КОНКУРСНОЕ ЗАДАНИЕ

Региональные чемпионаты 2021-22

Сокращенное типовое задание - 85 баллов

Корпоративная защита от внутренних угроз информационной безопасности

Модуль 1
День 2

Менеджер компетенции: А.В. Сергеев

Модуль 1

Динамичное развитие компании Demo.Lab привело к значительному расширению штата и переезду в новый офис. В связи с этим, принято решение о расширении всей ИТ-инфраструктуры компании, в том числе и систем обеспечения корпоративной безопасности.
Необходимо

- либо мигрировать решение (задание 2А) InfoWatch Traffic Monitor (IWTM), согласно рекомендациям, полученным от подразделений внедрения ГК Инфовотч. Основная идея – максимальное разнесение компонент уровня сети (network, IWTM) и хоста (endpoint, IWDM) для распределения нагрузки в связи с увеличением числа сотрудников
  По возможности все настройки и события в системе (как IWTM, так и IWDM) необходимо сохранить при миграции.
- либо провести установку IWTM по схеме all-in-one с нуля (задание 2Б). Этот вариант является допустимым, но менее предпочтительным.

Задание 1: Active Directory

Используется AD настроенный в 1 день соревнований.

Задание 2А: Развертывание DLP уровня сети. InfoWatch Traffic Monitor

В соответствии с Вашей частью пилотного проекта на отдельном сегменте сети «песочницы» Заказчика необходимо разнести на 2 разных машины следующие сетевые компоненты InfoWatch Traffic Monitor:

- Основной сервер безопасности IWTM (Node)
- База данных IWTM (Database)

Ваша задача – установить указанные компоненты IWTM используя распределенный сценарий установки (см рис. 1) или установить «all-in-one».

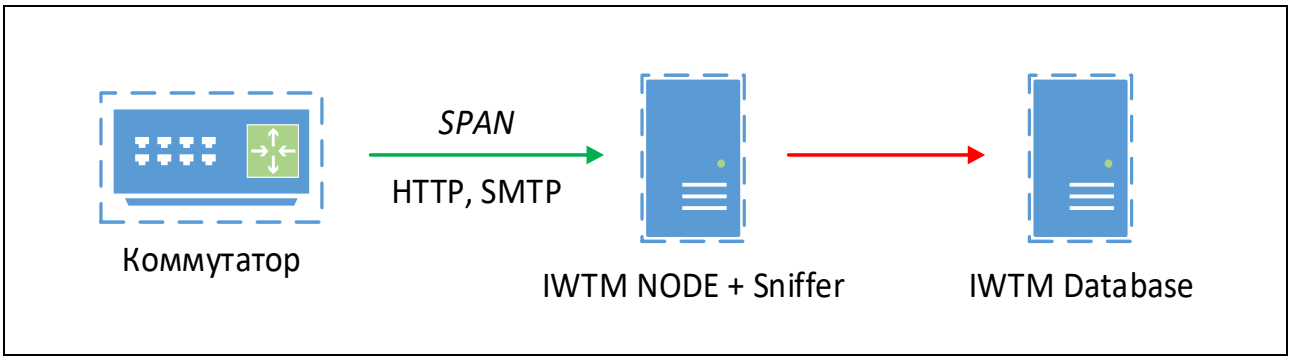

Рисунок 1. Схема развертывания DLP уровня сети

Необходимо мигрировать Node или Database сервер на отдельную машину с сохранением базы данных, установить и настроить перехватчик сетевого трафика (Sniffer) у которого есть 2 сетевых интерфейса (для управления и перехвата трафика).

- **VMNet9** – bridge на внешний сетевой адаптер, управление
- **VMNet10** – bridge на внутренний сетевой адаптер, перехват трафика

Параметры IWTM: версия - Enterprise, СУБД - PostgreSQL.

IP-адрес нового IWTM указан в карточке дополнительных сведений.

Все развернутые сервера должны быть доступны для управления (службы) и мониторинга из консоли управления IWTM.

Подтвердить выполнение задания скриншотами (основные моменты: правка конфигурационных файлов, изменение настроек, проверка работоспособности, отчет о состоянии системы в web-консоли IWTM).

Задание 2Б: Установка “all-in-one”

Установите сервер безопасности InfoWatch Traffic Monitor в виртуальной среде VMWare Workstation. Сервер и СУБД должны быть установлены на одной виртуальной машине со следующими параметрами:

- виртуальный диск размером 80 – 100 ГБ в динамическом режиме;
- 2 процессора, 2 логических ядра;
- 8ГБ ОЗУ.

Параметры IWTM для установки: версия - Enterprise, СУБД - PostgreSQL.

Все дистрибутивы находятся в каталоге с дистрибутивами D:\Additions.

Настройки сетевых интерфейсов указаны в дополнительных сведениях к заданию.

При установке IWTM задайте следующий пароль суперпользователя: `xxXX1234`

Измените пароль офицера безопасности для доступа к веб-интерфейсу IWTM на: `xxXX1234`

Активируйте лицензию, которая находится в каталоге с дистрибутивами.

Для интеграции с Active Directory необходимо получить информацию о пользователях и компьютерах компании «Домен локал» с помощью LDAP-синхронизации.

Запишите IP-адреса и соответствующие им имена машин, токен для подключения IWDM, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные Вами) системы в текстовом файле "iwtm.txt" на рабочем столе (первый ПК на котором развернуты сервера безопасности) ***хостовой машины****.*

Задание 3: Развертывание DLP уровня хоста. InfoWatch Device Monitor.

В соответствии с Вашей частью пилотного проекта сети Заказчика необходимо (а) либо развернуть с нуля (б) либо произвести миграцию InfoWatch Device Monitor (IWDM):

Основной сервер безопасности IWDM установить на машину IWDM-NODE

База данных IWDM должна остаться на виртуальной машине IWDM-DB. Сохранение всех событий и конфигураций будем значительным плюсом.

Версия СУБД IWDM — PostgreSQL.
Ваша задача — установить указанные компоненты IWDM на виртуальные машины (см рис. 2).

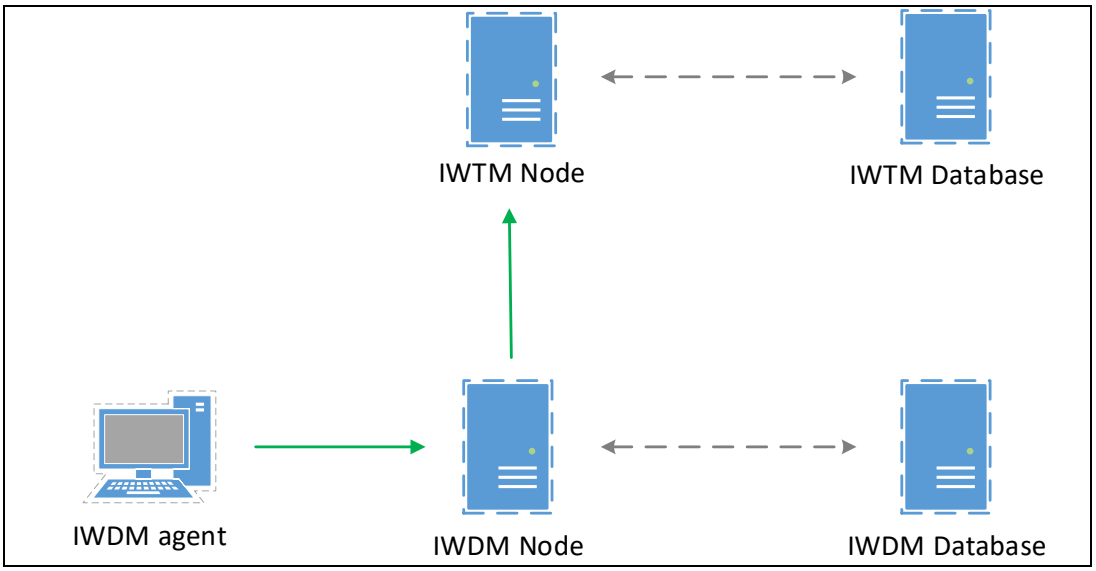

Рисунок 2. Схема развертывания DLP уровня хоста (+ интеграция с DLP уровня сети)

Доменная структура (подразделения и пользователи) уже создана.

Авторизацию на машинах необходимо осуществлять от ранее созданных (admin-dm, useroffice1 и др.) доменных пользователей.

Ключевые этапы процесса установки (миграции), изменения настроек и файлов конфигурации необходимо зафиксировать скриншотами.

Задание 4: Установка InfoWatch Device Monitor Agent

Ввести виртуальную машину нарушителя в домен и войти в систему от ранее созданного доменного пользователя.
Установите InfoWatch Device Monitor Agent на виртуальные машины-нарушителя

- На 1-ю пользовательскую машину – с помощью задачи первичного распространения (без формирования пакета установки) в Device Monitor Server.
- На 2-ю пользовательскую машину – с помощью групповых политик домена. Политика должна применяться только на конкретную машину.

Важно! Плюсом будет реализация всех действий при включенном Брандмауэре Windows, не снижая защищенность системы. Для корректной работы необходимо настроить Брандмауэр (и другие необходимые для этого подсистемы) для взаимодействия компонент IWDM/IWTM.
Проверьте работоспособность IWDM агента.

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.
Плюсом будет реализация всех действий при включенном Брандмауэре Windows. Для корректной работы необходимо настроить Брандмауэр/групповые политики для взаимодействия компонент IWDM/IWTM.

Задание 6: Включение технологии OCR

Необходимо показать Заказчику возможность работы DLP-системы с технологией OCR. Ваша задача – включить технологию OCR (ABBY FineReader Engine 11) в IWTM.

Задание 7: Беспарольное SSH-соединение защищенного доступа к IWTM

Для удаленного управления IWTM Node настройте безопасный беспарольный (по сертификату) доступ по SSH (используя программу PuTTY, с помощью RSA-ключа) с контроллера домена (Domain Controller).

Парольная фраза для ключа (если применимо): xxXX1234

Зафиксируйте все этапы (генерация ключа, подключение) выполнения задания скриншотами.

Сгенерированный ключ необходимо сохранить на рабочем столе компьютера в папке «Чемпионат День 2» с названием «Задание 3»

Задание 8: SSH-ключи для доступа между компонент IWTM

Аналогично заданию 6, сгенерируйте RSA-ключ на IWTM DB и настройте межсерверный доступ по SSH с IWTM Node.

Парольная фраза для ключа (если применимо): 4321XXxx

Зафиксируйте все этапы (генерация ключа, подключение) выполнения задания скриншотами. Сгенерированный ключ необходимо сохранить на рабочем столе компьютера в папке «Чемпионат День 2» с названием «Задание 4»

Задание 9. Защита HTTPS- соединения с IWTM. Создание цифровых сертификатов

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа и т.п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата – на выбор участника из доступных в операционных системах и дистрибутивах ИЛ (openssl или аналоги).

Атрибуты для сертификатов:

Страна:	RU
Область:	Moscow

Организация:	WorldSkills
Город:	Moscow
Отдел организации:	IT
E-mail:	support@demo.lab

Дерево сертификатов должно включать:

- корневой root-сертификат (ca)
- промежуточный (intermediate) сертификат
- серверный (server) сертификат
- пользовательский (user) сертификат

Итоговый результат должен включать:

- Дерево из 3-х сертификатов, представленные в виде отдельных файлов ключей и сертификатов (3 ключа .key, 3 сертификата .crt).
- Содержимое скрипта по генерации ключей и сертификатов (или перечень команд или скриншотов из использованной для генерации сертификатов утилиты)
- Скриншоты промежуточного серверного сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертификации»).
- Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании Demo.lab и т.п.

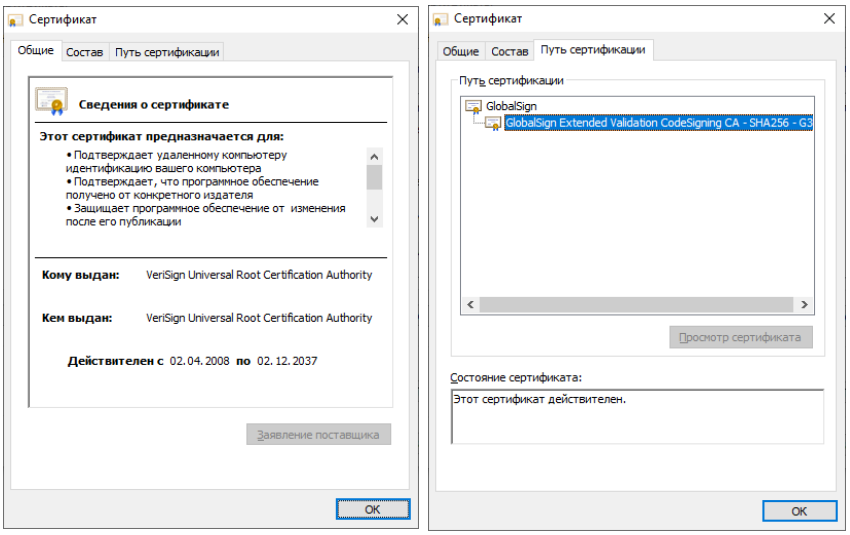

Рисунок 3. Пример сертификатов

Генерацию сертификатов зафиксируйте скриншотами
Созданные сертификаты, ключи, скрипты для их создания и скриншоты процесса разместите в папке «Certificates IWTM» на рабочем столе компьютера

Задание 10. Защита HTTPS- соединения с IWTM. Использование цифровых сертификатов

Примените цифровые сертификаты для защиты клиент-серверного соединения по протоколу HTTPS при подключении к веб-консоли IWTM с узлов: demolab.demo.lab (AD).

Наилучшим образом выполненное задание подразумевает клиент-серверную (двустороннюю) аутентификацию: сервер предъявляет серверный сертификат, клиент – клиентский.

Для корректной работы клиент-серверной аутентификации клиентский цифровой сертификат может быть установлен в системное хранилище («Личные» или «Другие пользователи») с использованием групповых политик (автоматически).

Использование только серверного сертификата (на стороне веб-сервера IWTM) менее безопасно.

Проверку необходимо осуществить с браузера Google Chrome.
Зафиксируйте все этапы выполнения задания (настройка веб-сервера, нахождение клиентских сертификатов в хранилище, установка защищенного HTTPS-соединения и т.п.) скриншотами

Задание 11: Проверка работоспособности системы с помощью политик безопасности

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 термины «Чемпионат» и «Чемпионат 2021», установить низкий уровень угрозы для всех событий, добавить тег «Чемпионат».

Все объекты, технологии и т.п., связанные с данной политикой, называйте «Чемпионат, Чемпионат 1» и т.д. 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.

Необходимо создать запрос, выводящий информацию только о четырех событиях разных типов (передача, копирование, хранение и буфер обмена), по одному событию на каждый тип.

Сохраните скриншот выборки на рабочем столе контроллера домена в папке: «Чемпионат».

Так же необходимо сделать 2 скриншота событий передачи, где перехватчиком является ICAP и sniffer. Скриншоты сохранить на рабочем столе компьютера в папке «Чемпионат».