**Конкурсное задание**

**Компетенция**

**«Корпоративная защита от внутренних угроз информационной безопасности»**

Конкурсное задание включает в себя следующие разделы:

1. Введение
2. Формы участия в конкурсе
3. Задание для конкурса
4. Модули задания и необходимое время
5. Критерии оценки
6. Необходимые приложения

Количество часов на выполнение задания: 20ч.

## ВВЕДЕНИЕ

1.1. Название и описание профессиональной компетенции.

1.1.1 Название профессиональной компетенции: Корпоративная защита от внутренних угроз информационной безопасности.

1.1.2. Описание профессиональной компетенции.

Специалисты по защите корпоративной информации от внутренних угроз обеспечивают защиту конфиденциальных данных организации от утечек, вызванных неправомерными действиями сотрудников (т.н. инсайдеров), совершенными как целенаправленно, так и вследствие проявленной халатности или невнимательности. Работа специалиста по корпоративной защите от внутренних угроз включает сборку, установку, тестирование и использование обслуживание специализированных программно-аппаратных комплексов по перехвату и анализу трафика данных, циркулирующего в организации (т.н. DLP-систем). На основе данных об организации и информации о её информационно-телекоммуникационной инфраструктуре он должен разрабатывать политики информационной безопасности, классифицировать объекты защиты, понимать аспекты применения нормативно-правовой базы для классификации и расследования инцидентов. Ему необходимо в совершенстве владеть современными DLP-системами и технологиями для применения политик информационной безопасности на практике, для перекрытия возможных каналы утечки данных и выявления инцидентов безопасности. Он обязан обладать аналитическими навыками, уметь использования механизмы фильтрации для выявления инцидентов в перехваченном трафика с целью выявления нарушений корпоративной безопасности.

1.2. Область применения

1.2.1. Каждый Эксперт и Участник обязан ознакомиться с данным Конкурсным заданием.

1.3. Сопроводительная документация

1.3.1. Поскольку данное Конкурсное задание содержит лишь информацию, относящуюся к соответствующей профессиональной компетенции, его необходимо использовать совместно со следующими документами:

• «WorldSkills Russia», Техническое описание. Электромонтажные работы;

• «WorldSkills Russia», Правила проведения чемпионата

• Принимающая сторона – Правила техники безопасности и санитарные нормы.

## 2. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

## 3. 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.

## 4. 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: Исследование (аудит) организации с целью защиты от внутренних угроз. | С1 11.00-13.00С1 14.00-18.00 | 2 часа4 часа |
| 2 | Модуль 2: Разработка политик информационной безопасности. | С2 09.00-13.00С2 14.00-18.00C3 09.00-13.00 | 4 часа4 часа4 часа |
| 3 | Модуль 3: Настройка и тестирование системы защиты от внутренних угроз  | С3 15.00-17.00 | 2 часа |
| 4 | Модуль 4: Контроль информационных потоков и применение политик | С3 17.00-18.00 | 1 час |
| 5 | Модуль 5: Анализ выявленных инцидентов |  |  |

**Модуль 1: 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. В случае, если отчёт не принят экспертной группой, участник может исправить ошибки воспользовавшись "второй попыткой" в рамках времени конкурсного задания. Время, затраченное экспертами на проверку отчёта, должно быть возмещено участнику.

**Модуль 2: Разработка политик информационной безопасности.**

Цель участника – разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6, а также, по средствам имитации процесса утечки конфиденциальной информации, протестировать факт перехвата системой, в соответствии с объектами защиты разработанной политики ИБ, удостовериться что перехват работает.

Участнику необходимо:

- Разработать политики безопасности;

- Занести политики информационной безопасности в DLP-систему

- Представить созданные политики в виде отчёта

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

Модуль 1 и Модуль 2 считаются выполненными при условии подписанного отчета, устного доклада участника об окончании работ и наличии занесённых политик безопасности в DLP-систему.

**Модуль 3: Настройка и тестирование системы защиты от внутренних угроз**

Участник должен:

- Запустить систему, проверить функциональность и соответствие настроек целевой сетевой инфраструктуре

- Провести имитацию процесса утечки конфиденциальной информации в системе;

- Устранить проблемы при появлении;

- Подготовить отчёт по оценке работоспособности системы;

Примерный алгоритм выполнения:

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 с рабочей станции «Нарушитель».
9. В консоли IWTM 6 и IWDM получить отчет о факте утечки конфиденциальной информации и
10. Оформить отчёт согласно шаблона и продемонстрировать его экспертам.

**Модуль 4: Контроль информационных потоков и применение политик.**

Участнику необходимо применить политики информационной безопасности в системе IWTM, выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда), отметив найденные инциденты их в отчете. Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. 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.

**Модуль 5: Анализ выявленных инцидентов**

Задача участник – использовать аналитический функционал и фильтры системы IWTM6 для детализированного поиска инцидентов безопасности и работы с ними.

Участник должен:

- Применить механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;

- Провести классификацию уровня угрозы инцидента;

- Использовать базы контентной фильтрации;

- Использовать дополнительных модули анализа информационных потоков, если это продиктовано особенностями модели организации и условиями её бизнеса;

- Подготовить итоговый отчёт.

Модули 4 и Модуль 5 считаются выполненными при условии подписанного отчета (согласно шаблона), а также устного доклада участника об окончании работ.

## 5. 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** |
| **Объективная** | **Общая** |
| А | Организация работы и управление | 5 | 5 |
| В | Коммуникация и общение | 10 | 10 |
| С | Исследование объекта защиты и нормативная проработка | 20 | 20 |
| D | Эффективность политик безопасности | 20 | 20 |
| E | Навыки практической работы с DLP-системой | 20 | 20 |
| F | Общая эффективность защиты | 25 | 25 |
| Итого =  | 100 | 100 |

**Субъективные оценки -** Не применимо.