КОНКУРСНОЕ ЗАДАНИЕ

«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

MODULE A: BASIC LINUX

Введение

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы сможете обслуживать информационную инфраструктуру большого предприятия.

Описание конкурсного задания

Данное конкурсное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

- Базовая конфигурация
- Сетевые службы
- Хранение данных
- Маршрутизация и удаленный доступ
- Аутентификация и безопасность
- Мониторинг и журналирование

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполнять поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает что работа не будет оценена. Например, для удаленного доступа к одной из организаций необходимо сконфигурировать IPsec, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE то вы все еще получите баллы за организацию удаленного доступа.

Обратите внимание, что организация «Left» использует только Debian Linux, и организация «Right» — только CentOS. Внешний клиент так же использует CentOS.

В зависимости от уровня сложности задания, выбранного для проведения демонстрационного экзамена, может присутствовать только одна организация Left.

Доступ ко всем виртуальным машинам настроен по аккаунту root/toor.

Инструкции для участника

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание в секции «Базовая конфигурация» предписывает автоматизировать удаленный доступ, который, разумеется, не будет работать без предварительной конфигурации, изложенной в секции «Маршрутизация и удаленный доступ». На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы

можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

Необходимое оборудование, приборы, ПО и материалы

Ожидается, что конкурсное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

Схема оценки

В соответствии с WorldSkills Standards Specifications текущего Технического Описания все оценки данного модуля конкурсного задания подпадают под пункт 6 «Install, upgrade and configure operating systems». Схема оценки также разделена на секции, которые можно наблюдать в тексте задания (каждый суб-критерий представляет одну секцию). Все суб-критерии имеют приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в суб-критерии.
Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в разделе «Базовая конфигурация» Вам предписывается настроить имена хостов для всех устройств, однако проверятся будет только одно устройство и оцениваться пункт будет только один раз. Одинаковые пункты проверки могут быть оценены несколько раз если они выполняются в разных конфигурациях для разных инсталляций или разных ОС. Например, в разделе «Маршрутизация и удаленный доступ» вам необходимо настроить удаленный доступ до разных сетей.
Детали методики проверки находятся в документе «How to Mark». Данный документ, как и схема оценки, является объектом внесения 30% изменений.

Базовая конфигурация

1) Установите имена компьютеров в соответствии со **схемой**
2) Настройте IP-адресацию в соответствии со **схемой**
3) Автоматизируйте удаленный доступ на хосте OUT-CLI с использованием bash-скриптов:
    a. Скрипт «**connect_left**» должен устанавливать VPN соединение до организации Left (Задание раздела «Маршрутизация и удаленный доступ»).
    b. После успешного подключения к организации через VPN, OUT-CLI должен разрешать имена, используя DNS-сервер организации Left
    c. Скрипт «**disconnect_any**» должен деактивировать VPN подключение
    d. Все скрипты должны находиться в **/opt/vpn**
    e. Пользователь должен иметь возможность вызывать скрипты без указания путей, причем вызываться должна копия скрипта, которая находится в **/opt/vpn**.
4) Автоматизируйте доступ к сетевым хранилищам на клиентских рабочих станциях:
    a. Скрипт «**mount_share**» должен осуществлять монтирование сетевого хранилища.
    b. Скрипт должен находиться в **/opt/scripts**.
    c. Пользователь должен иметь возможность вызывать скрипты без указания путей.

Сетевые службы

1) Настройте сервис автоматической конфигурации хостов на L-RTR-A в соответствии с требованиями:
    a. Машинам L-CLI-A, L-CLI-B должны быть присвоены:
        i. IP адреса из диапазона .50 - .150 соответствующей сети
        ii. Доменное имя соответствующей организации
        iii. Шлюз по умолчанию соответствующей сети
        iv. DNS сервер соответствующей организации
    b. DNS записи должны динамически добавляться и удаляться при выдаче адресов средствами DHCP.
2) Настройте службу DNS для сети Left на сервере L-SRV:
    a. Имя зоны wsr.left
    b. Файлы зон должны находиться в каталоге **/var/wsr/**
    c. Прямое и обратное разрешение имен должно быть реализовано для всех адресов
    d. Все компьютеры сети Left должны автоматически разрешать имена в соответствие с **таблицей 1**
3) Настройте трансляцию адресов
    a. Все исходящие во внешнюю сеть соединения должны получать адрес источника, равный адресу соответствующего выходного интерфейса FW.

Хранение данных

1) На L-SRV создайте каталог **/opt/samba/**. Организуйте общий доступ к каталогу с помощью Samba:
    a. Разделяемый ресурс должен называться “Share”
    b. Пользователи, аутентифицированные как smbuser:smbpass , должны получать доступ на чтение и запись
    c. Все файлы, создаваемые в директории, должны получать права «0700»
    d. Разрешите гостевой доступ с правами только для чтения.

2) Настройте клиентские машины организации
    a. Клиенты должны иметь доступ к разделяемым ресурсам своей организации
    b. Скрипт **«mount_share»** должен использоваться для подключения разделяемого ресурса в каталог **/opt/share**
3) Разверните TFTP сервер на L-SRV.
    a. Используйте **/opt/tftp-share** в качестве корневого каталога
    b. Все хосты организации “Left” должны иметь доступ на чтение и запись

Маршрутизация и удаленный доступ

1) Настройте site-to-site VPN и удаленный доступ на основе технологии OpenVPN:
    a. Общие параметры для соединений
        i. L-FW выступает в качестве VPN-сервера
        ii. Используйте TLS-шифрование
        iii. Используйте сжатие
        iv. Используйте TCP протокол
        v. RSA ключи должны храниться в каталоге **/opt/vpn/keys** соответствующего сервера\клиента.
    b. Удаленный доступ OpenVPN
        i. Используется устройство типа TUN
        ii. Сервер использует порт 1200
        iii. Подключенные клиенты должны получать IP адреса из пула 10.2.2.0/24
        iv. После успешного подключения к VPN-шлюзу весь трафик OUT-CLI должен проходить через туннель (в том числе и трафик, направленный в сеть OUT)
        v. Все хосты организации Left должны быть доступны через VPN

Аутентификация и безопасность

1) Разработайте и примените конфигурацию межсетевого экрана на L-FW:
    a. Разрешите доступ к сервисам VPN из сети OUT
    b. Запретите весь иной трафик
2) Для клиентов организации Left:
    a. Настройте sudo:
        i. Все пользователи (кроме root) не должны иметь возможность использовать visudo с помощью sudo
        ii. Все остальные команды должны выполняться через sudo с вводом пароля пользователя
    b. Доступ пользователя root к системе через tty1 должен быть запрещен в промежутке с 18-00 до 07-00

Мониторинг и журналирование

1) На сервере L-SRV установите и настройте систему мониторинга Cacti:
    a. В случае, если потребуется настроить аутентификацию, используйте пользователя “admin” и пароль Skills39
    b. Доступ к главной панели мониторинга должен осуществляться через URL http://172.16.20.100:80
    c. Настройте сбор информации с L-FW, L-RTR-X и L-SRV с применением протокола SNMPv2:
        i. Загрузка центрального процессора

ii. Использование оперативной памяти
iii. Использование дискового пространства
iv. Использование сетевых интерфейсов

Таблица 1. Правила разрешения имен для DNS-сервера организации «Left»

Хост	**DNS-имя**
L-SRV	srv.wsr.left; wsr.left;
L-RTR-A	rtr-a.wsr.left
L-RTR-B	rtr-b.wsr.left
L-RTR-X	rtr-x.wsr.left
L-FW	fw.wsr.left; tunnel.wsr.left

Linux Island.
Virtual network diagram