ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОМСКИЙ ТЕХНИКУМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Примерное задание на комплексный квалификационный экзамен по профессиональным модулям специальности

09.02.06 Сетевое и системное администрирование

(Квалификация – Сетевой и системный администратор)

Томск 2022

ОБЩИЕ ПОЛОЖЕНИЯ

В качестве итоговой аттестации по каждому профессиональному модулю после завершения обучения проводится экзамен (квалификационный), на котором представители учебного заведения и работодателей проверяют готовность обучающегося к выполнению соответствующего вида профессиональной деятельности и сформированность у него профессиональных (ПК) и общих компетенций (ОК).

Экзамен (квалификационный) проводится после изучения всех МДК модуля, прохождения учебной и производственной практики.

Для проведения процедуры квалификационного экзамена создается экзаменационная комиссия, в которую входят представители образовательного учреждения (преподаватели, представители администрации) и представители работодателей.

Экзамен (квалификационный) проводится в соответствии с графиком экзаменов и на основании приказа директора образовательного учреждения.

ПРИМЕРНОЕ ЗАДАНИЕ

Содержание практического задания по модулям:

Модуль 1: Установка и конфигурирование компонентов DLP системы.

Модуль 2: Технологии агентского мониторинга.

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов.

Продолжительность экзамена 180 минут.

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).
Подготовлены следующие виртуальные машины для работы (рекомендуется сделать нулевой Snapshot), сеть настроена в режиме NAT, с доступом в интернет, но без доступа к машинам других участников экзамена:

- Demo.lab. AD и DNS сервер (контроллер домена), 1,5ГБ ОЗУ, 2 ядра, статическая адресация с доступом в интернет,
- IWTM. DLP сервер установлен (но не настроен), активирована лицензия,
  8ГБ ОЗУ, 2 ядра,
- IWDM. Виртуальная машина для установки сервера агентского мониторинга, 2ГБ ОЗУ, 2 ядра,
- W10-Agent. Виртуальная машина «нарушителя» (1 шт), 1,5ГБ ОЗУ, 1 ядро.

В компании развернут домен со всеми сотрудниками с указанием ФИО,
должности и контактов (demo.lab)

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 находятся в каталоге, указанном в карточке задания. Все логины, пароли, сетевые настройки и прочее, относящееся к инфраструктуре площадки, указаны в карточке задания.

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

Описание модуля 1:

Айпишник втм 172.16.1.4/25
Шлюз 172.16.1.1
Днс 172.16.1.2
ПОСТАВИТЬ MANUAL

Задание 1: Настройка контроллера домена

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

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

Логин: user, пароль: xxXX1234, права пользователя домена
Логин: iw-admin, пароль: xxXX1234, права администратора домена
Логин: iwtm-officer, пароль: xxXX1234, права пользователя домена
Логин: ldap-sync, пароль: xxXX1234, права пользователя домена
Добавила компы в подразделение

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.
ВОШЛА ЧЕРЕЗ IW-ADMIN
ЛДАП
DEMO.LAB
172.16.1.2
DC=DEMO, DC=LAB
LDAP-SYNC
xxXX1234

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-officer ДОБАВИЛА В ПОЛЬЗОВАТЕЛЕЙ ЛДАП с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.
ДОБАВИЛА РОЛИ

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 iw-admin (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “QualExam” на домене.

Установить базу данных PostgreSQL с паролем суперпользователя xxXX1234.

Установить сервер агентского мониторинга с параметрами по умолчанию,

В КРАВЛЕРЕ СНАЧАЛО НУЖНО ОТКРЫТЬ ПОРТЫ 6556 И 1337 ЧЕРЕЗ БРАУНДМЕР

ПОМЕНЯТЬ /ETC/HOSTS ДОБАВИТ IWDM

В NANO /OPT/IW/TM5/ETC/WEB.CONF ПОМЕНЯТЬ ЗНАЧЕНИЕ В 1
подключившись к ранее созданной БД. НЕ ПОДКЛЮЧАЛОСЬ ПО АЙПИ ПОДКЛЧИЛОСЬ С IWTM (НА ЦЕНТОСЕ АКТИВАЦИЮ ПОДЕРГАТЬ)

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 xxXX1234
УСТАНОВИЛА ДШВАЙС МОНИТОР
LOCALHOST
POSTGRESS
POSTGRES
xxXX1234

Синхронизировать каталог пользователей и компьютеров с Active Directory.

ИНТЕГРАЦИЯ НАСТРОЙКИ ДОМЕН ВВОДИТЬ ВЫБРАТЬ ВСЕ КАТАЛОГИ И СОХРАНИТЬ

После синхронизации настроить беспарольный вход в консоль управления ===
от ранее созданного доменного пользователя iw-admin, 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 в домен, после перезагрузки войти в систему от ранее созданного пользователя user.

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

Установить агент мониторинга:

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

Необходимо делать снимки экрана для подтверждения создания и выполнения политик.

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

В МАСТЕРЕ СОЗДАНИЯ ЗАДАЧИ ДОБАВИТЬ 1 И 2 КОМП

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 Share в корне диска сервера IWDM 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).

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 новую группу компьютеров: «Отдел1», а также создать новую политику «Экзамен». Политика должна применяться на компьютер нарушителя

Зафиксировать выполнение скриншотом. Делать в монитьоре

Задание 2

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

Следующие правила создаются в политике «Отдел1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint, 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 облачным хранилищам GoogleDrive и YandexDisk.

Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Групповые политики домена

Групповые политики 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 - 192 дня, Минимальная длина пароля - 8, пароль должен отвечать требованиям сложности, Блокировка учетной записи при повторном вводе неверного пароля (3 раза), продолжительность блокировки 15 минут.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку: PowerShell, ножницы, сведения о системе.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование панели управления стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять обои рабочего стола.

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 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.

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 «Удалёнка» и добавьте в нее 3 пользователей.

Задание 3

Создать список веб-ресурсов. Добавить в список следующие сайты: rt.ru, infotecs.ru, dnevnik.ru\.

Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен компании, список веб-ресурсов, группа персон «Удалёнка», 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 кадров отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел кадров 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 договора за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела бухгалтерии и генерального директора. Они могут обмениваться документами внутри и за пределами компании без контроля. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 3

Политика 4

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 телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД и ОКОПФ и в 1 документе присутствует более 5 компаний. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 4

Политика 5

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

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

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 5

Политика 6

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 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#67рКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 6