Конкурсное задание

Компетенция

«Корпоративная защита от внутренних угроз информационной безопасности»

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Модули задания и необходимое время
4. Критерии оценки

Количество часов на выполнение задания: 18ч.

Утверждаю
Сергеев Антон Валерьевич
(Ф.И.О. менеджера компетенции)

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются применение на практике систем корпоративной защиты от внутренних угроз. Участники соревнований получают описание модели организации, включая описание её организационной структуры, информации, циркулирующей внутри периметра безопасности, информационной инфраструктуры, каналов связи, видов трафика, списков пользователей.

Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Конкурс включает исследование организации с целью защиты от внутренних угроз, настройку и проверку специализированного программного обеспечения, разработку и применение политик информационной безопасности, контроль информационных потоков, анализ выявленных инцидентов и подготовку отчётов.

Окончательные аспекты критериев оценки уточняются членами жюри. Оценка производится как в отношении работы модулей, так и в отношении процесса выполнения конкурсной работы. Если участник конкурса не выполняет требования техники безопасности, конфликтен, не владеет техниками управления стрессом и разрешения конфликтных ситуаций, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри.

Конкурсное задание должно выполняться помодульно. Оценка также происходит от модуля к модулю.

Если участник закончил выполнение модуля досрочно, он должен расписаться в ведомости времени напротив соответствующей информационной записи «Участник №__ закончил выполнение модуля __».

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время сведены в таблице 1

Таблица 1.

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Модуль 1: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	С1 10.00-14.00	3 часа
2	Модуль 2: Исследование (аудит) организации с целью защиты от внутренних угроз.	С1 15.00-18.00	3 часа
3	Модуль 3: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	С2 10.00-13.00	3 часа
4	Модуль 4: Технологии защиты и анализа сетевого трафика	С2 14.00-17.00	5 часов
5	Модуль 5: Технологии агентского мониторинга	С3 10.00-11.00 С3 11.30-12.30	2 часа
6	Модуль 6: Анализ выявленных инцидентов	С3 13.30-15.30	2 часа
	Итого		18 часов

Модуль 1: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Участник должен:

- Провести конфигурацию сетевой инфраструктуры: настроить хост-машину, сетевое окружение, виртуальные машины, и т.п.;
- Установить и настроить систему корпоративной защиты от внутренних угроз;

- Запустить систему, проверить функциональность и соответствие настроек целевой сетевой инфраструктуре
- Провести имитацию процесса утечки конфиденциальной информации в системе;
- Устранить проблемы при появлении;
- Продемонстрировать работоспособность системы
- Подготовить отчёт по оценке работоспособности системы;

Модуль 2: Исследование (аудит) организации с целью защиты от внутренних угроз.

Участник должен провести обследование и анализ структуры организации (как главного объекта защиты) на основании представленных материалов и стенда, её вычислительно-сетевой инфраструктуры, определить потоки данных, потенциальные угрозы и каналы утечек.

Участнику необходимо создать пакет документации, включающий

- список потенциальных внутренних угроз (согласно выданного шаблона)
- список возможных каналов связи для анализа (согласно выданного шаблона)
- проект положения о защите информации от внутренних угроз (согласно выданного шаблона)
- список ролей пользователей и потенциальных нарушителей
- список изменений в существующие внутренние нормативных документы (положения, приказы и т.п.) организации для эффективного и законного использования современных систем защиты.

Участник готовит отчёт, суммирующий итоги исследования организации. По окончании проверки участник ставит подпись в отчёте и сообщает о готовности экспертам. Эксперт фиксирует время готовности в отчёте. Проверку отчёта проводит назначенная группа экспертов.

Модуль 2 считается выполненным при условии подписанного отчета, устного доклада участника об окончании работ.

Модуль 3: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.

Цель участника – разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6 и успешно их применить для

выявления и/или блокирования инцидентов безопасности. Для создания инцидентов и других событий в IWTM используется специальное программное обеспечение – специальный Генератор трафика и инцидентов.

Участнику необходимо:

- Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;
- Занести политики информационной безопасности в DLP-систему;
- Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.;
- Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором трафика и инцидентов. Максимизировать число выявленных инцидентов безопасности;
- Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы корпоративной защиты информации IWTM.

Участнику необходимо применить политики информационной безопасности в системе IWTM, автоматически выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда и Генератора трафика и инцидентов). Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. Необходимо использовать весь набор технологий поиска и выявления уязвимостей, доступный в системе корпоративной защиты. Итоговый вариант политик должен быть зафиксированы в отчете.

В число инцидентов могут входить, например:

- передача персональных данных сотрудников и контрагентов по электронной почте;
- передача базы клиентов организации в архиве с использованием файловых протоколов;
- нецензурная лексика сотрудников в переписке с контрагентами;
- передача информации, составляющей коммерческую тайну и др.

Задание выполняется с помощью программного обеспечения DLP (Data Leaks Prevention) IWTM 6.

Примерный алгоритм выполнения на примере инцидентов и политик PCI DSS:

1. Запустить систему IWTM,

2. Ознакомиться со структурой виртуальной среды, используемой для выполнения лабораторного практикума (3 виртуальные машины: сервер IWTM 6; сервер IWDM; рабочая станция «Нарушитель»),
3. Проверить функциональность и соответствие настроек целевой сетевой инфраструктуре
4. Изучить предоставляемые материалы, используемые при создании политики ИБ в системе IWTM 6: концепция политики ИБ PCI DSS;
5. В консоли IWTM 6 создать объекты защиты и политику ИБ, используя технологии анализа, обозначенные в политике PCI DSS.
6. Провести проверку агента, установленного на рабочей станции «нарушитель», на предмет соединения с сервером DM.
7. В консоли DM провести проверку соединения сервера IWTM 6 с сервером IWDM, а также актуальность последней версии конфигурации IWTM 6.
8. Провести имитацию процесса утечки конфиденциальной информации:
    a. Вручную с рабочей станции «Нарушитель»
    b. Автоматически с Генератора инцидентов
9. В консоли IWTM 6 и/или IWDM автоматически получить информацию о факте утечки конфиденциальной информации. Инцидент должен быть автоматически выявлен и помечен как уязвимость соответствующего уровня согласно задания.

Модуль 4: Технологии анализа и защиты сетевого трафика.

Участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.
- Администрирование узлов и пользователей.
- Выполнение компрометации узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации.
- Организацию межсетевого взаимодействия и туннелированния.
- Внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

Участник выполняет следующие действия с использованием IDS-систем корпоративного класса:

- Развёртывание, настройка и проверка работоспособности IDS-системы на существующей и вычислительной инфраструктуре.
- Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий.

- Разработка и применение различных механизмов и технологий анализа трафика.
- Детектирование атак и угроз, проведение расследования инцидента

VPN и IDS системы могут применяться в рамках одного модуля как совместно, по отдельности или поодиночке.

Модуль 5: Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика в системе корпоративной защиты информации от внутренних угроз

Участнику необходимо применить политики информационной безопасности в системе IWTM/IWDM, автоматически выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда и Генератора трафика и инцидентов) .

- Продемонстрировать знание механизмов работы агентского мониторинга;
- Разработать и применить политики агентского мониторинга для работы с носителями и устройствами;
- Разработать и применить политики агентского мониторинга для работы с файлами;
- Работа с исключениями из перехвата;

Модуль 6: Анализ выявленных инцидентов

Задача участника – использовать аналитический функционал системы IWTM6 для создания отчётов о найденных инцидентах и анализа полученных данных.

Участник должен:

- Применить механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
- Подготовить детализированные отчёты о нарушениях;
- Провести классификацию уровня угрозы инцидента;
- Использовать дополнительных модули анализа информационных потоков, если это продиктовано особенностями модели организации и условиями её бизнеса;
- Разработать план по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу;

- Подготовить итоговый отчёт.

4. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 100.

Таблица 2.

Раздел	**Критерий**	**Оценки**		
		Мнение судей	**Объективная**	**Общая**
A	Организация работы и управление		5,00	5,00
B	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз		14,00	14,00
C	Исследование (аудит) организации с целью защиты от внутренних угроз	5,00	6,00	11,00
D	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз		20,00	20,00
E	Технологии анализа и защиты сетевого трафика		27,00	27,00

F	Технологии агентского мониторинга		14,00	14,00
G	Анализ выявленных инцидентов		8,00	8,00
	Итого =	100		100

Субъективные оценки - Не применимо.