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 точно 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
- Конфигурация сетевой инфраструктуры
- Службы централизованного управления и журналирования
- Конфигурация служб удаленного доступа
- Конфигурация веб-служб
- Конфигурация служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

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 выполняться 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 необходимо настроить IPsec-туннель, 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.

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. 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.

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

Если Вам требуется установить пароль, (и он не указан в задании) используйте: “P@ssw0rd”.

Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен. При попытке его сброса возникнут проблемы.

Организация LEFT включает виртуальные машины: L-SRV, L-FW, L-RTR-A, L-RTR-B, L-CLI-A, L-CLI-B.

Организация RIGHT включает виртуальные машины: R-SRV, R-FW, R-RTR, R-CLI.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

В качестве системной ОС в организации **LEFT** используется **CentOS 8**

В качестве системной ОС в организации **RIGHT** используется **CentOS 8**

В обоих офисах возможно замещение ОС на Alt Linux

Для установки дополнительных пакетов, вам доступны интернет репозитории через YUM-Proxy **http://10.10.10.1:3128**

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

СХЕМА ОЦЕНКИ

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимавшими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

Базовая настройка

1) Настройте имена хостов в соответствии с **Диаграммой.**
2) Если необходимо, сформируйте файл /etc/hosts. Данный файл будет использован при проверке, в случае неработоспособности DNS.
3) В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.
4) Разработайте адресацию для сетей на ваше усмотрение.
5) ***Все хосты должны быть доступны аккаунту root по SSH на стандартном(22) порту***

Конфигурация сетевой инфраструктуры

1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Диаграммой**.
2) Настройте сервер протокола динамической конфигурации хостов для L-CLI-A и L-CLI-B
    a) В качестве DHCP-сервера организации LEFT используйте L-RTR-A.
        i) Используйте пул адресов 172.16.100.65 — 172.16.100.75 для сети L-RTR-A
        ii) Используйте пул адресов 172.16.200.65 — 172.16.200.75 для сети L-RTR-B
        iii) Используете адрес L-SRV в качестве адреса DNS-сервера.
    b) Настройте DHCP-сервер таким образом, чтобы L-CLI-B всегда получал фиксированный IP-адрес в соответствии с **Диаграммой.**
    c) В качестве шлюза по умолчанию используйте адрес интерфейса соответствующего маршрутизатора в локальной сети.
    d) Используйте DNS-суффикс **skill39.wsr.**
    e) DNS-записи типа A и PTR соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.
3) На L-SRV настройте службу разрешения доменных имен
    a) Сервер должен обслуживать зону **skill39.wsr.**
    b) Сопоставление имен организовать в соответствии с **Таблицей 1.**
    c) Настройте на R-SRV роль вторичного DNS сервера для зоны **skill39.wsr.**
        i) Используете адрес R-SRV в качестве адреса DNS-сервера для R-CLI.
    d) Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя **ya.ru**.
    e) Реализуйте поддержку разрешения обратной зоны.
    f) Файлы зон располагать в **/opt/dns/**
4) На L-FW и R-FW настройте интернет-шлюзы для организации коллективного доступа в Интернет.
    a) Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.
    b) Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.
    c) Сервер L-FW должен перенаправлять внешние DNS запросы от OUT-CLI на L-SRV. www.skill39.wsr должен преобразовываться во внешний адрес R-FW.

Конфигурация систем централизованного управления пользователями и компьютерами

1) Разверните LDAP-сервер для организации централизованного управления учетными записями на базе 389 Directory Server
    a) В качестве сервера выступает L-SRV.
    b) Создайте учетные записи ldapuser1 и ldapuser2
    c) L-CLI-A, L-SRV и L-CLI-B должны аутентифицироваться через LDAP.

Конфигурация служб мониторинга,резервного копирования, журналирования

1) На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
    d) Журналы должны храниться в директории **/opt/logs/.**
    e) Журналирование должно производится в соответствии с **Таблицей 3.**
    f) Обеспечьте ротацию логов со следующими параметрами:
        i) Размер одного файла логов не превышает 1MB
        ii) При ротации следует использовать сжатие
        iii) Обеспечьте хранение не более 5 файлов журналов

2) Разверните приложение loganalyzer на сервере L-SRV
    a) В качестве источников данных используйте собираемые логи в /opt/logs
    b) Доступ должен осуществляться по имени logs.skill39.wsr, по протоколу https.
    c) Реализуйте перенаправление http->https

Конфигурация служб удаленного доступа

1) На L-FW настройте сервер удаленного доступа на основе технологии OpenConnect
    a) Сервер должен работать на порту 4443 для tcp и udp
    b) В качестве сертификатов используйте сертификаты, выданные R-FW
    c) Разрешите исследование mtu
    d) Если клиент не активен в течении 30 минут, подключение должно быть разорвано
    e) В качестве адресного пространства для клиентов используйте 10.8.8.0/24
    f) Настройте использование DNS серверов предприятия и выдачу корректного доменного имени
    g) Все DNS запросы должны проходить через VPN туннель
    h) Сконфигурируйте пользователя vpnuser с паролем vpnpass. В качестве места хранения пользователя используйте локальную базу данных
2) На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenConnect
    a) Реализуйте автоматическое подключение к VPN сервису предприятия
        i) Создайте юнит connect.service
        ii) Обеспечьте запуск юнита connect после достижения network-online.target
        iii) В качестве описания юнита задайте “VPN Connector to skill39.wsr”
3) Настройте защищенный канал передачи данных между L-FW и R-FW с помощью технологии IPSEC:
    a) Параметры политики первой фазы IPSec:
        i) Проверка целостности SHA-1
        ii) Шифрование 3DES
        iii) Группа Диффи-Хеллмана — 14 (2048)

iv) Аутентификация по общему ключу WSR-2019

b) Параметры преобразования трафика для второй фазы IPSec:
   i) Протокол ESP
   ii) Шифрование AES
   iii) Проверка целостности SHA-2

c) В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между L-FW и R-FW

4) Настройте GRE-туннель между L-FW и R-FW:
   a) Используйте следующую адресацию внутри GRE-туннеля:
      i) L-FW: 10.5.5.1/30
      ii) R-FW: 10.5.5.2/30

Настройка маршрутизации

5) Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета FRR:
   a) Анонсируйте все сети, необходимые для достижения полной связности.
   b) Применение статических маршрутов не допускается.
   c) В обмене маршрутной информацией участвуют L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW.
   d) Соседство и обмен маршрутной информацией между L-FW и R-FW должно осуществляться исключительно через настроенный GRE-туннель.
   e) Анонсируйте сети локальных интерфейсов L-RTR-A и L-RTR-B.
   f) Запретите рассылку служебной информации OSPF в сторону клиентских машин и глобальной сети.

Конфигурация веб- и почтовых служб

1) На R-SRV установите и настройте веб-сервер apache:
   a) Настройте веб-сайт для внешнего пользования www.skill39.wsr.
      i) Используйте директорию **/var/www/html/out.**
      ii) Используйте порт 8088.
      iii) Сайт предоставляет доступ к двум файлам.
         1) index.html, содержимое “Hello, www.skill39.wsr is here!”
         2) date.php(исполняемый PHP-скрипт), содержимое:
            a) Вызов функции date('Y-m-d H:i:s');
2) На R-FW настройте реверс-прокси на основе NGINX:
   a) Сайт www.skill39.wsr должен быть доступен из внешней сети по внешнему адресу R-FW
   b) Все настройки, связанные с заданием, должны содержаться в отдельном конфигурационном файле в каталоге /etc/nginx/conf.d/task.conf
      i) Конфигурация основного файла должна быть минимальной и не влиять на работу NGINX в рамках выполнения задания.
   c) Настройте SSL и автоматическое перенаправление незащищенных запросов на HTTPS-порт того же самого сервера.
   d) Реализуйте пассивную проверку работоспособности бекенда.

i) Считать веб-сервер неработающим после 4 ошибок.
ii) Считать веб-сервер неработающим в течение 43 секунд.

e) Реализуйте кэширование:
i) Запросы к любым PHP-скриптам не должны кэшироваться.
ii) Кэширование успешных запросов к остальным типам данных должно выполняться в течение 40 секунд.

Конфигурация служб хранения данных

1) Преобразуйте в физические тома LVM все свободные носители.
a) Создайте группу логических томов WSR_LVM
b) Создайте следующие логические тома.
c) Users, 200 Мб.
d) Shares, 40% от оставшегося свободного места.
e) Обеспечьте создание снапшотов тома Backup раз в час.
f) Снапшоты создаются в формате SNAP-XX, где XX - номер снапшота, (01, 02 и т.д.)
g) Снапшоту выделяется 5% от общего объема группы томов.
h) Снапшоты должны создаваться при помощи скрипта /root/create_snap.sh
i) Создайте снапшот чистого тома Users с названием CLEAR
j) Снимок должен позволять хранение 30% изменений указанного логического тома.
k) Обеспечьте монтирование тома Users в каталог /opt/Users
l) Обеспечьте монтирование тома Shares в каталог /opt/Shares
m) Монтирование должно происходить во время загрузки системы.
2) Реализуйте файловый сервер на L-SRV
a) Создайте 2 общие папки shares и users
b) В папке shares создайте каталог workfolders. Внутри каталога workfolders создайте папки Work1 и Work2
i. Назначьте владельцем папки Work1 пользователя ldapuser1, владельцем папки Work2 пользователя ldapuser2
ii. Обеспечьте автоматическое монтирование каталога workfolders по протоколу smb при входе пользователя в папку work на рабочем столе
iii. Папка work должна автоматически создаваться при входе пользователя в систему и удаляться при выходе пользователя
iv. Обеспечьте отображение рабочих папок в зависимости от прав пользователя. Пользователь должен видеть только файлы и папки к которым у него есть доступ.
c) В папке users создайте домашние папки для всех пользователей LDAP
d) Обеспечьте автоматическое подключение домашних папок при входе пользователя на машины CLI1-A и CLI1-B по протоколу SMB в директорию /home

Конфигурация параметров безопасности и служб аутентификации

1) Настройте CA на R-FW, используя OpenSSL.
a) Используйте **/etc/ca** в качестве корневой директории CA
b) Атрибуты CA должны быть следующими:
i) Страна RU

ii) Организация WorldSkills Russia
iii) CN должен быть установлен как WSR CA

c) Создайте корневой сертификат CA
d) Все клиентские операционные системы должны доверять CA
e) Обеспечьте автоматический импорт сертификатов из системного хранилища в браузер firefox для всех пользователей.

3) Настройте межсетевой экран **nftables** на L-FW и R-FW
   a) Создайте таблицу wsr39
   b) Создайте цепочки in_chain и out_chain для входящего и исходяшего трафика
   c) Реализуйте правила работы с трафиком
      i) Весь трафик, покидающий внутреннюю сеть должен проходить маскарадинг
      ii) Разрешите прохождение трафика, необходимого для выполнения задания
      iii) Весь остальной трафик следует запретить
4) На L-FW настройте удаленный доступ по протоколу SSH:
   a) Доступ ограничен пользователями **ssh_p, root** и **ssh_c**
      i) В качестве пароля пользователь (кроме root) использовать **ssh_pass.**
      ii) root использует стандартный пароль
   b) SSH-сервер должен работать на порту **22**
5) На OUT-CLI настройте клиент удаленного доступа SSH:
   a) Доступ к L-FW из под локальной учетной записи root под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация и установка системы

1. На сервере R-SRV требуется выполнить обновление дистрибьютива CentOS 8. Произведите обновление ОС с использованием внешних репозиториев. Учтите, что на сервере присутствуют важные данные, по этому переустанавливать систему запрещается.

Настройка подключений к глобальным сетям

1) Настройте корректную IP-адресацию между всеми устройствами в подсети 20.20.20.0/24

Конфигурация подсистемы телефонной связи

В данном модуле настройка не предусмотрена

Виртуализация

В данном модуле настройка не предусмотрена

СУБД

В данном модуле настройка не предусмотрена

Автоматизация администрирования

В данном модуле настройка не предусмотрена

Таблица 1 – DNS-имена

Хост	**DNS-имя**
L-CLI-A	A,PTR: l-cli-a.skill39.wsr
L-CLI-B	A,PTR: l-cli-b.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: server.skill39.wsr
L-FW	A: l-fw.skill39.wsr
R-FW	A: r-fw.skill39.wsr CNAME: www.skill39.wsr
R-SRV	A,PTR: r-srv.skill39.wsr

Таблица 3 – Правила журналирования

Источник	Уровень журнала (строгое соответствие)	Файл
L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log

*<HOSTNAME> - название директории для журналируемого хоста
**В директории /opt/logs/ не должно быть файлов, кроме тех, которые указаны в таблице

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ