Модуль 5: Технологии агентского мониторинга

Задания выполняются с помощью компонентов DLP системы InfoWatch.

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 «Политика 1-2» и т. д.

Для некоторых политик могут понадобиться дополнительные файлы, которые находятся в общей папке из дополнительной карточки задания.

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 на рабочем столе RDP машины в папке «Модуль 5».

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:
PW-1-2.jpg

где PW – сокращение от англ. policy work,

1 – номер задания;

2 – номер скриншота для задания 1.

Модуль 5: Технологии агентского мониторинга

Задание 1

Необходимо установить (сменить) пароль для удаления Device Monitor Agent всех виртуальных машин нарушителей с помощью средств DeviceMonitor Server (удаленно). Пароль: xxXX1234
Проверить работоспособность и зафиксировать успешное выполнение задачи скриншотом

Задание 2

Необходимо создать новую политику (кроме политики на устройства по умолчанию), назвав ее «Чемпионат», применить ее к группе компьютеров по умолчанию.
Последующие правила по заданиям должны быть добавлены в эту политику.
Зафиксировать выполнение скриншотом.

Задание 3

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления IWDM на компьютер с базой данных для удаленного доступа к серверу IWDM.
Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли на хост-машине.

Задание 4

Для удаленного управления необходимо создать дополнительного офицера безопасности для доступа к IWDM с полными правами на управление.
Для этого необходимо использовать ранее созданного пользователя **dbadmin** для организации входа в консоль без пароля от текущей учетной записи.
Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 5

Необходимо запретить пользоваться Microsoft Paint и стандартным приложением Таблица символов (charmap).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо запретить создание снимков экрана в табличных процессорах (Libre Office calc или MS Office Excel) и калькуляторе Windows (при наличии) для предотвращения утечки секретных расчетов и баз данных.
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 7

Необходимо поставить на контроль буфер обмена в стандартном текстовом процессоре WordPad, а также текстовом редакторе notepad++.
Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики Traffic Monitor.
Также подтвердить выполнение скриншотом.

Задание 8

Необходимо поставить на контроль копирования данных до 5 Мб на USB-накопители и сетевые папки.
Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики Traffic Monitor.
Также подтвердить выполнение скриншотом.

Задание 9

Создать политику по блокировке копирования исполняемых exe-файлов на USB-накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов), копирования всех файлов кроме exe.
Проверить работоспособность и зафиксировать выполнение скриншотом.
Необходим скриншот создания политики и скриншот события-запрета.

Задание 10

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

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.

Задание 12

Заблокируйте доступ к CD/DVD, MTP-устройствам и дискетам на клиентском компьютере (виртуальной машине).
Зафиксировать выполнение скриншотом.

Задание 13

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода.
В случае отсутствия CD привода обеспечить доступ к любому другому устройству (например USB носителю).
Зафиксировать скриншотами факт выдачи доступа и необходимые действия в IWDM.

Задание 14

Необходимо поставить на контроль печать документов на принтерах.
Продемонстрировать работоспособность на любую из политик IWTM с помощью виртуального принтера.
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 15

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера Google Chrome путем создания снимков экрана каждые 30 секунд или при смене окна.
Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в консоли IWTM. Подтвердить выполнение задания скриншотами.

Проверить работоспособность и зафиксировать выполнение скриншотом

Задание 16

На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.
Проверить работоспособность попыткой копирования чего-либо из RDP сессии внутри сети и зафиксировать выполнение скриншотом события блокировки.