

Образец задания

Образец задания для демонстрационного экзамена по комплекту оценочной документации.

Описание задания

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.

Политики трафика могут быть проверены вручную или с помощью генератора событий, предоставляемым по запросу.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены (кроме адреса DNS сервера на машинах).

Перед экзаменом должны быть подготовлены следующие виртуальные машины для работы (рекомендуется сделать нулевой Snapshot для быстрой подготовки к другим потокам), сеть настроена в режиме NAT (сеть NAT) или Bridge с DHCP, с доступом в интернет, но без доступа к машинам других участников экзамена:

- AD и DNS сервер (контроллер домена), 1,5ГБ ОЗУ и выше, 2 ядра, статическая адресация с доступом в интернет,
- DLP сервер установлен (но не настроен), активирована лицензия, 6ГБ ОЗУ и выше, 2 ядра,
- Виртуальная машина для установки сервера агентского мониторинга, 2ГБ ОЗУ и выше, 2 ядра,
- Виртуальные машины «нарушителей» (2 шт), 1,5ГБ ОЗУ и выше, 2 ядра.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов (demo.lab, должен быть развернут из эталонного, получить эталон можно по запросу).

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными. При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах.

Все дистрибутивы должны находиться в каталоге, указанном в карточке задания. Все логины, пароли, сетевые настройки и прочее, относящееся к инфраструктуре площадки, должно быть указано в карточке задания.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна.

Описание модуля 1:

Задание 1: Настройка контроллера домена

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

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

Логин: user1, пароль: ххХХ1234, права пользователя домена

Логин: user2, пароль: ххХХ1234, права пользователя домена

Логин: admin1, пароль: ххХХ1234, права администратора домена

Логин: user3, пароль: ххХХ1234, права пользователя домена

Логин: user4, пароль: ххХХ1234, права пользователя домена

Задание 2: Настройка DLP сервера

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

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя user4.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена user3 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 admin1 (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Test” на домене.

Установить базу данных PostgreSQL или аналог или функциональный аналог с паролем суперпользователя ххХХ1234.

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 токenu, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: officer с паролем ххХХ1234

Синхронизировать каталог пользователей и компьютеров с Active Directory или функциональным аналогом.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя admin1, 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.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user2.

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

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена.

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

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию.

Необходимо создать общий каталог Test 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).

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 некий термин, установить уровень угрозы для всех событий, добавить тег.

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

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, 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 должны удовлетворять общепринятым на сегодня стандартам и требованиям, 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

Поля сертификата заполняются по вариантам заданий.

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 DLP-системы уровня сети.

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. Содержимое команд по генерации ключей и сертификатов в текстовом файле 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»).

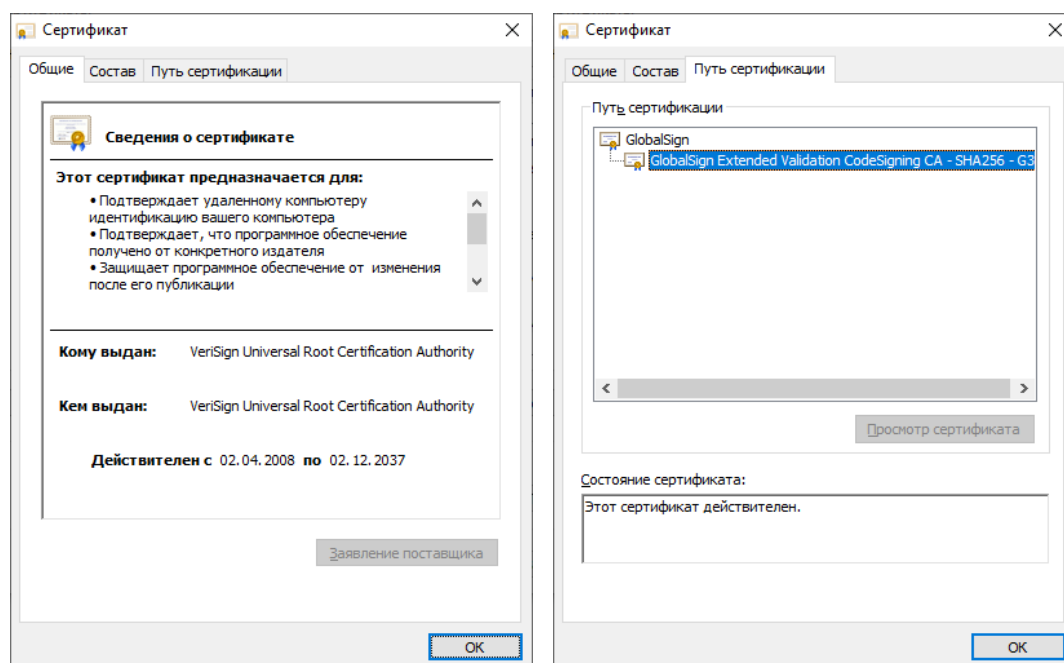


Рис1. Пример скриншотов задания

Описание модуля 2:

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).

Задание 1

Необходимо создать 2 новых группы компьютеров: «Test1» и «Test2», а также создать 2 новых политики: «Test1» и «Test2». Каждая из политик должна

применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Test1, а компьютер 2 — в Test2.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Test1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint или аналог, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам).

Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства не определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++. Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

Правило 12

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Групповые политики домена

Групповые применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля, Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Настроить дополнительные параметры системы, которые должны применяться для пользователя или компьютера (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Описание модуля 3:

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 заблокировать) 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.

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, ...

Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

Задание 2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задание 3

Создать список веб-ресурсов. Добавить в список следующие сайты: Site.ru, domain.com, ...

Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен, список веб ресурсов, группа персон, исключить из перехвата.

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела (по вариантам) отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел (по вариантам) может отправлять файлы без ограничений.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 1

Политика 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах определенного уровня.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика.

Вердикт: заблокировать

Уровень нарушения: низкий

Тег: Политика 3

Политика 4

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела (по вариантам) и определенного сотрудника. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Политика 5

В последнее время возникла необходимость обработки текстовых данных, а также сканов и фото кредитных карт. Необходимо отслеживать передачу всех возможных данных кредитных карт (в том числе сканов) за пределы компании.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 5

Политика 6

Сотрудники 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 определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются определенные поля и в 1 документе присутствует более 1 строчки. Для настройки используйте файл примера.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 6

Политика 7

Некая компания попросила обеспечить защиту от утечки важных данных. Необходимо создать политику на контроль правила передачи содержащие слова «один», «два», «три» в 1 сообщении или документе одновременно. Если в документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме определенного отдела, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 7

Политика 8

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 8

Политика 9

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов, например формата.mp4 и ссылок определенного формата (содержит уникальную последовательность, например urlname). Ложных срабатываний 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.

Важно, чтобы в одном сообщении содержалось минимум 2 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org и прочие. Детектирование только частей адресов (например @mail.ru) недопустимо.

Вердикт: разрешить

Уровень нарушения: высокий

Тег: Политика 10

Политика 11

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых стандартизированных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что отдел так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассылать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизированные форматы паролей (кириллица):

6 букв – 1 знак !?#\$%^/_& – 2-4 цифры – 4 буквы – 2-3 знака !?#\$%^/_&
(например, ПаРоль#67pКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 11

Политика 12

Необходимо контролировать передачу определенных типов файлов только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 12

Описание модуля 4:

Задание 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Задание 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка»

Задание 3: Виджеты

Создайте в сводке 4 виджета:

1. Выборка по событиям за период
2. Выборка по политикам с технологиями за период

Проверить доступность незащищённых машин друг другу любым другим протоколом; проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

- Настройка максимального количества туннелей на координаторах
- Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла
- Скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования

Необходимые приложения

Приложение 1: Пояснения по сбору площадки (документ pdf)

Приложение 2: Шаблоны документов для задания (архив zip)