Вариант № 2

Задание для демонстрационного экзамена по комплекту оценочной документации

|  |  |
| --- | --- |
| **Номер компетенции** | F7 |
| **Название компетенции** | Корпоративная защита от внутренних угроз информационной безопасности |
| **Номер КОД** | 1.1 |

# Описание задания.

Задание выполняется на подготовленных виртуальных машинах: контроллер домена с поднятым DNS и AD, чистая серверная система, чистая клиентская система (2 шт), предустановленный, но не настроенный DLP-сервер (с установленной лицензией).

В компании «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 электронная почта и различные интернет-ресурсы, если не указано иное.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса (и/или DNS сервер) нужно назначить согласно прилагаемой карточке. Подготовлены следующие виртуальные машины для дальнейшей работы:

* AD и DNS сервер (контроллер домена)
* DLP сервер установлен (но не настроен), активирована лицензия
* Виртуальная машина для установки сервера агентского мониторинга
* Виртуальные машины «нарушителей» (2 шт)

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

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными (проверить и исправить самостоятельно).

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

В случае отсутствия необходимых для выполнения задания данных, обратитесь к экспертам.

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание\_5\_копирование.jpg, все скриншоты и отчеты сохраняются на рабочий стол физического компьютера в один каталог или документ (важно соблюдать последовательность заданий) или передаются экспертам иным способом по запросу.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна. Не стоит вырезать только маленький кусочек (например, сообщение о событии), т. к. это не будет являться явным подтверждением работы. Допускается последующее выделение рамкой, стрелкой или иным способом результата работы.

# Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “DemoDept” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “DemoDept” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: iwtm-admin, пароль: xxXX2233, права пользователя домена

Логин: ldap-sync, пароль: xxXX2233, права пользователя домена

Логин: iwdm-root, пароль: xxXX2233, права администратора домена и локального администратора

Логин: user-pc, пароль xxXX2233, права пользователя домена

Логин: user-gp, пароль xxXX2233, права пользователя домена

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен. Необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случае несовпадений настроить DNS правильно.

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 ldap-sync.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-admin с полными правами офицера безопасности и 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» на рабочем столе компьютера.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя iwdm-root (важно).

После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “DemoDept” на домене.

Установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя xxXX2233.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: officer с паролем xxXX2233

Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие данные, измененные вами, в текстовом файле «отчет.txt» с на рабочем столе компьютера.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-pc.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-gp.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “DemoDept” на домене.

Установить агент мониторинга:

На машину 1 (user-pc) 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 и переноса любым способом пакета установки является некорректным выполнением задания.

На машину 2 (user-gp) с помощью групповых политик домена. Допускается как удаленная установка созданного вручную пакета, так и с помощью удаленной установки компонента Deploy Agent с последующей установкой через задачи сервера агентского мониторинга.

Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

В случае проблем при установке компонентов стоит проверить настройки брандмауэра и DNS.

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 с настройками по умолчанию.

Необходимо создать общий каталог MyShare в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

Зафиксировать выполнение задания скриншотом настройки и работоспособности в WEB-консоли.

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих термин «Демо экзамен» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «ДЭ».

Для отработки правил через сервер агентского мониторинга необходимо создавать правила в отдельной политике «Модуль 1». После отработки политик необходимо оставить политику и открепить ее от групп компьютеров или выключить правила, но не удалять.

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

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте 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 не более 1 года, длине ключа не менее 2048 бит и т. п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата

Дополнительная информация сертификатов должна включать в себя:

* Страна: RU
* Город: StPetersburg
* Компания (и иные дополнительные поля): demolab
* Отдел: Admins
* Почтовый адрес: из домена demo.lab
* Пароли ключей (если применимо): xxXX2233

Остальные поля заполняются самостоятельно.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли IWTM.

В случае невозможности это сделать, установить сертификат на машину домена и отобразить это в отчете.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе в каталоге «Сертификаты»

Содержимое команд по генерации ключей и сертификатов в текстовом файле «сертификаты.txt» на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании Demo.lab и т. п.

Изображение выглядит как текст

Автоматически созданное описание Изображение выглядит как текст

Автоматически созданное описание

Рис1. Пример скриншотов задания

# Описание модуля E: Технологии защиты узла и агентский мониторинг

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух и более 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 СP – сокращение от англ. сreating а 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: PW-1-2.jpg

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

Задание 1

Необходимо создать 2 новых группы компьютеров: «Департамент 1» и «Департамент 2», а также создать 2 новых политики: «Департамент 1» и «Департамент 2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 (user-pc) необходимо перенести в Департамент 1, а компьютер 2 (user-gp) — в Департамент 2.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на любую машину нарушителя для удаленного доступа к серверу агентского мониторинга. Необходимо хотя бы 1 раз подключиться с удаленной консоли.

Зафиксировать выполнение скриншотом (в заголовке окна консоли будет указан IP-адрес или DNS имя удаленного сервера).

Задание 3

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно). Пароль: xxXX2233

Проверить работоспособность и зафиксировать выполнение скриншотами.

Следующие правила создаются в политике «Департамент 1».

Правило 1

Запретить печать документов на сетевых принтерах. Также необходимо отдельным правилом разрешить печать на локальных принтерах.

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 2

Необходимо полностью запретить использование облачного сервиса GoogleDrive, разрешить полное использование сервиса DropBox, остальные сервисы настроить только в режиме чтения (разрешить скачивание).

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 3

Запретить запуск приложения calculator и mspaint.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 4

Необходимо запретить создание снимков экрана в текстовых процессорах (Word или Libre/Open Office Writer) для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 5

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. В случае отсутствия USB-накопителей создать правило на сетевые расположения.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 6

С учетом ранее созданной блокировки необходимо разрешить копирование только на один доверенный USB-накопитель с помощью белого списка. В случае отсутствия USB-накопителей создать исключение для любого другого конкретного устройства (кроме CD/DVD).

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 7

Полностью заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине). В случае отсутствия CD/DVD привода его необходимо создать.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 8

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD/DVD привода.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Необходимо зафиксировать основные шаги выдачи доступа (например ввод кода).

Следующие правила создаются в политике «Департамент 2».

Правило 9

Необходимо запретить доступ к буферу обмена в приложениях wordpad и firefox.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 10

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик IWTM.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами (обязательно с рабочим событием печати в веб-консоли).

Правило 11

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

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Для проверки работоспособности необходимо будет включить RDP доступ на любой из машин.

Правило 12

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера edge (или Internet explorer) путем создания снимков экрана каждые 90 секунд или при переходе в другое окно.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Также необходим скриншот сохраненных снимков экрана в системе.

Правило 13

Запретить передачу файлов документов типа MS Excel, Libre/Open Office Calc на съемные носители информации и в сетевые каталоги.

Проверить работоспособность любым из правил, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Групповые политики домена

Групповые применяются только на компьютер 2 (user-gp), должны быть созданы в домене, необходимо создать или 1 общий объект для всех политик и применить его к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю), или по 1 объекту на каждую политику и применить их к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю).

Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Использование компонентов DLP будет считаться некорректным выполнением задания.

Групповая политика 1

Настроить политику паролей и блокировки:

* Максимальный срок действия пароля: 30 дней
* Минимальная длина пароля: 6 символов
* Блокировка пользователя при неправильном вводе пароля: 5
* Блокировка учетной записи при вводе пароля: 20 минут

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений notepad++.exe, charmap.exe.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование командной строки и редактора реестра пользователем стандартной политикой запрета (не с помощью списка).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять изображение блокировки экрана.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Изменить изображение рабочего стола пользователя групповыми политиками с использованием SYSVOL или общего каталога в домене.

Изображение необходимо создать самостоятельно, должно содержать в себе название компании (Демолаб, demo.lab) текстом в картинке.

Изменение изображения вручную не будет считаться корректным выполнением задания.

Зафиксировать настройки политики и выполнение скриншотами.

# Описание модуля C: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

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

Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

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. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

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».

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

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.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, Политика 4, Политика 5, Политика 6, Политика 7, Политика 8, Политика 9, Политика 10, Политика 11, Политика 12

Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты. Стоит учесть, что стандартные политики и объекты можно модифицировать под свои нужды.

Задание 2

Создайте локальную группу пользователей «Подозрительные сотрудники» в Traffic Monitor. Добавьте в нее трех любых пользователей.

Задание 3

Создать список веб-ресурсов «Партнерские домены». Добавить в список следующие сайты: megademo.lab, act-demolab.ru, sysdem.lab.

Задание 4

Для работы системы необходимо настроить периметр компании:

* Почтовый домен: demo.lab.
* Список веб ресурсов «Партнерские домены» (созданный ранее).
* Группа персон: пользователи домена (все).
* Исключить из перехвата почту генерального директора.

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела бухгалтерии (Financial) отправлять документы, содержащие информацию о СНИЛС и паспортных данных (в текстовом и графическом виде) за пределы компании. Отдел бухгалтерии может отправлять файлы без ограничений. Можно использовать стандартные технологии и объекты.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 1

Политика 2

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа «Договор.docx» за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 35%.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

В связи с введением оплаты с помощью кредитных карт, необходимо запрещать передачу как текстовых, так и графических данных о кредитных картах за пределы компании для всех сотрудников, кроме отдела договоров (accounting). Политика может быть настроена с использованием стандартных технологий и объектов.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 3

Политика 4

Необходимо отслеживать любые документы, передающиеся за пределы компании и содержащие печать компании всем сотрудникам, кроме отдела продаж (Sales) и директора компании. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Политика 5

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID (внутри любой фразы), SARS (внутри любой фразы, например SARS-CoV-2), Коронавирус.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 5

Политика 6

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, для остальных контролировать не нужно.

Критичными данными в выгрузке являются телефоны, ИНН, ОКПО, ОКФС, ОКОГУ и ОКОПФ и в 1 документе присутствует 4 или более компаний. Для настройки используйте файл «Выгрузка из БД.csv».

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 6

Политика 7

Офицеру безопасности стало известно, что многих сотрудников не устраивает уровень заработной платы, поэтому планируется проведение несанкционированного мероприятия. Необходимо создать политику, которая позволит узнать точную дату и время проведения мероприятия.

Сообщение с датой можно найти по ключевым словам: «митинг», «пикет», «маленькая зарплата» Если в документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно работать на всех сотрудников, кроме совета директоров (BOD) и директора, которые могут отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 7

Политика 8

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 8%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 популярных на данный момент сериалов при передаче через веб-сообщения и почту.

Список сериалов:

«Игра в кальмара», «Бумажный дом», «Рик и Морти», «Очень странные дела», «Мир дикого запада».

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 8

Политика 9

Оказалось, что сотрудники не только обсуждают сериалы, а еще и обмениваются ссылками и torrent-файлами для их скачивания, после чего скачивают их, используя интернет-канал компании или обмениваются скачанным материалом внутри компании, что также нагружает сеть.

В связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов формата .torrent и ссылок формата magnet: (и содержащей urn (хеш) файла). Ложных срабатываний просто на слово Magnet (в т. ч. с двоеточием) быть не должно.

Вердикт: Заблокировать

Уровень нарушения: средний

Тег: Политика 9

Политика 10

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты доменов компании: demo и demolab, демо, демолаб.

Важно, чтобы в одном сообщении содержалось минимум 4 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org, lab. Детектирование только частей адресов (например @demo.ru) недопустимо. Пример формата адресов: e-mail@demolab.ru , mail+tag@demo.lab, elepochta@demo.org и т. п. Разрешенные спецсимволы в почте: \_ . - +

Вердикт: разрешить

Уровень нарушения: высокий

Тег: Политика 10

Политика 11

Сотрудники и партнеры компании стали получать много спама на телефоны, в связи с чем возникло подозрение о том, что кто-то производит «слив» номеров из баз данных компании путем передачи информации за пределы компании через браузер, почту или флешки. Необходимо контролировать передачу как минимум 3 номеров в сообщении, т.к. передача всего одного номера может быть контактной информацией.

Мобильные номера могут быть только операторов РФ (код страны 7, код оператора начинается с 9), в различных форматах, например:

+7 (987) 123-45-67, +79871234567, +7 987 123 4567, 8-987 123-4567 и т.д.

Необходимо учесть все варианты только для мобильных номеров, комбинации пробелов, скобок, дефисов.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 11

Политика 12

Необходимо контролировать передачу (веб, почта) любых зашифрованных архивов только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 12

# Описание модуля F: Предотвращение инцидентов и управление событиями информационной безопасности

Задание 1: Контроль доступа

Необходимо создать пользователя DLP системы с правами просмотра и выполнения сводок, отчетов и событий. Прав на редактирование (изменение) быть не должно.

Пользователь: infouser, пароль: xxXX2233

Задание 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка» под названием «ДЭ» и «Выборка»

Задание 3: Виджеты

При создании выборок для сводок необходимо помещать их в каталог выборок «ДЭ»

Создайте в сводке «ДЭ» 4 виджета:

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

Задание 4

Необходимо создать виджет в разделе «Сводка», вкладка «Выборка», отображающий события с уровнем угрозы от низкого до среднего на правила передачи и работы в приложениях (буфера) за последние 3 дня.

Зафиксировать скриншотом конструктора выборки.

Задание 5

Необходимо создать виджет в разделе «Сводка», вкладка «Выборка» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) с низким и высоким уровнем угрозы за последние 30 дней.

# Необходимые приложения

Приложение 1: Карточка настроек сети и оборудования (docx)

Приложение 2: Шаблоны документов для задания (zip)