

Региональный этап чемпионата по
профессиональному мастерству «Профессионалы» и
чемпионата высоких технологий Республики
Башкортостан

по компетенции:

F7 «Корпоративная защита от внутренних угроз
информационной безопасности»

Конкурсное задание

День 2

Уфа 2023

Модуль А: Установка и настройка системы

Описание

Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) системного интегратора DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и развернуть DLP-систему на отдельном сегменте сети.

В «песочнице» развернут контроллер домена (с каталогом AD), с которым необходимо будет осуществить интеграцию DLP-системы. До установки системы необходимо подготовить доменных пользователей.

В качестве виртуальной инфраструктуры для пилотного проекта используется среда виртуализации VMware Workstation.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM). Необходимо развернуть компоненты уровня сети (network) и хоста (endpoint).

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

Необходимо использовать следующие виртуальные машины:

- **AD-Demo.lab** (контроллер домена demo.lab, права хостовая машина)
- **Astra TM** (предустановленный, права хостовая машина)
- **DB-IWDM** (Windows Server для IWDM-DB, права хостовая машина)
- **WSRV-IWDM** (Windows Server для IWDM, левая хостовая машина)
- **Дополнительные ВМ для IWTM**

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

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

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

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

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.

С целью повышения безопасности сервер IWTM был развернут на ОС специального назначения Astra Linux SE 1.6.

Необходимо мигрировать решение InfoWatch Traffic Monitor (IWTM), согласно рекомендациям, полученным от подразделений внедрения ГК Инфотеч. Основная идея – максимальное разнесение компонент уровня сети (network, IWTM) и хоста (endpoint, IWDМ) для распределения нагрузки в связи с увеличением числа сотрудников.

По возможности все имеющиеся настройки и события в системе (как IWTM, так и IWDМ) необходимо сохранить при миграции.

Задание 1: Развертывание DLP уровня сети. InfoWatch Traffic Monitor.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM). Необходимо мигрировать или развернуть с нуля компоненты уровня сети (network) и хоста (endpoint).

В соответствии с Вашей частью пилотного проекта на отдельном сегменте сети «песочницы» Заказчика необходимо мигрировать или установить с нуля на 3 разных машины следующие сетевые компоненты InfoWatch Traffic Monitor:

- Основной сервер безопасности IWTM (Node) (Astra Linux SE 1.6)
- База данных IWTM (Database) (Astra Linux SE 1.6)
- Вспомогательный сервер IWTM (Sniffer) для приема копии трафика с виртуального коммутатора (CentOS 7)

Система, установленная без сохраненных событий допустима, но оценивается меньшим количеством баллов. Допускается установка IWTM Node и IWTM DB на CentOS 7, это не будет считаться полноценно выполненным заданием.

Необходимо мигрировать Node или Database сервер на отдельную машину с сохранением базы данных на отдельной машине, установить и настроить перехватчик сетевого трафика (Sniffer) на отдельный сервер IWTM (Sniffer). Для перехвата трафика можно использовать второй адаптер на хостовой машине.

Параметры IWTM: версия — Enterprise, СУБД — PostgreSQL.

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

Ваша задача — установить указанные компоненты IWTM используя распределенный сценарий установки (см рис. 1).

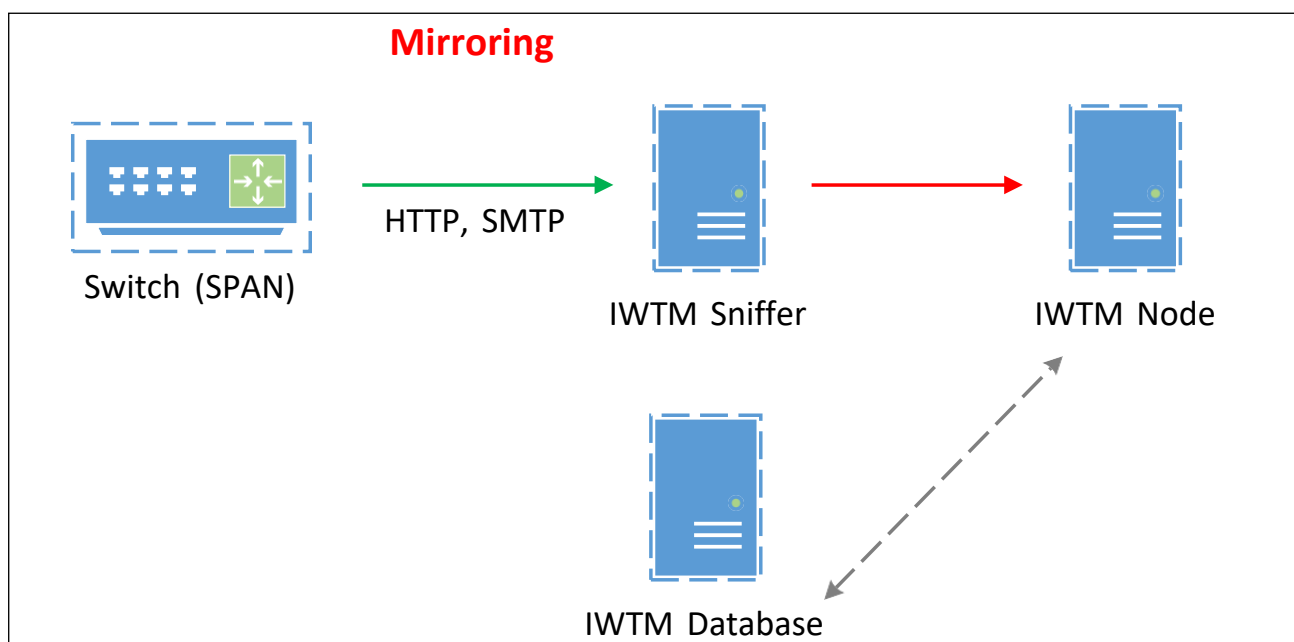


Рисунок 1. Схема развертывания DLP уровня сети.

Интерфейсы VMWare ESXi необходимо определить и настроить самостоятельно.

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

Задание 2: Развертывание DLP уровня хоста. InfoWatch Device Monitor.

В соответствии с Вашей частью пилотного проекта сети Заказчика необходимо произвести миграцию следующих endpoint-компонентов InfoWatch Device Monitor (IWDM):

- Основной сервер безопасности WSRV-IWDM (Node)
- База данных DB-IWDM (Database) . **Сохранение всех событий и конфигураций**

будет значительным плюсом.

Версия СУБД IWDM для установки или миграции — PostgreSQL.

В случае невозможности сохранения конфигурации допускается установка с нуля. Это не будет являться полным выполнением задания, но позволит перейти к следующим этапам.

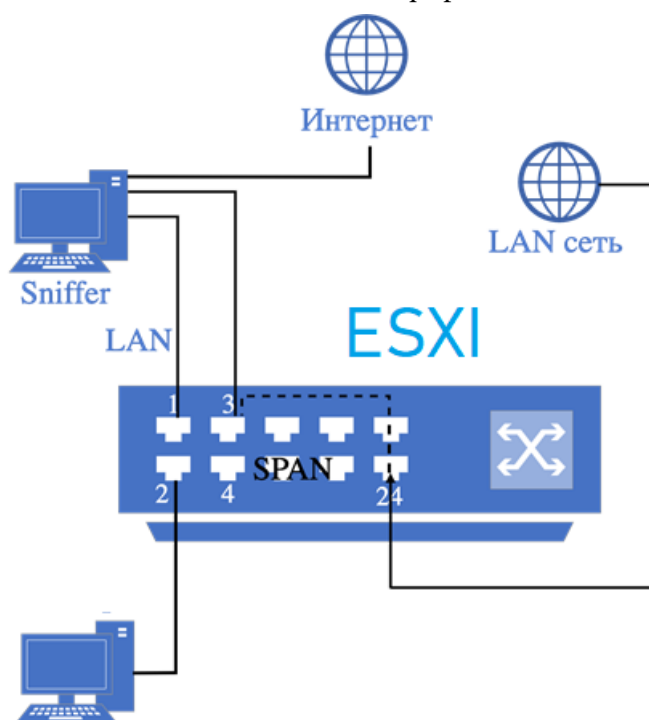
При разнесении компонентов необходимо учесть ПРАВИЛЬНОЕ расположение виртуальных машин на хостовых компьютерах. Модуль может быть аннулирован, при неправильном расположении виртуальных машин на хостах.

Задание 3: Подключение источников информации для DLP уровня сети (IWTM).

Зеркалирование трафика.

После развертывания сетевых компонентов IWTM необходимо включить приемкопии трафика с коммутатора (для протоколов HTTP).

Ваша задача – настроить IWTM на захват и анализ трафика в соответствии с рис. 1



и рис. 2.

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

Задание 4: Проверочная политика.

Необходимо создать новую или использовать имеющуюся политику на проверку установленной системы (после миграции).

Политика должна работать на: Правило передачи (используя только подключенный ранее режим SPAN), копирования, буфера обмена (или работы в приложениях), а также хранения.

Зафиксировать создание и выполнение политики скриншотами.

Также необходимо создать выборку только на правила SPAN (2 и более). Рекомендуется сделать скриншот подтверждения, что данная политика работает, используя Sniffer.

Задание 5. Защита HTTPS-соединения с IWTM. Создание цифровых сертификатов

Для корректной работы некоторых сервисов, предоставляемых внутри компании, заказчику необходимо развернуть структуру PKI. Сгенерированные сертификаты (и вся цепочка доверия) не должны иметь ошибок, критических полей (кроме указанных) или неверных данных. Так же после генерации всех сертификатов, они должны быть установлены в локальное хранилище на контроллере домена.

Все сертификаты и соответствующие им закрытые ключи должны быть помещены в папку на рабочем столе. Далее указана информация для сертификатов, которую они должны содержать. Можно использовать любое удобное ПО для работы с сертификатами, не допускается ошибок в основных и дополнительных полях сертификата.

Общие свойства (поля) для всех сертификатов:

Страна: RU
Город: Ufa
Организация: Proffessional
Подразделение: IT

Корневой сертификат:

commonName: CA
E-mail: ca-support@demo.lab
Период действия: 10 лет
Альтернативные имена субъекта по DNS: CA; CA.demo.lab

Промежуточный сертификат:

commonName: Intermediate
E-mail: support@demo.lab
Альтернативные имена субъекта по DNS: Intermediate; Intermediate.demo.lab

Серверный сертификат (должен запрашиваться с сервера IWTM при соединении с ним через браузер):

На усмотрение участника, должно поддерживаться защищенный доступ подоменному имени и/или IP сервера

Пользовательский сертификат (должен запрашиваться с клиентов присоединении с сервером IWTM через браузер):

На усмотрение участника, должно поддерживаться защищенный доступ подоменному имени и/или IP сервера

Генерацию сертификатов зафиксируйте скриншотами.

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

Задание 6. 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 узла AD-demo.lab по DNS-имени вашего Traffic Monitor. Корневой сертификат должен быть установлен на всех машинах сети с помощью групповых политик. Также необходимо установить серверный сертификат на веб-сервер Traffic Monitor, а клиентский — на необходимые устройства в сети.

Проверку необходимо осуществить с помощью браузера Google Chrome. Предъявление сертификата сервером и клиентом оценивается выше, чем только сервером.

Необходимо также сделать доступ с помощью Rutoken

Зафиксируйте все этапы выполнения задания (настройка веб-сервера, создание групповой политики, список сертификатов в хранилище домена, установка защищенного HTTPS-соединения и т. п.) скриншотами.

Необходимо указать в отчете, с помощью какого DNS имени осуществлялась проверка соединения.

Задание 7: Беспарольное SSH-соединение защищенного доступа к IWTM

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

Парольная фраза для ключа (если применимо): xxXX1234 (или своя, поместить в

файл отчета на рабочем столе), файл ключа также сохранить рядом с файлом отчета.

Зафиксируйте все этапы (генерация ключа, подключение) выполнения задания скриншотами. Необходимо сохранить SSH-сессию в SSH-клиенте для проверки

Задание 8: SSH-ключи для доступа между компонент IWTM

Аналогично заданию 7, сгенерируйте RSA-ключ на IWTM DB и настройте межсерверный доступ по SSH с IWTM Node на IWTM DB.

Парольная фраза для ключа (если применимо): xxXX1234 (или своя, поместить в файл отчета на рабочем столе)

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

Задание 9: Разверните ALD Pro

В связи с последними событиями и санкциями ваша задача начать переход на инфраструктуру Astra Linux, поэтому ваша задача развернуть ALD PRO протестировать и синхронизировать с AD.

Зафиксируйте все этапы (настройка конфига) выполнения задания скриншотами.

Модуль Е. Анализ выявленных инцидентов.

Работа с IDS/SIEM

Введение

Необходимо установить, настроить и проверить IW ARMA IF.

Задание включает проверку на обнаружение известных атак (сгенерированных участником).

Все действия необходимо документировать скриншотами в формате: IDS-2-1-3, где Т — Task (задача), 1 — номер задания, 2 — подпункт задания (при наличии), 3 — шаг.

На каждое задание **ОБЯЗАТЕЛЬНО** необходимо сохранять скриншоты всех действий по изменению настроек (установка, использование конструктора фильтров, создание отчетов и т. д.) и проверке работоспособности системы и правил. Формат скриншотов для документирования действий указан выше.

ВАЖНО! Запрещается воздействовать на инфраструктуру чемпионата, объекты информатизации на площадке и за пределами площадки, машины других участников и экспертов. Объектами атак при моделировании угроз должны быть только собственные виртуальные машины.

При выполнении заданий рекомендуется использовать следующие виртуальные машины: IW ARMA IF (необходимо создать и настроить), незащищенные машины OWASP (необходимо создать и настроить), дистрибутивы для тестирования (Kali) или иные свободные утилиты и ОС.

Задание 1. Начальная установка и настройка систем IW ARMA IF

1. Образ IW ARMA IF необходимо развернуть в VMWare Workstation.

а. Для подключения возможны два варианта (настроить интерфейсы, адресацию для интерфейсов выбрать самостоятельно):

1) Использовать 1 сетевой интерфейс для управления, 2 — для перехвата трафика (в общей сети NAT)

2) Использовать один интерфейс для всех VM в неразборчивом режиме

б. Настроить нового администратора системы с полным доступом (officer).

с. Загрузить и применить актуальные правила (результат успешной загрузки зафиксировать).

Зафиксировать выполнение задания скриншотами: настройка сетей, пользователей.

Записать все логины и пароли в файле ARMA.txt на рабочем столе!

Задание 2. Базовая работа с правилами IW ARMA IF

1. Создать и применить пользовательское правило IW ARMA IF обнаружения попыток доступа к сетевым папкам виртуальной машины (win). Проверить выполнение с помощью виртуальной машины.

2. Провести детектирование трафика согласно указанным правилам с помощью ARMA

Зафиксировать выполнение задания (правила и обнаруженные события) скриншотами.

Задание 3 Проверка системы на выявление известной атаки:

1. Самостоятельно, с помощью утилит Kali Linux или аналогичных имитировать атаку (на выбор) на любую виртуальную машину (в дистрибутивах выложена машина OWASP) или иной сетевой трафик

2. Зафиксировать детектирование атаки с помощью IW ARMA IF

4. Подготовить отчет об обнаруженной атаке согласно прилагаемому в дополнительных файлах шаблону, назвать Отчет об известной атаке.docx

Зафиксировать выполнение задания скриншотами. Разместить отчет на Рабочем столе компьютера.

Задание 5. Формирование отчетов

1. Сформировать отчет в IW ARMA IF по событиям из задания 3 (параметры на выбор)

Все отчеты зафиксировать скриншотами.

Отчеты DLP

Задание 1. Пользователь

Необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий.

- Логин: reportsuser, пароль: XxXx5467

Задание 2. Сводки

Создайте новые вкладки сводки в разделе «Сводка» под названием «ХТ2022» и «Особые сводки»

Задание 3. Виджеты

При создании выборок для сводок необходимо помещать их в каталогвыборок «НТ2022»

Выборки, виджеты, сводки должны содержать минимум 1 событие!

Создайте в сводке «ХТ2022» 4 виджета:

1. Выборка по событиям краулера за последний месяц
2. Выборка по политикам с технологиями: текстовые объекты, печати, эталонные документы за последние 7 дней
3. Статистика по политикам за последние 14 дней
4. Топ нарушителей за последнюю неделю

Задание 4 Особая сводка

5. Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки», отображающий события с уровнем угрозы от низкого до высокого на правила копирования и хранения за последние 7 дней.

Зафиксировать скриншотом конструктора выборки.

6. Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) только с высоким уровнем угрозы за последние 3 дня.

Зафиксировать скриншотом конструктора выборки.

7. Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки» для отображения нарушений событий Sniffer (SPAN) за последние 3 дня.

Зафиксировать скриншотом конструктора выборки.