Согласовано

ООО НПП «Гарант-Уфа»

Дмитриченко Александр

Викторович  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Региональный этап чемпионата по

профессиональному мастерству «Профессионалы» и

чемпионата высоких технологий Республики

Башкортостан

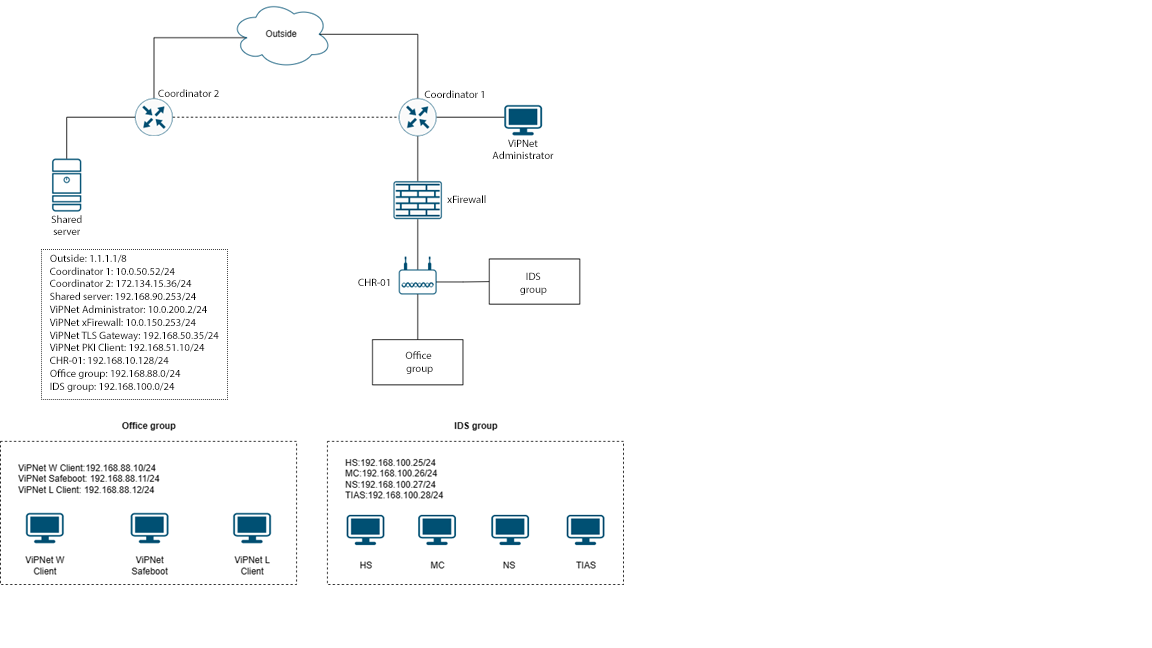
*по компетенции:*

F8 «Информационная безопасность»

Конкурсное задание

День 1

**Модуль А. Защита корпоративной ИТ-инфраструктуры**

****

ООО «ИБ» - является IT компанией, имеющая основной филиал в г. Уфа, Россия и удаленный сервер в собственном центре обеспечения данных в г. Санкт-Петербург, Россия. Группа работников офисной сети должна иметь доступ к удаленному серверу по сетевому протоколу уровня, позволяющий производить удаленное управление операционной системой (SSH) по порту 10022. Для доступа к серверу необходимо установить защищенное VPN соединение между двумя филиалами, используя семейство шлюзов безопасности ViPNet Coordinator.

|  |
| --- |
| *Для реализации интернет-соединения разрешается использовать одноранговое соединение, имитирующее простое интернет-соединение* |

Для организации защищенной инфраструктуры предприятия в условиях импортозамещения на базе программно-аппаратных комплексов необходимо оборудовать рабочее место администратора сетевой инфраструктуры.

В комплексе ЦУС и УКЦ, Вам необходимо сформировать защищенную сеть предприятия, создать объекты, роли и пользователей для всей инфраструктуры, а также выпустить все необходимые справочники и ключи для активации лицензионных ограничений для необходимых программно-аппаратных комплексов.

При настройке ЦУС и УКЦ, также необходимо ввести в эксплуатацию сервер базы данных для дальнейшего взаимодействия с программно-аппаратным комплексом ViPNet Administration.

Для обеспечения возможности подключения сотрудников офисной группы к защищенной сети удаленного сервера их устройства должны иметь программное обеспечение для защиты сетевого трафика на рабочих местах ViPNet Client. Помимо этого, на устройстве начальника офисной группы необходимо установить программное обеспечение доверенной загрузки операционной системы для избегания возможности загрузки вредоносного кода в UEFI.

Компания дорожит целостностью и конфиденциальностью данных, для этого необходимо внедрение программно-аппаратной группы оборудования для обнаружения вторжений в информационные системы ViPNet IDS и ViPNet TIAS. Для обеспечения реагирования на вторжения необходимо установить и настроить сенсоры IDS HS и IDS NS и центр управления и мониторинга IDS MC. Для обеспечения корректной работы сенсорного оборудования необходимо установить последнее обновление баз правил и сигнатур вредоносного ПО. Для эффективной работы всей группы IDS необходимо настроить рабочую инфраструктуру и ее взаимодействие с сенсорами IDS.

Для разграничения сетевого трафика среди сотрудников компании, необходимо внедрить межсетевой экран нового поколения (NGFW) ViPNet xFirewall. Компания дорожит эффективностью рабочего процесса и считает недопустимым доступ к следующему контенту:

URL: vk.com, ok.ru, facebook.com, instagram.com, youtube.com, rutube.ru, tik-tok.com

Software: Skype, Microsoft Teams, Torrent-клиенты

При реализации внутренней офисной сети компания временно не готова отказаться от использования оборудования на базе RouterOS, но видит явную необходимость в повышении его защищенности. Для этого необходимо запретить все доступы к интерфейсу кроме локального и по защищенному протоколу удаленного доступа, с использованием порта 2022.

Для удобства будущей эксплуатации руководство предлагает использовать протоколы прикладного уровня для автоматического назначения IP-адресов всем подключаемым устройствам. Помимо этого, так же предлагает разрешить доступ к веб-интерфейсам ключевых объектов, обеспечивающих защищенность инфраструктуры по протоколам прикладного уровня следующих портов: 80, 8080, 443. Также для доступа к объектам рекомендуется использоваться сложные пароли, которые не входят в словарь паролей rockyou.txt. Критически важные устройства должны иметь дополнительные учетные записи отличные от стандартных.

Для обеспечения максимальной отказоустойчивости рекомендуется выполнять резервные копирования всех ключевых устройств компании.

Отчет (формат .docx, название REPORT\_DAY1\_ TEAM №\_команды) о проделанной работе должен содержать подробную инструкции по внедрению и настройке предоставленного оборудования, а также должен содержать в себе всю необходимую информацию для доступа к инфраструктуре.

|  |  |
| --- | --- |
| **ВМ** | **Доступ** |
| HS | admin:admin |
| NS | idsuser:vipnet |
| MC | root: |
| TIAS | admin:admin |
| Shared | user:user |

Для реализации технического задания Вам предоставлен максимальный уровень допуска.

Подготовить отчет о проделанной работе

Согласовано

ООО НПП «Гарант-Уфа»

Дмитриченко Александр

Викторович  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Региональный этап чемпионата по

профессиональному мастерству «Профессионалы» и

чемпионата высоких технологий Республики

Башкортостан

*по компетенции:*

F8 «Информационная безопасность»

Конкурсное задание

День 2

**Модуль Б. Расследование инцидентов информационной безопасности**

*Время на выполнение модуля* 3 часа.

**Задания:** Вас пригласили в компанию ООО «ИБ» для проведения расследования инцидентов информационной безопасности.

Вам будет предоставлен набор заданий (тасков), к которым требуется найти и отправить ответ. Ответ даётся в виде флага, состоящего из набора символов или произвольной фразы. За верное выполнение каждого задания команда получает очки. Чем сложнее таск, тем больше очков даётся за правильный ответ. Задания будут выданы в формате Task-Based, по следующим возможным категориям: задачи на нахождение веб-уязвимостей (web), поиск и эксплуатацию уязвимостей в приложениях (PWN), исследование программ без исходного кода (reverse), расследование инцидентов (forensic), администрирование (admin), криптографию (crypto), стеганографию (stegano), поиск информации из открытых источников (OSINT).

Задача – решить максимальное количество инцидентов (тасков), подготовить отчет по каждому решению.

**Модуль В. Аудит информационной системы**

*Время на выполнение модуля* 3 часа.

**Задания:** Вас пригласили в компанию ООО «ИБ» 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 до-ступ 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 найденной уязвимости, а также рекомендации к устранению выявленных инцидентов.

Согласовано

ООО НПП «Гарант-Уфа»

Дмитриченко Александр

Викторович  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Региональный этап чемпионата по

профессиональному мастерству «Профессионалы» и

чемпионата высоких технологий Республики

Башкортостан

*по компетенции:*

F8 «Информационная безопасность»

Конкурсное задание

День 3

**Модуль Г. Проактивный анализ**

*Время на выполнение модуля* 4 часа.

**Задания:** Вас пригласили в компанию ООО «ИБ» для проведения проактивного анализа инцидентов информационной безопасности. На один из филиалов организации была совершена кибер-атака.

Вас направили для расследования инцидента и восстановления инфра-структуры и работоспособности сети и системы филиала, восстановление картины инцидента, рекомендаций, а также составления отчета о кибер-преступлении.

Задача – провести анализ произошедшей атаки, подготовить отчет о проделанной работе.