

**Конкурсное задание**

Компетенция «Кибербезопасность»

Типовое задание Вузовской линейки чемпионатов

Конкурсное задание включает в себя следующие разделы:

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

Разработано:

Сверчков Евгений Евгеньевич

1. **ФОРМЫ УЧАСТИЯ В КОНКУРСЕ**

Индивидуальный конкурс.

1. **ОБЩЕЕ ВРЕМЯ НА ВЫПОЛНЕНИЕ ЗАДАНИЯ**

Количество часов на выполнение задания: 10 ч.

1. **ЗАДАНИЕ ДЛЯ КОНКУРСА**

Содержанием конкурсного задания являются анализ и обеспечение защищенности информационных систем, целостности данных, расследование происшествий (инцидентов) и их предотвращение в будущем. Конкурсанты получают инструкции и необходимые для работы вводные файлы, а также доступ к сетевым ресурсам.

Конкурсное задание состоит из двух модулей, выполняемых и оцениваемых последовательно, вне зависимости от результатов выполнения предыдущего. Конкурс включает в себя поиск уязвимостей предоставленных операционных систем, серверов и программ; анализ защищенности, проектирование и создание безопасной конфигурации информационной системы; расследование инцидентов; документирование, формирование отчетов и рекомендаций. Результат работы оценивается как по полученному результату, так и на основании формального отчета с указанием результатов исследований, рекомендаций, хода работ и т.п. Отдельно оценивается этика информационной безопасности и аккуратность в ходе работы на виртуальной машине.

1. **МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ**

Модули и время сведены в таблице 1

Таблица 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование модуля | Рабочий день | Рабочее время | Время на задание |
| 1 | Модуль С. Восстановление ИТ-инфраструктуры после инцидентов ИБ  | С1 | 10.00-13.00 | 3 часа |
| 2 | Модуль А. Защита корпоративной ИТ-инфраструктуры | С1 | 14.00-16.00 | 2 часа |
| 3 | Модуль B. Расследование инцидентов информационной безопасности | С2 | 10.00-13.0014.00-16.00 | 3 часа2 часа |

Модуль A: Защита корпоративной ИТ-инфраструктуры

Вы работаете в новом офисе крупной компании ООО «F8», где возглавляете отдел обеспечения информационной безопасности. После вступления в должность вам необходимо обеспечить защиту инфраструктуры корректно настроев действующее приобретенное компанией программное обеспечение должным образом для повышения уровня информационной безопасности:

* В качестве защиты периметра применить NGFW, включив и настроив необходимые функции обеспечения ИБ на нем.
* В качестве сетевого коммутатора предлагается использовать виртуальную машину на RouterOS, с проведением необходимых настоек для обеспечения безопасности локальной сети.
* Компания будет иметь ряд публичных сервисов, опубликованных через NGFW.
* Провести сегментацию пользователей ЛВС.
* Ограничить доступ до ресурсов внешней сети согласно выданному ТЗ.
* Повысить уровень защищенности периметра ЛВС, демилитаризованной зоны, публичных сервисов компании.
* Предпринять меры по повышению уровня ИБ рабочих станций (компьютеров) сотрудников компании.
* С помощью NGFW повысить эффективность использования рабочего времени сотрудниками компании, в зависимости от функциональных обязанностей.
* Настроить оборудование компании согласно ТЗ

**ВХОДНЫЕ ДАННЫЕ**

Образы, ТЗ.

**ВЫХОДНЫЕ ДАННЫЕ**

Отчет в папке DAY\_1 в файле report\_day1 с данными, указанными в доп. задании, результат автоматизированной системы.

Модуль B: Расследование инцидентов информационной безопасности

Вас пригласили в компанию ООО «F8» для проведения аудита компании с целью поиска возможных уязвимостей в действующем программном обеспечении и сервисах используемыми компанией. Ваша работа будет осуществляется в формате Red Team – вам разрешены попытки получить доступ к системе любыми способами, включающими в себя тестирование на проникновение; тестирование линий связи, беспроводных и радиочастотных систем; тестирование сотрудников посредством сценариев социальной инженерии.

Вам будет предоставлена вводная информация о компании. Необходимо провести анализ и дать описание происходящего (будет указано в доп. задании) а также рекомендации к устранению выявленных инцидентов.

**ВХОДНЫЕ ДАННЫЕ**

Вводная информация.

**ВЫХОДНЫЕ ДАННЫЕ**

Отчет в папке DAY\_2 в файле report\_day2 с данными, указанными в доп. задании, результат автоматизированной системы.

# Модуль C: Восстановление ИТ-инфраструктуры после инцидентов ИБ

На один из филиалов Вашей организации была совершена кибер-атака. Вас направили для расследования инцидента и восстановления структуры и работоспособности сети, и системы филиала, а также составления отчета о киберпреступлении.

**ВХОДНЫЕ ДАННЫЕ**

Удаленный доступ до виртуальной структуры филиала, ТЗ.

**ВЫХОДНЫЕ ДАННЫЕ**

Отчет в папке DAY\_3 в файле report\_day3 с данными, указанными в доп. задании, восстановленная инфраструктура филиала(сеть, системы, сервисы), результат автоматизированной системы.

1. **Критерии оценки**

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

Таблица 2.

|  |  |  |
| --- | --- | --- |
| КРИТЕРИИ | МОДУЛИ | ИТОГО: |
| A | B | C |
| M | J | M | J | M | J |
| 1 | Защита корпоративной ИТ-инфраструктуры | 33 | 4 |  |  |  |  | 37 |
| 2 | Расследование инцидентов информационной безопасности |  |  | 36,5 | 1,5 |  |  | 38 |
| 3 | Восстановление ИТ инфраструктуры после инцидента ИБ |  |  |  |  | 22 | 3 | 25 |
| ИТОГО: | 33 | 4 | 36,5 | 1,5 | 22 | 3 | 100 |
| 37 | 38 | 25 |