

**ЗАДАНИЕ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА**

|  |  |
| --- | --- |
| **Код комплекта оценочной документации** | КОД 1.1-2023 |
| **Номер варианта задания** | 1 |

**ОПИСАНИЕ ЗАДАНИЯ**

**Описание модуля 1**: **«****Защита корпоративной ИТ-инфраструктуры»**

Вы приняты на работу в компанию «ООО F8» техником по защите информации. Руководитель отдела ИБ делегировал Вам полномочия на развертывании сетевой инфраструктуры, повышения безопасности внутри нее, а также разграничения прав в демилитаризированной зоне (DMZ) на сетевом оборудовании.

IT отдел предоставили Вам на данный момент схему сети компании (Приложение 1) с ее основными элементам. Вам необходимо установить виртуальные машины и реализовать средства защиты (Приложение 2), а так же установить особые параметрам защищенной сети. В Вашем распоряжении имеются все необходимые образы для выполнения задания.

Также стоит учитывать, при настройке конфигурации сетей в ESXi категорический запрещены одноранговые сети.

Так же необходимо произвести установку и настройку сетевого сенсора системы обнаружения атак NS, MC, и программно-аппаратный комплекс TIAS, HS Server и Agent в соответствии с топологией, предоставленной в приложении 2.

Во время работы следует соблюдать правила цифровой гигиены:

* "пароль" должен соответствовать требованиям к сложности: не менее 8 символов, разного регистра, наличие специальных символов и минимум одной цифры, получившийся пароль не должен содержаться в словаре rockyou.txt;
* по завершении рабочего времени запрещается выключать физические или виртуальные машины и/или оставлять их в свободном доступе;
* по завершении работы (обед, перерыв, выход, конец рабочего дня) необходимо соблюдать порядок на рабочем месте).

Стоит обратить внимание на резервирование в среде виртуализации и сохранение резервных копий конфигурации в следующих машинах: MC, TIAS, NS. Обеспечен вход в данные машины под альтернативной учетной записью, отличной от предустановленного. Настроить механизм преобразования адресов для внутренней сети во внешнюю сеть.

В виртуальной среде ESXi в качестве виртуального коммутатора между сетями используется Router OS. Для эффективного использования ресурсов компании ВМ должны иметь следующие характеристики:

* оперативная память – 512 Мб;
* процессор – 1 потока.

При настройке Router OS стоит учитывать пожелания руководителя отдела безопасности о полном локальном управлении, но оставить доступ по защищенной оболочке по 5459. Добавленные подсети должны соответствовать Приложению 2.

На виртуальной машине «AD1» настроить компонент Active Directory с доменом «cyber-info.local», также ввести в домен виртуальную машину «AD2» как второстепенный контроллер домена. В этой ВМ должны быть установлены такие же компоненты, что и на «AD1».

При настройке DNS нужно настроить перенаправление запросов DNS, не относящихся к зоне «cyber-info.local», на внешний DNS сервер, которым выступает виртуальная машина «M2». В дополнение сконфигурировать зону обратного просмотра на «AD1». Главное руководство желает увидеть настроенный DHCP сервер.

Виртуальная машина WIN-01 должна находится в домене, в отчете вы должны указать все учетные данные, которые есть в домене и которые Вы использовали для входа.

Так же в желания заказчика входит настройка сетевых папок с разграничением доступа исходя из должности сотрудника. Сетевые папки должны быть расположены по пути: C:\Share\, все папки скрыты от посторонних, кроме all\_share. На эту папку также необходимо настроить политику аудита для все пользователей домена, сама политика должна включать фиксацию действий удаления файлов, папок и подпапок. С картой разграничения доступа к сетевым ресурсам можно ознакомится в таблице 1.

*Таблица 1. Карта разграничения доступа к сетевым ресурсам*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Доступ  Название  папки | Everyone | Buhg | HR | Sysadmin | Progr | VIP | Domain Admins | |
| All\_share | чтение/запись | чтение/запись | чтение/запись | чтение/запись | чтение/запись | чтение/запись | | Полный доступ | |
| Buhg | - | чтение/запись | - |  | - |  | | Полный доступ | |
| HR | - |  | чтение/запись |  | - |  | | Полный доступ | |
| Sysadmin | - |  |  | чтение/запись |  |  | | Полный доступ | |
| Progr | - |  | - | - | чтение/запись |  | | Полный доступ | |
| VIP | - |  |  |  |  | чтение/запись | | Полный доступ | |

Для большей безопасности заказчик попросил настроить на корневом домене следующие политики безопасности с конкретными требованиями к ним:

1. Название политики «mimikatz»: отключен компонент debug, отключен протокол WDigest, защита LSA от подключения сторонний модулей, отключение LM и NTLM протоколов аутентификации, запрет на использование сохраненный паролей, запрет на кэштрование учетный данных.
2. Название политики «Default Domain Controller Policy»: включить отслеживание события аудита доменных групп, включить аудит сетевых папок, включить аудит файловой системы.
3. Название политики «audit\_services\_cmd\_posh»: включить командную строку в события создания процессов, включить ведение журнала и модулей powershell.

Виртуальная машина AD2 будет является HS Server, на WIN-03 будет установлен агент. Для установки HS Server нужно включить компонент telnet и разрешить подключения по портам 25000-25001. Вам необходимо активировать лицензию и загрузить базы правил с использованием консоли управления на HS Server. База правил расположена на виртуальной машине «AD1». Виртуальная машина WIN-03 должна находится в группе «Главная». Необходимо на HS Server настроить автоподключение агентов.

Интегрируйте в сеть ВМ NS согласно приложению 2, настройте управляющий интерфейс, настройте интерфейс захвата, выгрузите и установите сертификат, установите временную зону по Москве, создайте администратора и пользователя, загрузите базы правил и базы сигнатур вредоносного программного на NS и включите сохранение вредоносного ПО.

Интегрируйте в сеть ВМ MC согласно приложению 2, подключить HS Server и NS к MC, создайте на этой машине домен «cyber-info».

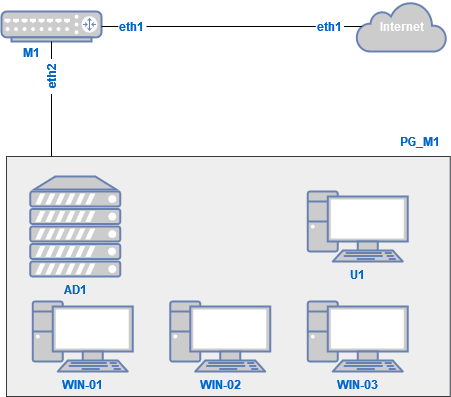
Интегрируйте в сеть ВМ TIAS согласно приложению 2, подключите вм NS и HS к TIAS. Создайте филиал «Москва» и добавьте туда сенсор HS.

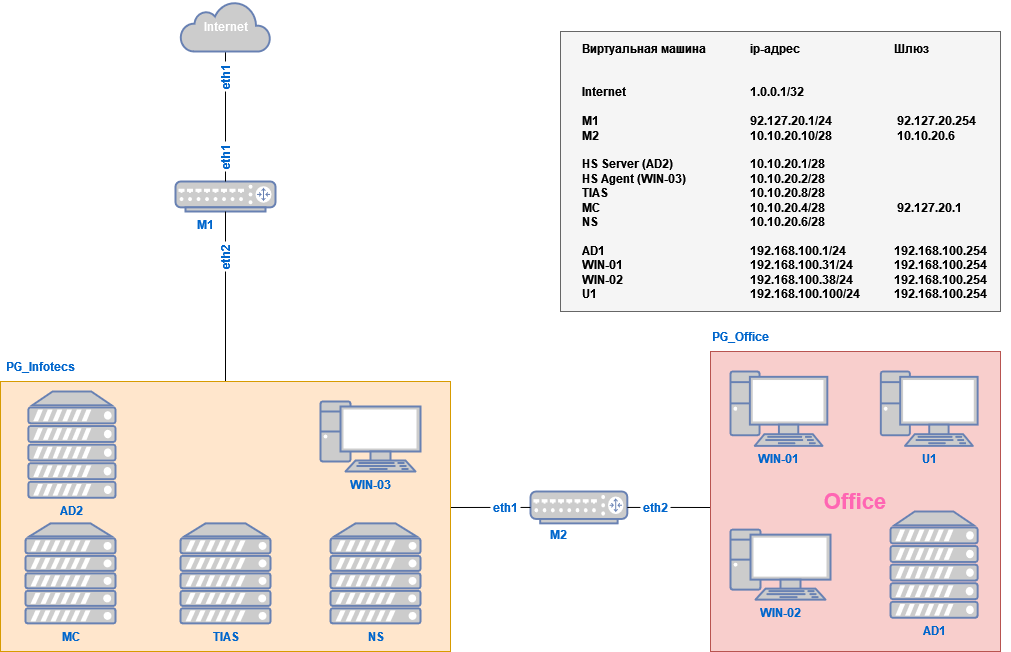
На ВМ U1 установлен файловый сервер vsftpd. Вам предстоит настроить его и обеспечить полный безопасный доступ по sftp, также настроить внутренние средства межсетевого взаимодействия. Установить удаленный доступ по ssh на 10022 порт, отключить авторизацию от суперпользователя и настроить подключения с локальной подсети, отключение авторизации по паролю.

По завершении работы необходимо подготовить отчет о проделанной работе в файле «REPORT\_MODULE\_A\_TEAM[НОМЕР РАБОЧЕГО МЕСТА]» в формате pdf (экспорт файла производить через печать). Отчет необходимо сохранить на рабочем столе рабочей машины.

*Таблица 2. Логины и пароли для установки на виртуальные мышины*

|  |  |  |
| --- | --- | --- |
| Виртуальная машина | Пользователь | Пароль |
| AD1 | Administrator | xxXX.1234 |
| AD2 | Администратор | xxXX.1234 |
| U1 | wsr | xxXX.1234 |
| HS Server | admin | admin |
| NS | idsuser | vipnetvipnet45 |
| NS | admin | vipnetvipnet45 |
| MC | Admin | vipnetvipnet45 |
| TIAS | admin | Vipnetvipnet45! |
| TIAS | Administrator | Administrator |





**При выполнении модуля 1 ставятся следующие цели:**

1. Повысить уровень защиты инфраструктуры

**При выполнении данного модуля 1 ставятся следующие задачи:**

1. Собрать инфраструктуру виртуальной сети
2. Внедрить средства защиты
3. Настроить виртуальное оборудование согласно задания.

**Требования к оформлению письменных материалов**

При оформлении отчета следует учесть необходимость наличия титульной страницы, оглавления (созданного автоматическим путем), соблюдение отступов, наличие заголовков, а , также отражение всех создаваемых участником логинов, паролей и снимков экранов при выполнении задания.

**Представление результатов работы**

Настроенный виртуальный стенд, отчет о проделанной работе.

**Необходимые приложения**

**Необходимые приложения смотреть в папке «КОД 1.1 Приложения к вариантам».**

Образы виртуальных машин для установки