Модуль 1: Установка и настройка системы

Описание

В компания «Демо Лаб» возникла необходимость внедрения DLP системы InfoWatch Traffic Monitor **версии 6.10** для лучшей защиты разработок и предотвращения утечек прочей информации.

Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием.

Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде VMWare Workstation, сервер с контроллером домена уже установлен и развернут с правильно настроенными сетевыми адаптерами, серверы для установки базы данных Device Monitor и для Device Monitor также предустановлены.
В сети есть виртуальная машина «нарушителя» для установки агента.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов. До установки системы необходимо подготовить доменных пользователей в соответствии заданием.

Стоит отметить, что имена компьютеров (hostname) должны быть уникальными.

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в общем сетевом каталоге.

! *Если в задании необходимо сделать скриншот, необходимо называть его по номеру задания, например: Задание_5_копирование.jpg.*

*Все скриншоты хранятся в папке «**Чемпионат**» на рабочем столе RDP-машины.*

Модуль 1: Установка и настройка системы

Задание 1: Настройка Домена demo.lab

Необходимо создать доменных пользователей и настроить их в соответствии с карточкой дополнительных сведений.

Логин: dbadmin (Админ БД) пароль: xxXX.1234
(права администратора домена)
Логин: dmadmin (Админ ДМ) пароль: xxXX.1234
(права администратора домена)
Логин: user01 (Иван Петров) пароль: xxXX.1234
(пользователь домена)
Логин: iwtmofficer пароль: xxXX.1234
(без права локального входа в систему)

Задание 2: Установка и настройка InfoWatch Traffic Monitor

IWTM уже установлен с активированной лицензией.

Для корректной работы необходимо синхронизировать каталог пользователей и компьютеров LDAP с доменом.

Для управления IWTM необходимо добавить ранее созданного пользователя домена iwtmofficer в качестве офицера безопасности с доступом ко всем разделам и со всеми зонами видимости.
Продолжить работу от данного пользователя.

Запишите IP-адреса, token, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле “iwtm.txt” на рабочем столе RDP машины.

В компании имеется необходимость перехватывать сканы документов, для чего необходимо настроить OCR перехватчик ABBYY. Лицензия и инструкции по установке находятся в общем каталоге.

Необходимо зафиксировать скриншотом момент настройки конфигурационных файлов.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Задание 3: Установка и настройка InfoWatch Device Monitor

Установка IWDM производится в режиме разнесения компонентов: база данных и сервер IWDM на разных машинах.

Необходимо ввести Windows Server DB (**IWDM-DB**) в домен от ранее созданного пользователя **dbadmin**.
Установить базу данных PostgreSQL с паролем суперпользователя `xxXX1234` и разрешить доступ к базе данных извне со всей подсети компании.

Необходимо ввести Windows Server DM (**IWDM-Server**) в домен от ранее созданного пользователя **dmadmin**.

Установить InfoWatch Device Monitor с параметрами по умолчанию, в качестве базы данных использовать ранее установленную базу данных PostgreSQL на другом сервере. Для доступа к БД может понадобиться настройка PostgreSQL.

При установке необходимо настроить локального пользователя для доступа к консоли управления: `officer` с паролем `xxXX1234`

Синхронизируйте IWDM с Active Directory (компьютеры и пользователи) и свяжите IWDM с вашим InfoWatch Traffic Monitor.

Для управления IWDM необходимо добавить ранее созданного пользователя домена dmadmin в качестве офицера безопасности с доступом ко всем разделам и пользователям.
Продолжить работу от данного пользователя в беспарольном режиме (галочка при входе: использовать данные сессии Windows).

Запишите IP-адреса, пароли и названия машин в файл “iwtm.txt” на рабочем столе RDP машины.

Задание 4: Установка InfoWatch Device Monitor Agent (IWTM-W10-Agent)

Необходимо создать доменного пользователя для клиентских машин. Ввести виртуальную машину (одну) нарушителя в домен и войти в систему от ранее созданного доменного пользователя.

Установите InfoWatch Device Monitor Agent на виртуальную машину нарушителя с помощью задачи первичного распространения (без формирования пакета установки) в Device Monitor Server. Зафиксируйте выполнение задачи скриншотом. Проверьте работоспособность IWDM агента.

Запишите IP-адрес и хостнеймы машин в файл “iwtm.txt” на рабочем столе RDP машины.

Задание 5: Установка и настройка подсистемы Crawler

Необходимо установить и настроить подсистему Crawler на Windows Server IWMD.

Создайте общий доступ только на каталог `c:\data\share` на Windows Server IWDM с правами чтения и записи для всех.

Настройте Crawler на автоматическое ежедневное сканирование только ранее созданного каталога вашего Windows Server и зафиксируйте выполнение задания скриншотом настройки crawler в web-консоли IWTM. Сохраните скриншот на рабочем столе компьютера в папке: «Чемпионат».

Задание 5: Проверка работоспособности системы

Необходимо создать проверочную политику под названием «Чемпионат» в InfoWatch Traffic Monitor на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих термин «Чемпионат WorldSkills», установить низкий уровень угрозы для всех событий, добавить тег «Чемпионат».

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя с установленным агентом.

Сделать одну выборку событий, которая будет содержать только по 1 событию каждого типа (передачи, копирования, хранения и буфера обмена). Зафиксировать выполнение скриншотом.

Также необходимо произвести хотя бы одну проверку с помощью технологии OCR (отправить изображение с текстом термина) и зафиксировать сработку скриншотом.