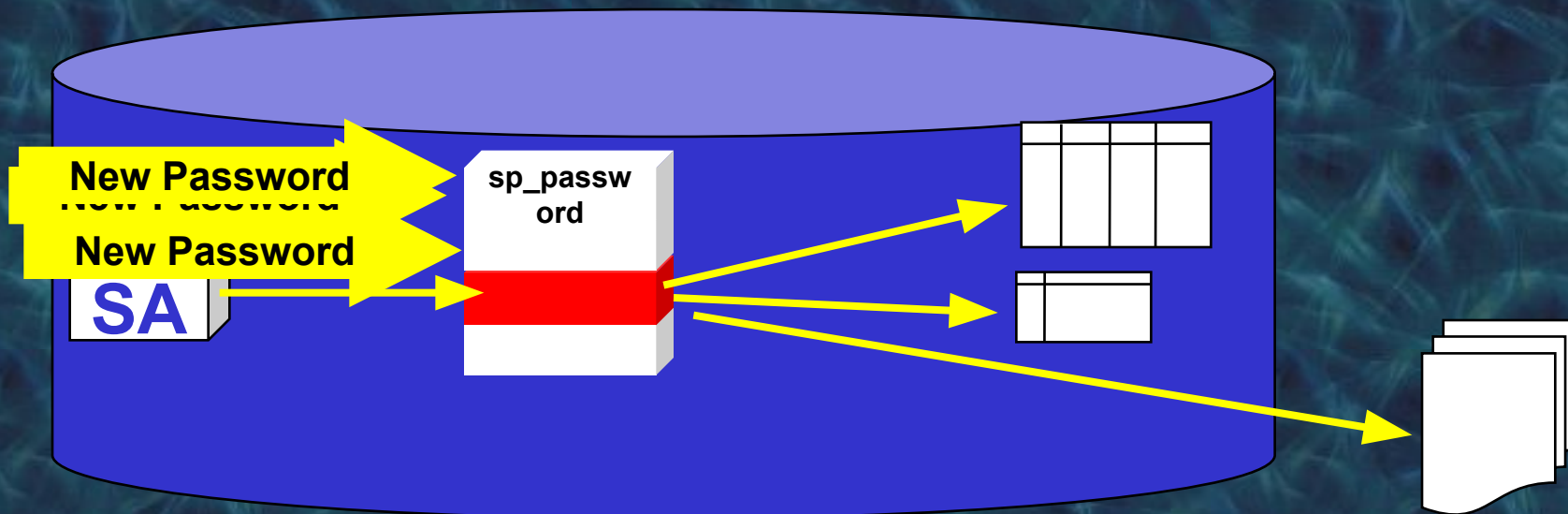
Уязвимости СУБД

- Microsoft SQL Server, Sybase, and Oracle 7 не имеют механизмов контроля возраста пароля
- Определение разумного интервала смены пароля уменьшает риск
- Oracle 8 имеет средства контроля возраста пароля:
 - Password Grace Time
 - Password Life Time
 - Password Reuse Max
 - Password Reuse Time

ELEMENT	MS SQL Server	Sybase AS	Oracle
Login / Account Management			
Stale Logins/ Accounts			
Off Hours Usage			
Attacks			
Password Management			
Strength			
Ageing	No Facility	No Facility	No Facility in 7
Trojan Horses			
Rights / Permissions			

Возраст пароля

Уязвимости СУБД



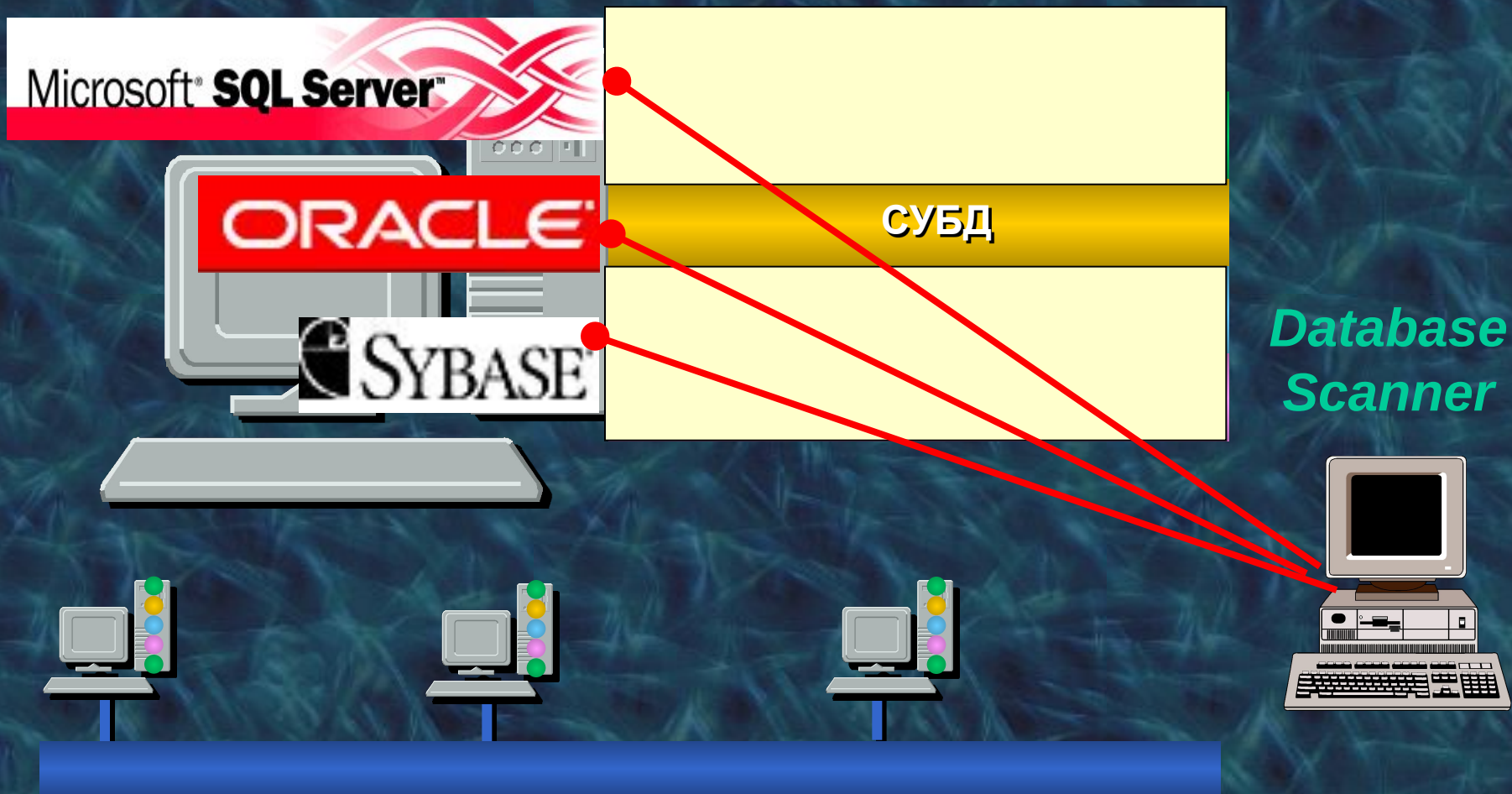
Троянские кони в хранимых процедурах

Уязвимости СУБД

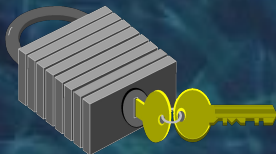


Доступ к ОС через СУБД

Database Scanner

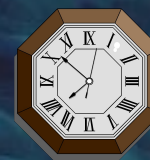


Характеристики Database Scanner

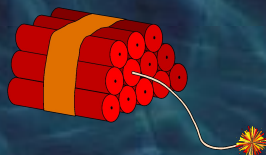


- Выявление слабых паролей.

- Проверка срока действия пароля.



- Обнаружение атак.



- Выявление неиспользуемых бюджетов.



- Проверка ограничений по времени работы.



Группы выполняемых проверок

Authentication	Параметры идентификации и аутентификации
Authorization	Права и допуски пользователей к объектам БД
System Integrity	Параметры ОС (платформы)