Областное государственное бюджетное профессиональное

образовательное учреждение «Томский индустриальный техникум»

Компетенция: **Корпоративная защита от внутренних угроз информационной безопасности**

Методическое пособие по подготовке к демонстрационному экзамену для специальности 09.02.06 «**Сетевое и системное администрирование»**

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

В наши дни одним из наиболее актуальных вопросов защиты корпоративной информации является обеспечение безопасности от внутренних утечек по техническим каналам связи. Одна из главных угроз корпоративной информационной безопасности – неправомерные действия сотрудников, приводящие к потере конфиденциальных данных, совершенные как целенаправленно, так и из-за халатности, невнимательности или незнания элементарных правил безопасности предприятия.

Специалисты по корпоративной безопасности должны обладать теоретическими знаниями по обеспечению корпоративной защиты от внутренних угроз, понимать аспекты применения нормативно-правовой базы для классификации и расследования инцидентов, в совершенстве владеть системами и технологиями для достижения целей защиты.

Корпоративная защита от внутренних угроз информационной безопасности обеспечивает защиту от внутренних утечек данных, произошедших умышленно или по неосторожности через технические каналы связи.

Компетенция «Корпоративная защита от внутренних угроз информационной безопасности» включает в себя реализацию профессиональных мер и действий, связанных с защитой предприятия от внутренних угроз информационной безопасности.

Студенты, которые сдают демонстрационный экзамен по данной компетенции должны знать основы корпоративной защиты от внутренних угроз, понимать, как применять нормативно-правовую базу для классификации и расследования инцидентов, уметь использовать системы и методы, предназначенные для защиты данных.

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 54.

| №п/п | Модуль, в котором используется критерий | Критерий | Время выполнения Модуля | Баллы | | |
|---|---|---|---|---|---|---|
| | | | | Судейские | Объективные | Общие |
| 1 | 1. Установка и конфигурирование компонентов DLP системы | A. Организация работы и управление | 2 часа | 0 | 18 | 18 |
| | | B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз | | | | |
| 2 | 2. Технологии агентского мониторинга | C. Технологии агентского мониторинга | 1.5 часа | 0 | 13 | 13 |
| 3 | 3. Разработка и применение политик, анализ выявленных инцидентов | D. Разработка политик безопасности, анализ выявленных инцидентов | 3 часа | 0 | 23 | 23 |
| | | | Итого: | | 54 | 54 |

**Список оборудования и материалов, запрещенных на площадке**

• Мобильные телефоны, смартфоны, рации, беспроводные, проводные наушники и другие средства связи;

• Собственные заметки, шпаргалки, книги и прочие документы;

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

• Личная электронная почта, мессенджеры и прочие средства связи посредством сети Интернет за исключение разрешенных ресурсов для тестирования систем в процессе работы;
• Компьютеры, ноутбуки, планшеты и прочие устройства, за исключением устройств, предоставленных площадкой;
• Периферийные устройства (клавиатуры, манипуляторы типа мышь и прочие устройства) за исключением устройств, предоставленных площадкой.

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

**Модуль 1: Установка и конфигурирование компонентов DLP системы**

Введение

В компания «Демо Лаб» возникла необходимость внедрения DLP системы 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, сетевые интерфейсы настроены, но IP адреса нужно назначить согласно прилагаемой карточке. Подготовлены следующие виртуальные машины для дальнейшей работы:

AD Сервер с контроллером домена

DLP сервер установлен (но не настроен), активирована лицензия

Виртуальная машина для установки сервера агентского мониторинга

Виртуальные машины «нарушителей» для установки агентов

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

Для большей сетевой безопасности в компании все устройства должны иметь статический IP-адрес. Сетевые настройки указаны в дополнительных сведениях к заданию.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными в соответствии с номером рабочего места (например, server-16).

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

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания.

Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания

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

Модуль А. Организация работы и управление

- Прибрать за собой рабочее место (после каждого модуля)
- Не опаздывать с перерывов
- Закрыть профиль после выполнения модулей (Win+L)

Модуль В. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Пред настройка:

| | | | | |
|---|---|---|---|---|
| Demo.lab | 172.16.X.2 | 255.255.255.248 | 172.16.X.1 | 127.0.0.1 |
| IWTM | 172.16.X.3 (Linux) | 255.255.255.248 | 172.16.X.1 | 172.16.X.2 |
| IWDM | 172.16.X.4 | 255.255.255.248 | 172.16.X.1 | 172.16.X.2 |
| W10-agent | 172.16.X.5 | 255.255.255.248 | 172.16.X.1 | 172.16.X.2 |

Изменение Ip адреса на ОС Linux

Nmtui

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

Edit a com…..
<edit>
Изменяем на manual
Ip адрес вводим в формате: 172.16.X.3/29 ( вводим основной шлюз и DNS)
Вводим домен: demo.lab
!!!!!!!!!
Необходимо на виртуальной машине Demo.lab, открыть оснастку DNS – readme – iwtm – меняем IP адрес на 172.16.X.3
Выполним проверку:
Заходим на виртуальную машину Demo.lab, открываем браузер Google, вводим Ip адрес 172.16.X.3 (Linux) – должен открыться сайт
Задание 1. Настройка контроллера домена
Необходимо создать и настроить следующих доменных пользователей с соответствующими правами: Логин:
user1, пароль: 12345678, запретить локальный вход в систему
Логин: user2, пароль: 12345678, запретить локальный вход в систему
Логин: user3, пароль: 12345678, права администратора домена и локального администратора
Логин: user4, пароль 12345678, права пользователя домена
Создание пользователей:
AD пользователи и компьютеры – Users
Пароль по заданию 12345678 создать нельзя, не позволит политика безопасности:
Есть 2 варианта решения проблемы:

1. Изменить политику безопасности
2. Поставить пароль P@ssw0rd и записать его в документе, чтобы эксперты знали пароль

   User 1 и User 2

   Необходимо создать новую групповую политику в домене demo.lab
   Имя политики – запрет анимации
   Переходим во вкладку – «прошедшие проверку» - добавить – user1 – проверить имена - добавить
   user2 – проверить имена - добавить
   domain computers – проверить имена - добавить
   Ок
   Нажимаем на нашу политику – изменить
   Конфигурация ПК – политики – конфигурация Windows – параметры безопасности – локальные политики – назначение прав пользователя – запретить локальный вход
   Политика безопасности – определить
   user1 – проверить имена - добавить , user2 – проверить имена - добавить/применить/ок
   user 3
   Члены групп – добавить – Domain Admins – проверить имя – добавить – ок
   user 4
   Только проверить! Члены групп – Domain users

Задание 2. Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Настроить DNS на сервере для корректной работы.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя.

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWTM.

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

Добавить машины **IWDM, W10-agent** в домен Demo.lab (изменить имя ПК, пользователь demo\user3)

Заходим на виртуальную машину Demo.lab, входим в системы (открыть браузер и ввести ip адрес 176.16.X3)

Логин: officer

Пароль: xxXX1234

ШАГ 1: Проверяем наличие активной лицензии (управление – лицензии, статус – активная)

ШАГ 2: Управление – LDAP синхронизация – серверы

+ добавить LDAP сервер

Имя: demo.lab

Тип: AD

Ежеминутно – 15 минут

LDAP сервер: 172.16.x.2

Использовать глобальный каталог ∨

LDAP запрос: DC=demo,DC=lab

Логин: demo\user3

Пароль: от пользователя user3

Проверить соединение - сохранить – проверить соединение

ШАГ 3:

Пользователи

управление доступом – роли – область видимости - пользователи – добавить из LDAP – user3 – сохранить

Добавить следующие данные:

Роль: администратор, офицер безопасности

Область видимости: постоянный доступ

E-mail : придумать

Задание 3. Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить базу данных с паролем суперпользователя 12345678.

Установить сервер агентского мониторинга с параметрами по умолчанию.

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

При установке необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, но можно сделать это и после установки сервера агентского мониторинга.

Настроить пользователя консоли управления: officer с паролем 12345678.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить вход в консоль управления от ранее созданного пользователя, установить полный доступ к системе, установить все области видимости.

Зафиксировать факт создания пользователя и настройку скриншотом.

Проверить работоспособность входа в консоль управления без ввода пароля. Стоит обратить внимание, что если сервер не введен в домен, данная опция работать не будет.

Зафиксировать факт подключения без пароля скриншотом.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM

Зайдите на виртуальную машину **IWDM** под пользователем **user3**

ШАГ 1. Устанавливаем базу данных **PostgreSQL** с паролем 12345678

ШАГ 2. Установить сервер агентского мониторинга **InfoWatch Device Monitor**

Во время установки выбрать: и сервер и консоль – основной сервер – сервер БД 127.0.0.1, имя:IWDM имя: postgres, пароль 12345678

Создать новый ключ ( сохранить где лежат установщики)

Смотрим задание имя: officer , пароль:12345678

ШАГ 3. На рабочем столе смотрим «консоль управления»

Адрес: 127.0.0.1 officer 12345678

Инструменты – настройки – синхронизация политик .....

Адрес 172.16.X.1

Вводим токен ( чтобы его узнать заходим в виртуальную машину Demo.lab, открываем DLP систему. Управление – плагины – токены – содержание)

Применить – сохранить

ШАГ 4:

Инструменты – настройки – интеграция AD

Выбрать домен из леса – проверка соединения

Логин: demo\user3

Синхронизируем директорию – выбрать весь домен – запустить

ШАГ 5:

Инструменты – пользователи консоли – роли – добавить пользователя из AD – найти user3 – роли: администратор, офицер безопасности – далее везде добавить

Зайти от пользователя user3 сделать скриншот

Задание 4. Установка агента мониторинга на машине нарушителя

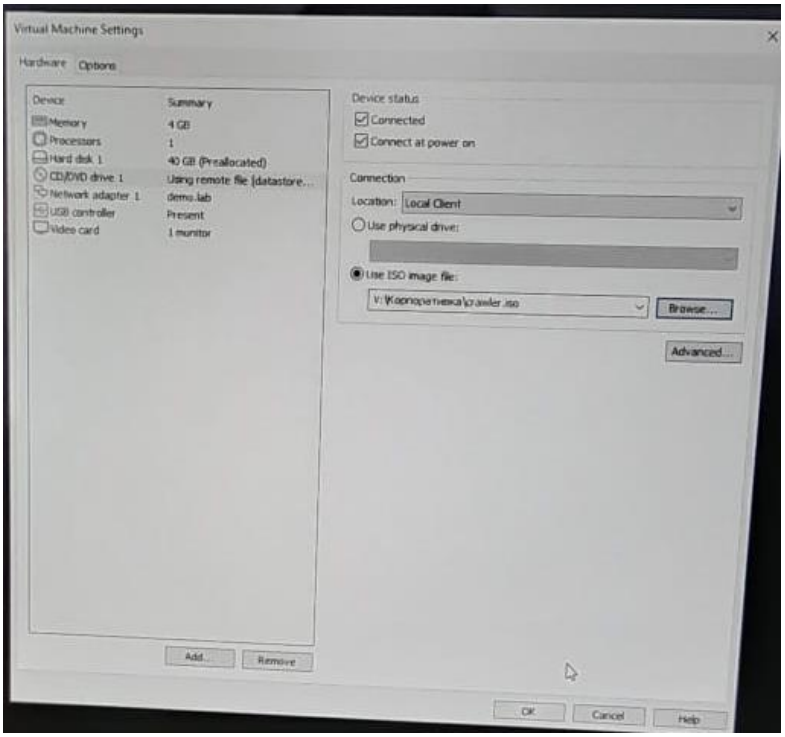
Необходимо ввести клиентскую машину в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить агент мониторинга с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания пакета установки является неверным выполнением задания. Зафиксировать успешное выполнение задачи скриншотом

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

В случае проблем стоит проверить настройки брандмауэра и DNS
IWDM
Рабочий стол-консоль управления - интеграция с AD - проверить ПК и пользователей
Задачи - +(добавить) - наименование: установка - тип: задача первичного распространения - далее - добавить (директория - Computeres - W-10 (клиент)) - далее - далее по задание пароль не нужен, но мы добавим
Пароль: 12345678
логин: demo\user3
пароль: тот который вы поставили пользователю user3
далее – готово
сразу запускается и сама перейдет в статус установка, после статус ожидается перезагрузка - зайти на клиент и перезагрузить

Задание 5. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)
Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга.
Необходимо создать общий каталог Share в корне диска и установить права доступа на запись и чтение для всех пользователей.
Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.
Зафиксировать выполнение задания скриншотом настройки в webконсоли.
Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.
IWDM
Устанавливаем **Crambler**
Заходим в настройки виртуальной машины
Settings (см.фото)




Открываем установщик

Далее – соглашаемся - далее – далее – далее - выбираем postgreSQL - Ip адрес или DNS ... 172.16.X.3 - имя базы данных: postgres - имя пользователя: iwtm_linux - пароль xxXX1234 – далее

Параметры подключения агента Consul

Для того, чтобы посмотреть имя центра обработки данных и ключ, заходим на виртуальную машину linux и прописываем команду

**#cat /etc/infowatch/consul/consul.json**

нам нужны: datacenter, encrypt

Вводим данные в установщик – далее

Заходим в DLP систему

Управление - плагины - infoWatch Crawler - токены - содержание - вводим в установщик - далее - далее – установить

Проверка

Заходим в DLP систему

Краулер - если написано "Выберите задачу или создайте новую" - все настроено верно

Заходим на машину IWDM

Этот ПК - диск С - создать папку Share - предоставить доступ - отдельные люди - все - чтение и запись - добавить - поделиться – готово

Заходим в DLP систему

**Смотрим задание!**

Краулер - +(добавить) - название: share - цель сканирования: разделяемые сетевые ресурсы - сканируемые группы и компьютеры: IWDM - режим сканирования: только папки - фильтр: C:\Share - период сканирования: ежедневно - начало действий: поставить сегодняшнее число

Сделать скриншот

Задание 6. : Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

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, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Заходим в DLP систему

Политики - добавить политику: политика защиты данных – название: проверочная политика – сохранить

Списки - тэги - +(добавить) – название :экзамен – сохранить

Объект защиты - создать – название :экзамен – сохранить

Технологии - текстовые объекты - +(создать) – название :экзамен - сохранить - выбрать его из списка - редактировать - + (добавить) шаблон - тип шаблона: строка - строка: экзамен – сохранить

Открываем созданную политику : проверочная политика

Видим 4 вкладки : Передача, копирование, хранение, работа в прил.

**По заданию!!!!**

Передача - добавить правило - направление маршрута: в оба направления - тип события: выбрать все - назначить событию теги: экзамен - уровень нарушения: низкий - каталоги объектов защиты: экзамен – сохранить

Остальные вкладки настраиваем по аналогии

Общая настройка проверочной политики с правой стороны "защищаемые данные" - выбрать экзамен

## Модуль С. Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т.д. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где CP – сокращение от англ. creating a policy, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики: P
W-1-2.jpg

где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание 1. Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику. Зафиксировать выполнение скриншотом.

Машина IWDM

Консоль управления

Политики – создать – политика 1 – сохранить

Группа компьютеров – группа компьютеров по умолчанию – выбираем компьютер нарушителя (клиент) - политика: политика1 – сохранить

Сделать скриншот

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.

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

Машина IWDM
Установщик копируем в папку share
Заходим на машину клиента – этот ПК – вводим в строку поиска: **\\IWDM\Share** и установщик копируем на рабочий стол
Приступаем к установки – сервер удалить, оставить только консоль управления – далее – установить – готово
Сделать скриншот по заданию

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: user1, пароль: 12345678
Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.
Машина IWDM
Консоль управления – инструменты - пользователи консоли и роли – создать
Смотрим задание
Логин: user1
Пароль:12345678
Видим сотрудников – добавить – офицер безопасности
Видим компьютеры – для всех групп компьютеров – сохранить
Заходим на клиента – консоль управления – 172.16.X.4 – user1 – 12345678
Сделать скриншот
Задание 4. Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.
Проверить работоспособность и зафиксировать выполнение скриншотом.
Машина IWDM
Консоль управления – приложения - +правило 1 – сохранить
Правило 1 – загрузить приложения – локальный диск С – windows – system 32 – mspain (в поиске) – открыть – сохранить
Политика – политика 1 – добавить правило – наименование: правило 1 - ∨запретить запуск приложения – черные списки – добавить – правило 1 – сохранить

Задание 5. Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.
Проверить работоспособность и зафиксировать выполнение скриншотом.
Заходим в Demolab – диск С – program.files – lible office – program – scalc (ярлык) – в папку share
Машина IWDM
Консоль управления – приложения - +правило 2 – сохранить
Приложения – правило 2 – загрузить приложение - \\Demolab\Share - выбираем calc - сохранить
Политики – создать – правило 2 – перехватчик: ScreenShot control monitor – если запущены приложения

Задание 6. Необходимо поставить на контроль буфер обмена в текстовых процессорах. Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.
Машина IWDM
Консоль управления – приложения - +правило 3 – сохранить
Правило 3 – загрузить приложения – prog.fails – windows nt – access ories – wordpad – открыть – сохранить
Политики – создать правило 3 – перехватчик:Clipbaad Monitor – убрать галочку: в приложение тер. сессии – поставить галочку: в приложениях кроме тер. сиссий – правило 3 – сохранить

Задание 7. Необходимо запретить печать на сетевых принтерах.
Зафиксировать создание политики скриншотом.
Машина IWDM
Политики – создать правило 4 – перехватчик: Device Monitor – тип устройства: сетевой принтер – использование запрещено – сохранить

Задание 8. Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.
Проверить работоспособность и зафиксировать выполнение скриншотом.
Машина IWDM
Политики – создать правило 5 – перехватчик: Device Monitor – тип устройства: съемное устройство хранения – только чтение – сохранить

Задание 9. С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.
Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.
Машина IWDM
Белые списки – добавить – тип: съемное устройство хранение – найти в интернете USB ключ флешки и ввести его – проверить – сохранить

Задание 10. Создать политику по блокировке копирования файлов формата zip на USB-накопители.
Проверить работоспособность и зафиксировать выполнение скриншотом.
Машина IWDM
Политики – создать правило 6 – перехватчик: File Monitor – маска файла: *.**zip** – разрешить копирование и создавать событие с теневыми копиями – убрать ∨ размер файла - сохранить

Задание 11. Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик.
Проверить работоспособность и зафиксировать выполнение скриншотом
Машина IWDM
Политики – создать правило 7 – перехватчик: Print Monitor –сохранить

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

Задание 12. Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Машина IWDM

Приложения - +новое правило – браузер – загрузить приложение – копируем путь браузера – сохранить

Политики - +правило 8 – перехватчик: ScreenShot Monitor – если активны приложения выбираем браузер – меняем время на 15 секунд – сохранить

Задание 13. Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Машина IWDM

Политики – создать правило 9 – перехватчик: Device Monitor – тип:CD/DVD – нет доступа – сохранить

Задание 14. Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода.

Зафиксировать скриншотами факт выдачи доступа и необходимые действия для выдачи доступа.

Машина IWDM

Инструменты – временный доступ сотрудника – далее – далее – учетная запись:user3 - тип устройства: CD/DVD – код устройства: 111 – время доступа: 30 минут – далее – готово

Сделать скриншот

Задание 15. На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Машина IWDM

Политики - +правило 10 – перехватчик: Application Monitor – запрет буфера обмена: в терминальной сессии между разными рабочими станциями – сохранить

Задание 16. Необходимо установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно).

Проверить работоспособность и зафиксировать выполнение скриншотом

Машина IWDM

Задачи - +новая задача – наименование: смена пароля – тип: задача смены пароля деинсталляции – далее – добавить: группа ПК по умолчанию (клиент) – далее – новый пароль ввести от 1 до 8 – далее – готово – смотрим статус

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

## Модуль D. Разработка и применение политик безопасности, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании

После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg

где CP – сокращение от англ. creating a policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

ВНИМАНИЕ!

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

ВНИМАНИЕ!

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Задание 1. Создайте локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей. Подтвердите выполнение задания скриншотами.

Машина IWDM - Браузер – вводим IP машины IWTM – officer xxXX1234

Персоны – пользовательские группы - + «сотрудники под наблюдением» - сохранить

Сотрудники под наблюдением - + (с правой стороны) - и создаем 3х любых пользователей

Задание 2. Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Списки – параметры – компания – почтовый домен – demo.lab – сохранить

Еще – веб-ресурсы – создать новый список – доверенные домены – сохранить

Доверенные домены – добавить – смотрим список в задании

Еще – параметры – исключить из перехвата ( сначала ищем посту генерального директора) – вводим почту – сохранить

Задание 3. Для недавно нанятого аудитора компании необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Области видимости: все.

Логин: auditor, пароль: 12345678 Подтвердите выполнение задания скриншотами.

Еще – управление доступом – создать пользователя – логин и пароль по заданию - сохранить

Роли – создать по заданию

Политика 4. В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

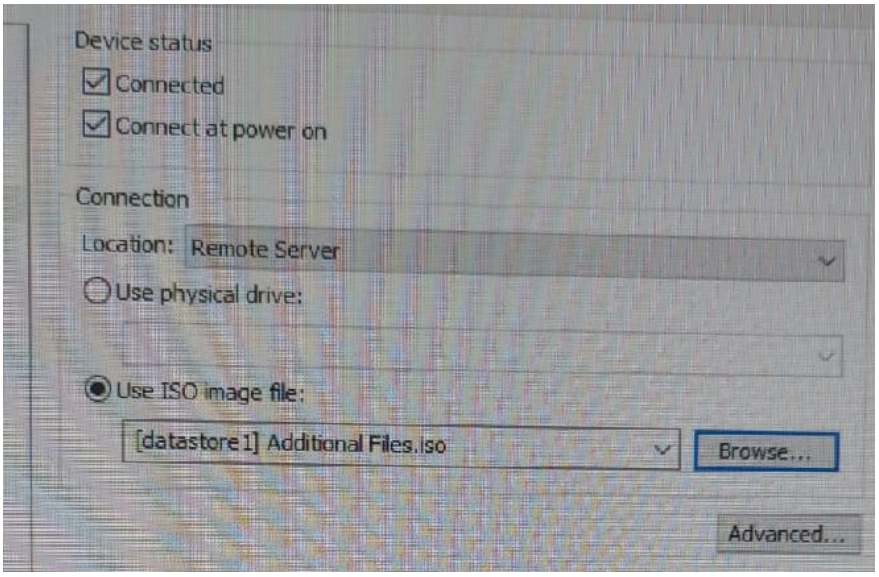
Уровень нарушения: средний •

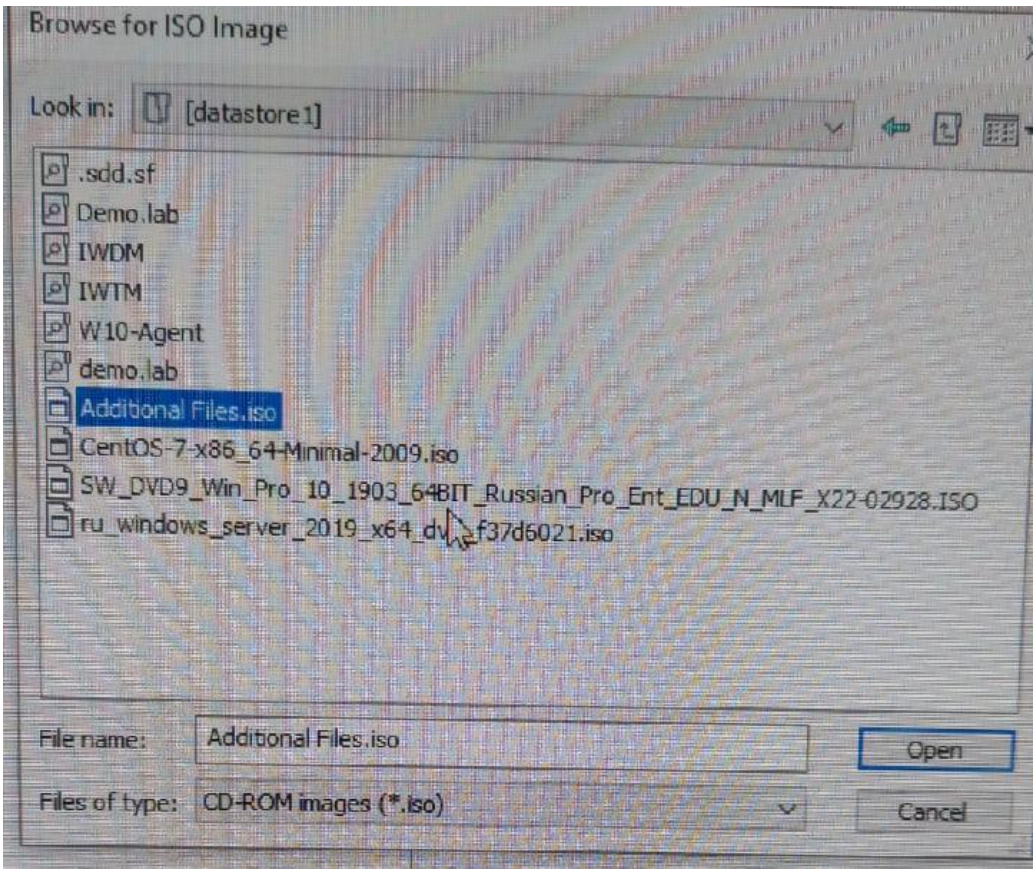
Тег: мобильники

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

Проверить работоспособность.
Тэги – добавить все тэги по всему оставшемуся заданию
Технологии – текстовые объекты – создать – политика 4 – сохранить
Политика 4 – редактировать – добавить шаблон – записываем фразу **([Ww]orld|[Вв]орлд)(\s+)?([Ss]kills|[Сс]килл[зс])** – сохранить
Объекты защиты – создать группу защиты – политики
Политики – создать – текстовые объекты - политика 4 – создать – название: объект защиты 4 – условие: политика 4
Еще – политики – добавить политику защиты данных - защищаемые данные – объекты защиты – объект защиты 4 – название: политика 4 – сохранить
Передача – добавить правило – в одну сторону – дальше настраиваем по заданию

Политика 5. Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%. Для пустого документа:
Вердикт: разрешить √
Уровень нарушения: нет
Тег: договор
Для заполненного документа:
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: договор
Проверить работоспособность.
Заходим в настройки виртуальной машины ( смотрим фото)






Технологии – эталонные документы – добавить - на основе текстовых данных – договор компании – редактирование – 2 ползунка на 50% - сохранить
Объекты защиты – политики – создаем новую – эталонные документы – выбираем документы – создать – название: для заполненного объекта 5.1 – условия: договор – создать
Еще – политики – добавить политику – политика защиты данных – защищаемые данные: для заполненного объекта 5.1 – название: политика 5.1 для заполненного документа
Передача – добавить правило – в одну сторону – остальное настраиваем по заданию
Технологии – бланк – добавить – название: для пустого документа – создать
Объект защиты – политики – добавить – бланки – для пустого документа - название: для пустого документа объект 5.2 – условие: для пустого документа
Еще – политики – добавить политику защиты данных – зачищаемые данные: для пустого документа - название: политика 5.2 для пустого документа – сохранить
Передача – добавить правило – в одну сторону – остальное по заданию настраиваем

Политика 6. Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.
Вердикт: запретить ×
Уровень нарушения: средний •
Тег: бланк
Проверить работоспособность.
Технологии – бланки – каталоги бланков – название: анкета – сохранить
Создать – выбираем анкету – сохранить

Объекты защиты – политики – добавить – бланки – анкета – название: политика 6 – условие: анкета участника
Политики – добавить политику защиты данных - название: политика 6 – защищаемые данные: политика 6
Передача – добавить правило – в одну сторону – остальное настраиваем по заданию

Политика 7. Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений. Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: печать
Проверить работоспособность.
Технологии – печати – создать – название: печать – создать
Печать – создать – выбираем печать из папки
Объекты защиты – политики – добавить печати – выбираем печать – создать – название: политика 7 – условия: печать
Еще – политики – создать политику защиты данных - название: политика 7 – защищаемые данные: политика 7
Передача – добавить правило – в одну сторону – отправители ≠по заданию выбираем людей и далее настраиваем по заданию

Политика 8. В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (10 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.
Передача кодов внутри компании:
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: коды
Передача кодов за пределы компании:
Вердикт: запретить ×
Уровень нарушения: средний •
Тег: бланк
Проверить работоспособность.
Технологии – текстовые объекты – добавить – название: коды компании – шаблоны - +10 штук (из файла промокоды) – сохранить
Объекты защиты – политики – добавить – текстовые документы – коды компании – условия: коды компании – название: политика 8
Еще – политика – добавить политику защиты данных – название: политика 8 – защищаемые данные: политика 8 – сохранить
В передаче создаем 2 правила по заданию
Передача кодов внутри компании – в обе стороны
Передача кодов за пределы компании – в одну сторону

Политика 9.

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания, планируется к внедрению в эксплуатацию. Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф. Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенноцифирными кодами на русском языке:
Р-Цифры-Буквы или РЦифрыБуква или Р-ЦифрыБуква
• Р – русская буква «Р»
• Цифры – не более 4-х подряд, например, 27 или 5000 (обязательно наличие хотя бы одной цифры)
• Буквы – от 1 до 2-х подряд, например, Р-27АЭ
Вердикт: запретить ×
Уровень нарушения: высокий •
Тег: ракеты
Проверить работоспособность.
Технологии – текстовые объекты – добавить – политика 9 – редактировать – добавить шаблон – регулярные выражения - [A-z]{3}-\.[А-ЯЁ]{1,2}
Объекты защиты – политики – добавить - текстовые объекты – политика 9 – создать – название: политика 9 – условия: политика 9 – создать
Политики – добавить политику защиты данных – название: политика 9 – защищаемые данные: политика 9 – сохранить
Передача – добавить правило – в одну сторону – получатели ≠ периметр: компания - остальное по заданию

Политика 10. Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации.
Вердикт: разрешить √
Уровень нарушения: средний •
Тег: база
Проверить работоспособность.
Технологии – выгрузка из БД - добавить – мониторинг выгрузок из БД – добавить файл – сохранить – редактировать – условия по умолчанию – редактирование – условия обнаружения:5+7+14+15+16+17+18 – сохранить
Объекты защиты – политики – добавить – выгрузка из БД – политика 10 – условия: выгрузка из БД – создать
Добавляем политику 10 – передача – в одну сторону – отправители: Users – IT – далее по заданию

Политика 11. В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси.
Вердикт: разрешить √
Уровень нарушения: средний •
Тег: подработка
Проверить работоспособность.

Разработчик: Алькова Мария Анатольевна, ОГБПОУ «Томский индустриальный техникум»

Технологии – категории и термины – создать – перевозки – далее добавляем все термины по заданию
Объекты защиты – политики – добавить – категории перевозки – создать - политика 11 – условия: перевозки
Добавляем политику – в передаче добавляем новое правило – в оба направления – остальное по заданию

Политика 12. Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» любым сотрудникам за пределы компании. Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции, а также писать название компании на русском языке, например, «ООО Demo Лаб», «ООО Демо Лаб».
Вердикт: запретить ×
Уровень нарушения: высокий •
Тег: печать
Проверить работоспособность.
Технологии – текстовые объекты – добавить – политика 12 – создать – редактировать – регулярные выражения ([\w\d-.+_])+@(demo|demolab|демо|демолаб)\.(org|su|ru|lab|рф)
Добавляем объект защиты
Добавляем политику – добавляем в передаче новое правило – получатели ≠ компания – остальное по заданию

Политика 13. В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: вирус
Проверить работоспособность
Технологии – категории и термины – добавить – ковид – добавляем все термины по заданию
Добавляем объект защиты
Добавляем политику – добавляем в передаче новое правило – отправитель = компания - все остальное по заданию

Политика 14. Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.
Вердикт: запретить ×
Уровень нарушения: высокий •
Тег: пдн
Проверить работоспособность.
Объект защиты – политики – добавить – политика 14 – элементы технологий: по заданию – условия выбрать все – создать
Добавляем политику - добавляем новое правило – в одну сторону – отправители ≠ HR

Политика 15. Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации. Стоит учесть, что файлы могут передаваться в том числе и на съемных носителях информации.
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: печать
Проверить работоспособность.
Добавляем политику – защищаемые данные: файловые форматы – таблица – конструкторская документация – сохранить
Передача – добавить правило – далее по заданию
Копирование – добавить правило – приемник копирования – тип: съемное устройство и все ≠ - далее все настраиваем по заданию

Задание 16. Анализ инцидентов, обычные сводки
Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:
Динамика активности по событиям за последнюю неделю
Статистика по политикам за последние 7 дней
По типу событий: необработанные нарушения за три дня
По топ-нарушителям за текущий месяц.
Сводка – добавить – экзамен – добавить виджет – добавляем по заданию ( топ нарушителей, подборка, динамика нарушений за период, статистика по политикам) Редактировать – настроить по заданию