

Лабораторная работа №1

«Создание политики информационной безопасности в IWTM 6»

Цель работы – разработать политику информационной безопасности, используя инструментарий автоматизированной системы IWTM 6, а также, по средствам имитации процесса утечки конфиденциальной информации, протестировать процесс перехвата системой, в соответствии с объектами защиты разработанной политики ИБ.

1. Содержание технологических этапов выполнения работы.

1. Ознакомиться со структурой виртуальной среды, используемой для выполнения лабораторного практикума (3 виртуальные машины: сервер IWTM 6; сервер IWDM; рабочая станция «Нарушитель»).

2. Изучить предоставляемые материалы, используемые при создании политики ИБ в системе IWTM 6: концепция политики ИБ PCI DSS; файл MS Excel с базой данных (см. приложение).

3. В консоли IWTM 6 создать объекты защиты и политику ИБ, используя технологии анализа, обозначенные в политике PCI DSS (см. приложение).

4. Провести проверку агента, установленного на рабочей станции «нарушитель», на предмет соединения с сервером DM.

5. В консоли DM провести проверку соединения сервера IWTM 6 с сервером IWDM, а также актуальность последней версии конфигурации IWTM 6.

6. Провести имитацию процесса утечки конфиденциальной информации с рабочей станции «Нарушитель».

7. В консоли IWTM 6 и IWDM получить отчет о факте утечки конфиденциальной информации и продемонстрировать его тренеру.

2. Контрольные вопросы.

1. Каналы передачи данных: определение и виды.
2. Какие разделы системы IW TM используются для администрирования системы?
3. Какие разделы системы IW TM используются офицером безопасности в повседневной работе?
4. Перечислите особенности технологии «Лингвистический анализ», используемой в системе IW TM.
5. Какие каналы передачи информации контролирует IW TM?
6. Перечислите технологии анализа корпоративного трафика, используемые в IW TM.
7. Перечислите виды и особенности баз контентной фильтрации, используемые в системе IW TM.
8. Общая информация. Как запросить\ загрузить лицензию?
9. Какие сетевые устройства могут быть использованы как источники событий для анализа?
10. Как сконфигурировать систему, чтобы она получала теневые копии от Device Monitor?

Концепция настройки политик в InfoWatch Traffic Monitor 6 для «ОАО Банк»

1. Концепция

Настоящий документ содержит правила реагирования Системы на перехваченные объекты, в зависимости от принадлежности объекта к одной из категорий защищаемых данных. К защищаемым данным могут относиться:

- Термины (слова или их сочетаний);
- Тестовые объекты (регулярные выражений) определённого формата;
- Эталонные документы (цифровые отпечатки документов фиксированной структуры)
- Эталонные выгрузки из баз данных (цифровые отпечатки эталонных выгрузок – определённые столбцы или их сочетания)

В рамках текущего этапа внедрения необходимо реализовать детектирование фактов передачи за периметр Компании следующих категорий документов:

1. Строго конфиденциальная информация;
2. Конфиденциальная информация;
3. PCI DSS;
4. Персональные данные;

В таблице ниже описаны правила реагирования Системы на вышеуказанные категории информации, включая:

- Правила передачи – пересылка объекта, содержащего определённую политикой информацию по любому из контролируемых каналов;
- Правила копирования – копирование объекта, содержащего определённую политикой информацию на съемное устройство;
- Правила хранения – размещение объекта, содержащего определённую политикой информацию на рабочей станции пользователя/ разделяемом сетевом ресурсе.
- Правила буфера обмена – копирование объекта, содержащего определённую политикой информацию из одного приложения в другое.
- Правила защиты данных на агенте при передаче – пересылка объекта, содержащего определённую политикой информацию по любому из контролируемых каналов;
- Правила защиты данных на агенте при копировании - копирование объекта, содержащего определённую политикой информацию на съемное устройство;

2. Политики защиты данных (в соответствии со стандартом PCI DSS)

Название политики	Правила реагирования	Пояснение
1. PCI DSS	<ul style="list-style-type: none"> • Категории <ul style="list-style-type: none"> ◦ PCI DSS: CVV, криптопериод, ключи шифрования • Текстовый объект <ul style="list-style-type: none"> ◦ Номер кредитной карты • Эталонные документы <ul style="list-style-type: none"> ◦ Выгрузка из БД с данными держателей карт <p>1.1. Правило передачи 1:</p> <ul style="list-style-type: none"> • Каналы: все • Отправители – любой отправитель, получатели – любой получатель, кроме «Внутренний периметр» 	<p>1.1. При отправке сообщения, содержащего в теле объекта или вложении информацию категории PCI DSS на внешний адрес, в консоли Traffic Monitor появится событие с высоким уровнем угрозы.</p> <p>1.2. При отправке сообщения, содержащего в теле объекта или вложении информацию категории PCI DSS на внешний адрес «@sentinelcredit.ru», в консоли Traffic Monitor</p>

	<ul style="list-style-type: none"> • Уровень угрозы – высокий <p>1.2. Правило передачи 2:</p> <ul style="list-style-type: none"> • Канал: Исходящая почта • Отправители – любой отправитель, получатели – @sentinelcredit.ru • Уровень угрозы – средний <p>1.3. Правило передачи 3:</p> <ul style="list-style-type: none"> • Каналы: все • Отправители – «группа e-business», получатели – любой внутренний получатель, кроме «группа e-business»; • Уровень угрозы - низкий <p>1.4. Правило копирования:</p> <ul style="list-style-type: none"> • Уровень угрозы – высокий <p>1.5. Правило хранения:</p> <ul style="list-style-type: none"> • Любой сотрудник, кроме «группа e-business» • Уровень угрозы – средний <p>1.6. Правило буфера обмена</p> <ul style="list-style-type: none"> • Уровень угрозы – высокий • Назначить событию теги: Подозреваемый <p>1.7. Правило защиты данных на агенте при передаче</p> <ul style="list-style-type: none"> • Каналы: Все • Отправители – «группа e-business», получатели - @enemy.com • Назначить событию вердикт: Заблокировать • Уровень угрозы: Высокий • Назначить инициатору статус: Под наблюдением 	<p>появится событие со средним уровнем угрозы.</p> <p>1.3. При отправке сотрудником, входящим в группу Процессинга сообщения, содержащего в теле объекта или вложении информацию категории PCI DSS любому получателю, кроме сотрудников группы Процессинга, в консоли Traffic Monitor появится событие со средним уровнем угрозы.</p> <p>1.4. При копировании на съемный носитель файла, содержащего информацию категории PCI DSS, в консоли Traffic Monitor появится событие с высоким уровнем угрозы.</p> <p>1.5. При обнаружении файлов, содержащих информацию категории PCI DSS на рабочих станциях сотрудников, не входящих в группу Процессинга, в консоли Traffic Monitor появится событие со средним уровнем угрозы.</p>
--	--	--

База данных предоставляется дополнительным файлом MS Excel