1.Создать пользавателей

iwtm-officer, пароль: xxXX1234, запретить локальный вход в систему

Логин: ldap-user, пароль: xxXX1234, запретить локальный вход в систему

Логин: iwdm-admin, пароль: xxXX1234, права администратора домена

Логин: user-agent, пароль xxXX1234, права пользователя домена

2.Заходим в браузер логин officer пароль xxXX1234 так же делаем синхронизацию

и добавляем iwtm-officer,а так же в настройках ldap-user. Потом перезаходим под iwtm-officer

3.Ввести машины в домен

4. Устанавливаем базу данных PostgreSQL потом ставим device monitor

Вводим ip TM, и токен TM в device monitor

После установки заходим в консоль, вводим логин и пароль

В разделе политики. Создаем даем ей имя “Новое подразделение”

Перемещаем пользователей в это подразделение users а так же создать подразделение computers и тоже перекинуть

5.далее делаем LDAP с AD(редактирование настроек синхронизации)

Выбираем каталог office (то есть синхронизировать computers,users)

6. Делаем беспарольный вход для пользователя iwdm-admin

Добавляем из AD

7. Назначаем роль и сохраняем и Заходим

8.потом вводим в домен user-agent но он уже введен ищем на нем device monitor Выбираем нашего нарушителя user-agent Пишем логин и пароль

И ждем пока не будет завершен процесс распространения

9.

**Задание 1**

Необходимо создать новую политику под названием «Новое подразделение», применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Прописываем правило на HTTPS

**Задание 2**

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину нарушителя для удаленного доступа к серверу агентского мониторинга.

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

**Задание 3**

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: iwdmassistant, пароль: xxXX1234

**Задание 4**

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании

Создаем политику на запрет запуска paint application monitor

Обновляем правила на нарушителе и проверяем работоспособность.

**Задание 5**

Необходимо запретить создание снимков экрана в wordpad для предотвращения утечки секретных расчетов и баз данных.