КОНКУРСНОЕ ЗАДАНИЕ
для регионального чемпионата
чемпионатный цикл 2021-2022г
компетенции
«Кибербезопасность»
Основной возрастной категории
от 16 до 22 лет

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

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Командная – в составе команды 2 участника. Знания, умения и навыки необходимые для участников команды: знание операционных систем, знание компьютерных сетей, знание языков программирования, умение понимать исходные коды программ и логику построения компьютерных сетей, знание уязвимостей на уровне сетей, систем и приложений, умение находить и эксплуатировать найденные уязвимости, умение исправлять найденные или предложенные уязвимости.

2. ОБЩЕЕ ВРЕМЯ НА ВЫПОЛНЕНИЕ ЗАДАНИЯ

Количество часов на выполнение задания: 16 ч.

3. 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.

4. 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 А. Защита корпоративной ИТ-инфраструктуры	С1	09.30-13.30 14.30-17.30	3 часа 3 часа
2	Модуль В. Расследование инцидентов информационной безопасности	С2	09.30-13.30 14.30-17.30	3 часа 3 часа
3	Модуль С. Восстановление ИТ-инфраструктуры после инцидентов ИБ	С3	09.30-13.30	4 часа

Модуль А: 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 современный актуальный фаервол, включив и настроив необходимые функции обеспечения ИБ на нем, а также настрои правила Active Directory (AD).
- Компания будет иметь ряд публичных сервисов, опубликованных через фаервол.
- 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 фаервола 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. Вам будут выданы дампы инцидентов и разрешены попытки получить доступ к системе любыми способами, включающими в себя тестирование на проникновение; тестирование линий связи, беспроводных и радиочастотных систем.

Вам будет предоставлена вводная информация о компании. Необходимо провести анализ и дать описание, 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.

5. 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.

<table>
<tr><td colspan="2" rowspan="3">КРИТЕРИИ</td><td colspan="6">МОДУЛИ</td><td rowspan="3">ИТОГО:</td></tr>
<tr><td colspan="2">A</td><td colspan="2">B</td><td colspan="2">C</td></tr>
<tr><td>M</td><td>J</td><td>M</td><td>J</td><td>M</td><td>J</td></tr>
<tr><td>1</td><td>Защита корпоративной ИТ-инфраструктуры</td><td>33</td><td>4</td><td></td><td></td><td></td><td></td><td>37</td></tr>
<tr><td>2</td><td>Расследование инцидентов информационной безопасности</td><td></td><td></td><td>36,5</td><td>1,5</td><td></td><td></td><td>38</td></tr>
<tr><td>3</td><td>Восстановление ИТ инфраструктуры после инцидента ИБ</td><td></td><td></td><td></td><td></td><td>22</td><td>3</td><td>25</td></tr>
<tr><td colspan="2" rowspan="2">ИТОГО:</td><td>33</td><td>4</td><td>36,5</td><td>1,5</td><td>22</td><td>3</td><td rowspan="2">100</td></tr>
<tr><td colspan="2">37</td><td colspan="2">38</td><td colspan="2">25</td></tr>
</table>