Модуль 1 Подключение и настройка сетевого оборудования.

1. Ознакомьтесь с данным заданием и со схемой подключения Схема 1. Учтите, что заданные заранее, а также задаваемые Вами логины и пароли должны быть в английской раскладке клавиатуры;

2. Не обязательно выполнять пункты задания по очереди, а также задание целиком, скорее всего Вам не хватит на это времени.

! ВНИМАНИЕ !

По окончании работы Вам необходимо предоставить на проверку сетевое оборудование и виртуальные машины в выключенном состоянии.

В любом случае всё предоставленное Вам оборудование будет перезагружено экспертами перед началом проверки.

Серверы Windows предоставляются для проверки с графическим интерфейсом.

В случае невозможности входа в систему через консоль с заданными в задании учетными данными или отсутствие графического интерфейса в серверах Windows, эксперты не устанавливают графической оболочки, не производят подбора паролей, в том числе по оставленным участником записям, и не запускают процедур его обхода. В результате выполнение работы по данной части конкурсного задания экспертами не оценивается.

Исходя из этого подумайте, как оптимизировать свою работу, приступите к решению задачи;

3. Произведите подключения сетевого оборудования согласно Схемы 1;

4. Подключение дополнительных проводов проводите с учетом техники безопасности. Не загромождайте свое рабочее место.

5. Для настройки устройств используйте следующие параметры локальной сети LAN: 192.168.N.192/27;

6. Настройте коммутатор:

6.1. задайте имя: SWITCH_N (где N – номер участника);

6.2. установите пароли:

6.2.1. на привилегированный режим: ab_adm

6.2.2. на 5 (пять) на терминальных линии: ab_vty

6.2.3. на консольное подключение: ab_con

6.3. Пароли в файле конфигурации НЕ должны отображаться в открытом текстовом виде, пароль на привилегированный режим должен быть зашифрован хэш-функцией;

6.4. Настройте вывод консольных сообщений в синхронном режиме, чтобы выводимые сообщения не разрывали ввод команд в консоли;

6.5. Обеспечьте безопасное удаленное подключение к коммутатору по протоколу SSH версии 2, используя следующие параметры:

6.5.1. локальный пользователь: cisco

6.5.2. пароль пользователя: SanFranCisco

6.5.3. имя домена: domain.com

6.5.4. длина ключа: 512 бит

6.6. Удаленное подключение должно быть возможно только по протоколу SSH;

6.7. Включите систему port security на интерфейсе fa0/9 со следующими параметрами:

6.7.1. максимально количество MAC адресов на порту – 50;

6.7.2. MAC адреса должны оставаться в настройках после перезагрузки;

6.7.3. способ отработки нарушения безопасности – блокировка с уведомлением;

6.8. Для настройки VLAN на коммутаторе используйте следующие параметры для локальной сети LAN:

6.8.1. номер VLAN – 9;

6.8.2. имя – LAN.

6.9. Все неиспользуемые интерфейсы отключите и переведите в VLAN с номером 99 и именем OUT;

6.10. Настройте виртуальный интерфейс управления коммутатором согласно Схемы1.

6.11. Настройте баннер «Сообщение дня» (message-of-the-day) следующего содержания: «Attention! Authorized access only!».

6.12. Настройте шлюз по умолчанию на интерфейс маршрутизатора;

7. Настройка маршрутизатора:

7.1. задайте имя: ROUTER_N (где N – номер участника);

7.2. установите пароли с функцией требования их ввода:

7.2.1. на привилегированный режим: ab_adm

7.2.2. на 5 (пять) терминальных линий: ab_vty

7.2.3. на консольное подключение: ab_con

7.2.4. на подключение aux: ab_aux

7.3. Пароли в файле конфигурации НЕ должны отображаться в открытом текстовом виде, пароль на привилегированный режим должен быть зашифрован хэш-функцией;

7.4. Настройте вывод консольных сообщений в синхронном режиме, чтобы выводимые сообщения не разрывали ввод команд в консоли.

7.5. Настройте баннер «Сообщение дня» (message-of-the-day) следующего содержания: «Attention! Authorized access only!».

7.6. Настройте интерфейсы маршрутизатора согласно Схемы 1 (где N – номер участника);

7.7. Обеспечьте безопасное удаленное подключение к маршрутизатору по протоколу SSH версии 2, используя следующие параметры:

7.7.1. локальный пользователь: cisco

7.7.2. пароль пользователя: SanFranCisco

7.7.3. имя домена: domain.com

7.7.4. длина ключа: 512 бит

7.8. Удаленное подключение должно быть возможно только по протоколу SSH;

7.9. Используя списки контроля доступа (ACL) обеспечьте, чтобы удаленное подключение к маршрутизатору было возможно только с

компьютера участника, но при этом никак не ограничивало трафик через маршрутизатор;

Модуль 2. Установка и настройка ОС

8. Настройте параметры BIOS компьютера для работы с ПО виртуализации.

9. Переведите ваш компьютер с предустановленной ОС Windows 2012R2 в режим гипервизора HYPER-V, сохранив графическую оболочку сервера.

10. Настройте на нем IP-адрес согласно Схемы 1.

11. Установите в виртуальную среду гипервизора ОС Windows Server 2016 с именем WIN2016_N (где последняя N – номер участника) с графической оболочкой, используя дистрибутив. Пароль на администратора: B!111111. Параметры для виртуальной машины: версия машины – 1, ресурсы: ядра – 2, оперативная память – 2 ГБ динамическая, сетевая карта, жесткий диск 20 ГБ.

11.1. Поднимите службу Active Directory (AD) на сервере. Имя домена: abN.local (где N – номер участника);

11.2. Установите и настройте службы DNS и DHCP;

11.3. Служба DHCP должна иметь пул из 6 (шести) адресов, начиная с 7го по счету доступного адреса из сети. В параметрах передается корректный шлюз и DNS сервер.

11.4. Службу DNS настройте на серверы пересылки: 8.8.8.8 и 8.8.4.4;

11.5. В структуре AD создайте подразделение USER. Заведите в AD пользователя USER_N (где N – номер участника) с паролем B!000000 и наделите его правами администратора домена. Пользователя разместите в подразделении USER;

11.6. В структуре AD создайте подразделение WIN10. Создайте групповую политику PC10_GP и примените к этому подразделению. В параметрах политики задайте минимальную длину пароля пользователей: 7 символов;

12. Установите в виртуальную среду ОС Windows10 professional используя дистрибутив. Параметры для виртуальной машины: версия машины – 2, ресурсы: ядра – 1, оперативная память – 2 ГБ динамическая, сетевая карта, жесткий диск 160 ГБ.

12.1. Задайте имя компьютера: WINX_N (где последняя N – номер участника);

12.2. Введите ОС Windows10 в домен;

12.3. Разместите WINX_N (где последняя N – номер участника) в подразделении WIN10.

12.4. ОС Windows10 должна получать зарезервированный IP-адрес от Windows Server 2016 (Схема 1);

13. Установите в виртуальную среду ОС Ubuntu16 server, используя готовый виртуальный диск ABI2018MOSCOW.vhdx. Для входа используйте учетные данные: пользователь: nemo, пароль: toor . Параметры для

виртуальной машины: версия машины – 1, ресурсы: ядра – 1, оперативная память – 512 ГБ статическая, сетевая карта.

13.1. Задайте имя компьютера: UBUNTU-N (где последняя N – номер участника),

13.2. Включите режим суперпользователя и установите ему пароль: B!111111

13.3. Настройте сетевой интерфейс согласно Схемы1. Установите корректные DNS и шлюз.

13.4. Заведите пользователей User1-N и User11-N (где N – номер участника) пароли: A!123456 и B!123456 соответственно.

13.5. Создайте группу ablmpx и добавьте в нее пользователя User11-N (где N – номер участника);

13.6. Добавьте сервер в списки репозиториев для скачивания свободно-распространяемого ПО http://mirror.abylimpix.ru/test/

14. Установите в виртуальную среду ОС CentOS 7 используя готовый виртуальный диск ABI2018KAZAN.vhdx. Параметры для виртуальной машины: версия машины – 1, ресурсы: ядра – 1, оперативная память – 512 МБ динамическая, сетевая карта.

15. Для входа в систему используйте логин/пароль: root/toortoor

15.1. Задайте имя компьютера: CENTOS-N (где последняя N – номер участника),

15.2. Установите пароль на суперпользователя root: A!111111

15.3. Настройте сетевой интерфейс согласно Схемы1. Установите корректные DNS и шлюз;

15.4. Измените DNS-суффикс для данной машины на abN.local (где N – номер участника);

15.5. Разрешите удаленное подключение по протоколу SSH для суперпользователя root.

N – НОМЕР УЧАСТНИКА

СХЕМА 1