Задание по уроку: Подготовка к собеседованию специалиста по информационной безопасности

ФИО: Мочалов Дмитрий Владимирович

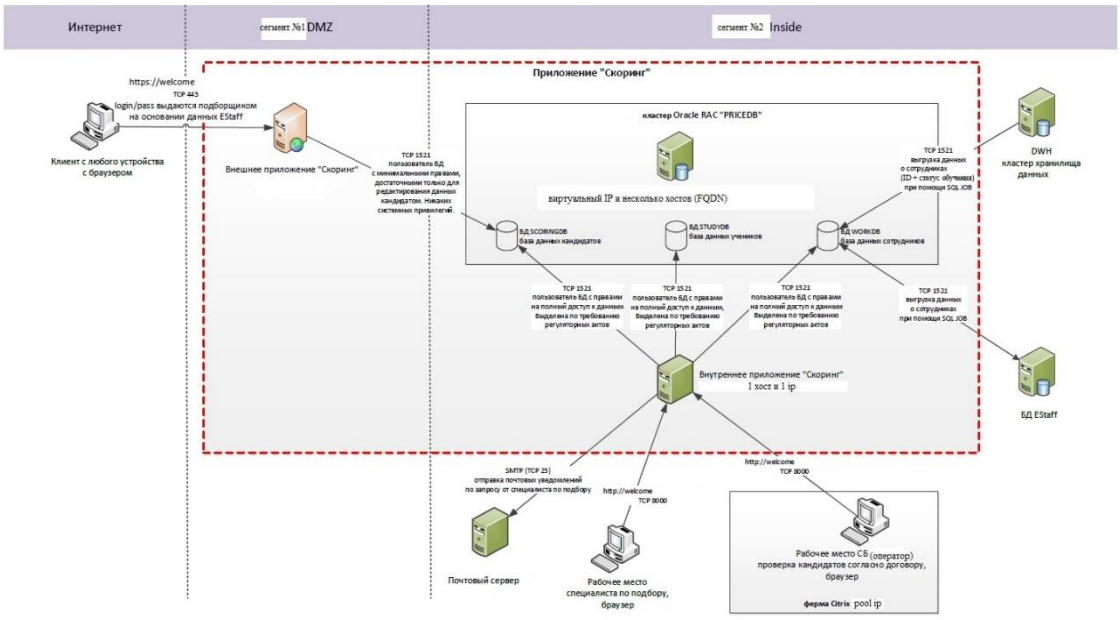
22.09.21

Добрый день!
Направляю первое задание по теме: «Как встать на путь соискателя в сфере ИБ»

Задачи:

Домашнее задание:

1. К уроку приложена схема реализации цифрового проекта. Составить свое экспертное мнение по поводу защищенности планируемой реализации, IT-инфраструктуры и ландшафта, составить предложения по модернизации схемы и внедрению средств защиты (процессы защиты).



Решение:

Мне даётся сложно это задание. Возможно, потому что основную теорию мы прошли несколько месяцев назад и теперь приходится вынимать из памяти сильно забытые вещи.

Пункт 1

Я бы начал защиту с пересмотра защиты от нагрузки

ИБП — защита нагрузки от возможных проблем в цепях электропитания (источник бесперебойного питания).

Пункт 2

Следующее решение было бы за обновлением всех используемых в компании программ до актуальных версий

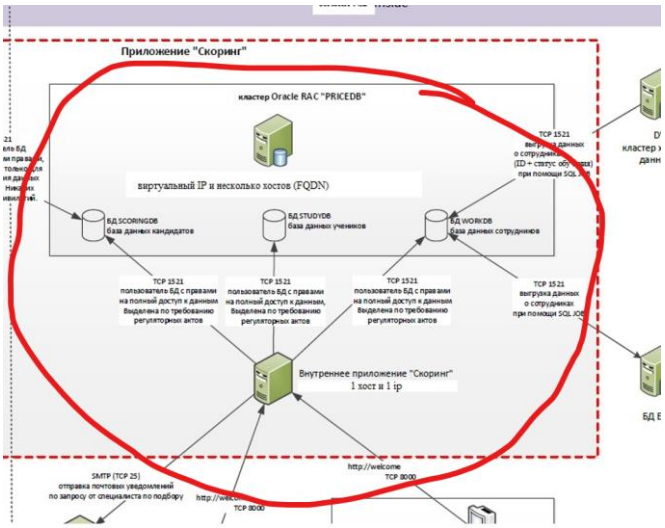
Понимаю, что возможно новые версии программ не совместимы между собой и какие-то костыли бы отвалились. Но для перекрытия базовых рисков пожертвовал бы временем на устранение и создание новых внутренних зависимостей

Пункт 3

Настроил бы права доступа и установил парольную политику в компании
Включил обновление паролей всех пользователей каждый месяц. Хоть и гемор конечному сотруднику, но зато чуть исключает шанс использование старых паролей злоумышленнику

Пункт 4

На этом этапе пришло время для firewall ов. Исключение прав пользователей и зависимости при доступе к БД



Пункт 5

Проработал удалённые подключения пользователей по SSH

Особенно актуально в условиях карантина. Обновить ключ, использовать последнюю версию OpenSSH

Пункт 6

ЛОГИИИИ
Использовал и настроил актуальную систему сбора логов. Для фиксации аномальных запросов и общим слежением за ситуацией