Лаб1

1. **Для чего предназначен Vagrant?**

Vagrant — это инструмент для создания и управления средами виртуальных машин в одном рабочем процессе. Этот инструмент, по сути, позволяет автоматизировать процесс установки на виртуальную машину как основного дистрибутива операционной системы, так и настройки необходимого в дальнейшем программного обеспечения.

2. **Что такое box-файл? В чём назначение Vagrantfile?**

Box-файл — сохранённый образ виртуальной машины с развёрнутой в ней ОС, по сути, box-файл используется как основа для клонирования виртуальных машин с теми или иными настройками;

Vagrantfile — конфигурационный файл, написанный на языке Ruby, в котором указаны настройки запуска виртуальной машины.

3. **Приведите описание и примеры вызова основных команд Vagrant:**

- vagrant help — вызов справки по командам Vagrant;
- vagrant box list — список подключённых к Vagrant box-файлов;
- vagrant box add — подключение box-файла к Vagrant;
- vagrant destroy — отключение box-файла отVagrant и удаление его из виртуального окружения;
- vagrant init — создание «шаблонного» конфигурационного файла Vagrantfile для его последующего изменения;
- vagrant up — запуск виртуальной машины с использованием инструкций по запуску из конфигурационного файла Vagrantfile;
- vagrant reload — перезагрузка виртуальной машины;
- vagrant halt — остановка и выключение виртуальной машины; Королькова А. В., Кулябов Д. С. Администрирование сетевых подсистем 7
- vagrant provision — настройка внутреннего окружения имеющейся виртуальной машины (например, добавление новых инструкций (скриптов) в ранее созданную виртуальную машину);
- vagrant ssh — подключение к виртуальной машине через ssh.

4. **Дайте построчные пояснения содержания файлов vagrant-rocky.pkr.hcl, ks.cfg, Vagrantfile, Makefile.**
    - vagrant-rocky.pkr.hcl — специальный файл с описанием метаданных по установке дистрибутива на виртуальную машину в частности, в разделе переменных этот файл содержит указание на версию дистрибутива, его хэшфункцию, имя и пароль пользователя по умолчанию;
    - ks.cfg — определяет настройки для установки дистрибутива, которые пользователь обычно вводит вручную, в частности настройки языка интерфейса, языковые настройки клавиатуры, тайм-зону, сетевые настройки и т.п.; файл должен быть расположен в подкаталоге http.
    - Vagrantfile — файл с конфигурацией запуска виртуальных машин — сервера и клиента;
    - Makefile — набор инструкций для программы make по работе с Vagrant

Лаб2

1. Что такое DNS? – распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP-адрес и наоборот.
2. Каково назначение кэширующего DNS-сервера ?

   Кэширующий DNS-сервер получает рекурсивные запросы от клиентов и выполняет их с помощью нерекурсивных запросов к авторитативным серверам.

3. Чем отличается прямая DNS-зона от обратной?

   Задача поиска доменного имени по IP-адресу является обратной к прямой задаче — поиску IP-адреса по доменному имени. Прямая решается в DNS при помощи записей типа A (Address). Обратная же при помощи записей-указателей типа PTR (Pointer), которые совместно с записями SOA и NS составляют описание так называемой «обратной» зоны.

4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.

   В файле host.conf содержатся опции программы-определителя, в файле resolv.conf содержатся адреса серверов имен, к которым имеет доступ данная система. Файл

named.ca организует кэширование для сервера имен.

5. Что указывается в файле resolv.conf?

   В файле resolv.conf содержатся адреса серверов имен, к которым имеет доступ данная система.

6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?
   - SOA-запись — указывает на авторитативность для зоны
   - NS-запись — перечисляет DNS-серверы зоны
   - A — отображение имён узлов в адреса
   - PTR — отображение адресов в имена узлов
   - CNAME — каноническое имя (для псевдонимов)
   - MX — отображение имён почтовых серверов
7. Для чего используется домен in-addr.arpa?

   Для отображения IP-адресов IPv4 в пространство доменных имен

8. Для чего нужен демон named?

   Демон named может реализовывать функции серверов любого типа: master, slave, cache.

9. В чём заключаются основные функции slave-сервера и master сервера?
   - master — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых
   - slave — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны. Служит для снижения нагрузки с главного DNS-сервера.
10. Какие параметры отвечают за время обновления зоны?

    За обновление отвечает третий параметр в файле kreachna.net

11. Как обеспечить защиту зоны от скачивания и просмотра?

    Задать подходящие права доступа на чтение и запись.

12. Какая запись RR применяется при создании почтовых серверов?

    При создании почтовых серверов используют A записи.

13. Как запустить, перезапустить или остановить какую-либо службу в системе?

    Использовать в терминале команды systemctl start, restart, stop.

14. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?

    Посмотреть в journalctl.

15. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli.

    nmcli connection edit System\ eth0

    remove ipv4.dns

    set ipv4.ignore-auto-dns yes

    set ipv4.dns 127.0.0.1

    save

    quit

16. Что такое SELinux?

    (SELinux) - это модуль безопасности ядра Linux, который обеспечивает механизм поддержки политик безопасности контроля доступа, включая обязательные элементы управления доступом (MAC).

17. Что такое контекст (метка) SELinux?

    Каждый файл, процесс, каталог и порт имеют специальную метку безопасности, известную как контекст SELinux, который является именем, используемым для определения, может ли процесс получить доступ к файлу, каталогу или порту.

18. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?

    restorecon.

19. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?

    Использовать команду chown -R

20. Что такое булевый переключатель в SELinux?\

21. Как посмотреть список переключателей SELinux и их состояние?

    Команда getsebool -a | grep named

22. Как изменить значение переключателя SELinux

    Необходимо использовать команду setsebool.

Лаб3

1. В каких файлах хранятся настройки сетевых подключений?

   Настройки сетевых подключений хранятся в файле dhcp.conf.

2. За что отвечает протокол DHCP?

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

3. Поясните принцип работы протокола DHCP. Какими сообщениями обмениваются клиент и сервер, используя протокол DHCP?
    - DHCPDISCOVER – широковещательная передача клиента для определения местоположения доступных серверов.
    - DHCPOFFER – Сервер клиенту в ответ на DHCPDISCOVER с предложением параметров конфигурации.
    - DHCPREQUEST – клиентское сообщение серверам, либо (а) запрашивающее предлагаемые параметры у одного сервера и неявно отклоняющее предложения от всех остальных, (б) подтверждающее правильность ранее выделенного адреса после, например, перезагрузки системы, либо (в) продлевающее аренду определенного сетевого адреса.
    - DHCPACK – Сервер для клиента с параметрами конфигурации, включая фиксированный сетевой адрес.
    - DHCPNAK – Сервер клиенту, указывающий, что представление клиента о сетевом адресе неверно (например, клиент перешел в новую подсеть) или срок аренды клиента истек.
    - DHCPDECLINE – Соединение клиента с сервером, указывающее, что сетевой адрес уже
    - в использовании.
    - DHCPRELEASE – передача сетевого адреса от клиента к серверу иотмена оставшейся аренды.
    - DHCPINFORM – Клиент на сервер, запрашивающий только параметры локальной конфигурации; у клиента уже есть внешне настроенный сетевой адрес.
4. В каких файлах обычно находятся настройки DHCP-сервера? За что отвечает каждый из файлов?
    - dhcpd.conf – содержащий список инструкций, которые dhcpd использует для

настройки DHCP.

- dhcpd.lease – хранит базу данных аренды DHCP-клиента.

5. Что такое DDNS? Для чего применяется DDNS?

DDNS – Dynamic dns. Она применяется для назначения постоянного доменного имени устройству (компьютеру, сетевому накопителю) с динамическим IP-адресом.

6. Какую информацию можно получить, используя утилиту ifconfig? Приведите примеры с использованием различных опций.

Команда ifconfig используется для конфигурирования и диагностики сетевых интерфейсов операционной системы.

```
[kreachna@client.kreachna.net ~]$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe5c:b0b8  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:b0:b8  txqueuelen 1000  (Ethernet)
        RX packets 1571  bytes 176678 (172.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1558  bytes 230478 (225.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Например, ifconfig eth0 : для просмотра сетевых настроек в интерфейсе eth0.

7. Какую информацию можно получить, используя утилиту ping? Приведите примеры с использованием различных опций.

Утилита ping предназначена для проверки соединений в сетях на основе TCP/IP.

```
[root@server.kreachna.net dhcp]# ping dhcp.kreachna.net
PING dhcp.kreachna.net (192.168.1.1) 56(84) bytes of data.
64 bytes from ns.kreachna.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from dhcp.kreachna.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.081 ms
64 bytes from server.kreachna.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.224 ms
64 bytes from server.kreachna.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.103 ms
64 bytes from dhcp.kreachna.net (192.168.1.1): icmp_seq=5 ttl=64 time=0.105 ms
64 bytes from dhcp.kreachna.net (192.168.1.1): icmp_seq=6 ttl=64 time=0.087 ms
^C
--- dhcp.kreachna.net ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 0.042/0.107/0.224/0.056 ms
```

Лаб4

1. Через какой порт по умолчанию работает Apache?

По умолчанию Apache прослушивает порта 80.

2. Под каким пользователем запускается Apache и к какой группе относится этот

пользователь?

Apache запускается под суперпользователем.

3. Где располагаются лог-файлы веб-сервера? Что можно по ним отслеживать?

   Лог файлы располагаются в каталоге httpd.conf.

4. Где по умолчанию содержится контент веб-серверов?

   Умолчанию контент содержится в файле index.html.

5. Каким образом реализуется виртуальный хостинг? Что он даёт?

   Создаем файлы server.user.net и www.user.net, вносим в них основные диретивы, в файле индекса прописываем необходимую информацию, не забывая дать нужные права на исполнение.

Лаб5

1. В чём отличие HTTP от HTTPS?

HTTPS (HyperText Transfer Protocol Secure) — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.

2. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?

Улучшение безопасности при использовании HTTPS вместо HTTP достигается за счёт

использования криптографических протоколов при организации HTTP-соединения и передачи по нему данных. Для шифрования может применяться протокол SSL (Secure

Sockets Layer) или протокол TLC (Transport Layer Security). Оба протокола используют асимметричное шифрование для аутентификации, симметричное шифрование для

конфиденциальности и коды аутентичности сообщений для сохранения целостности

сообщений.

3. Что такое сертификационный центр? Приведите пример.

Сертификационный центр (Certification authority, CA) представляет собой компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Его открытый ключ широко известен общественности и не вызывает сомнений в подлинности.

Лаб6

1. Какая команда отвечает за настройки безопасности в MariaDB?

Команда mysql_secure_installation

2. Как настроить MariaDB для доступа через сеть?

При вводе команды mysql_secure_installation нажать n при запросе на запрет подключение по сети.

3. Какая команда позволяет получить обзор доступных баз данных после входа в среду оболочки MariaDB?

Команда SHOW DATABASES;

```
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.001 sec)
```

4. Какая команда позволяет узнать, какие таблицы доступны в базе данных?

Команда SHOW TABLES;

5. Какая команда позволяет узнать, какие поля доступны в таблице?

Команда DESCRIBE

```
MariaDB [addressbook]> DESCRIBE city;
+-------+-------------+------+-----+---------+-------+
| Field | Type        | Null | Key | Default | Extra |
+-------+-------------+------+-----+---------+-------+
| name  | varchar(40) | YES  |     | NULL    |       |
| city  | varchar(40) | YES  |     | NULL    |       |
+-------+-------------+------+-----+---------+-------+
2 rows in set (0.001 sec)
```

6. Какая команда позволяет узнать, какие записи доступны в таблице?

Команда SELECT

```
MariaDB [addressbook]> SELECT * FROM city;
+---------+--------+
| name    | city   |
+---------+--------+
| Ivanov  | Moscow |
| Petrov  | Sochi  |
| Sidorov | Doubna |
+---------+--------+
3 rows in set (0.000 sec)
```

7. Как удалить запись из таблицы?

Команда: DELETE FROM <таблица> WHERE <столбец>='значение’;

8. Где расположены файлы конфигурации MariaDB? Что можно настроить с их помощью?

Конфигурационные файлы mariadb расположены в каталоге /etc/my.cnf.d и в файле /etc/my.cnf

9. Где располагаются файлы с базами данных MariaDB?

/var/lib/mysql/

10. Как сделать резервную копию базы данных и затем её восстановить?

```
[root@server.kreachna.net my.cnf.d]# mkdir -p /var/backup
[root@server.kreachna.net my.cnf.d]# mysqldump -u root -p addressbook > /var/backup/addressbook.sql
Enter password:
[root@server.kreachna.net my.cnf.d]# mysqldump -u root -p addressbook | gzip > /var/backup/addressbook.sql.gz
Enter password:
[root@server.kreachna.net my.cnf.d]# mysqldump -u root -p addressbook | gzip > $(date +/var/backup/addressbook.%Y%m%d.%
H%M%S.sql.gz)
Enter password:
[root@server.kreachna.net my.cnf.d]# mysql -u root -p addressbook < /var/backup/addressbook.sql
Enter password:
[root@server.kreachna.net my.cnf.d]# zcat /var/backup/addressbook.sql.gz | mysql -u root -p addressbook
Enter password:
```

Лаб7

1. Где хранятся пользовательские файлы firewalld?

   /usr/lib/firewalld/services/ssh.xml

2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?

   <port protocol="tcp" port="2022"/>

3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?

   firewall-cmd --get-services

4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?

   NAT производит замену адреса на любой указанный, а маскарадинг только на адрес,

машины, выполняющей маскарад.

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?
   firewall-cmd --add-forward-port=port=4404:proto=ssh:toaddr=10.0.0.10
6. Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?
   firewall-cmd --zone=public --add-masquerad

Лаб8

1. В каком каталоге и в каком файле следует смотреть конфигурацию Postfix?
   /etc/postfix/main.cf
2. Каким образом можно проверить корректность синтаксиса в конфигурационном файле Postfix?
   postfix check
3. В каких параметрах конфигурации Postfix требуется внести изменения в значениях для настройки возможности отправки писем не на локальный хост, а на доменные адреса?
   В параметры mydestination и mynetworks.
   Пример команды: postconf -e 'mydestination = $myhostname, localhost.$mydomain, postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'.
4. Приведите примеры работы с утилитой mail по отправке письма, просмотру имеющихся писем, удалению письма.
   Отправка письма: mail -s “тема” <адрес_назначения>
   Просмотр писем: mail -f
   Удаление письма: mail -d
5. Приведите примеры работы с утилитой mail по отправке письма, просмотру имеющихся писем, удалению письма.
   Очередь сообщений: postqueue -p

   Определить число сообщений:postqueue -p | wc -l

   Отправить сообщения из очереди: postqueue -f

   Удалить письмо: postsuper -d ID_mail

Лаб9

1. За что отвечает протокол SMTP?

Протокол SMTP предназначен для передачи исходящей почты с использованием порта TCP 25.

2. За что отвечает протокол IMAP?

Протокол отвечает за отправку электронных сообщений. Порт TCP 143.

3. За что отвечает протокол POP3?

Протокол отвечает за получение электронных сообщений. Порт 110.

4. В чём назначение Dovecot?

Dovecot — агент доставки почты (MDA) по протоколам POP3 и IMAP с возможностью обеспечения безопасности и надёжности за счёт использования протокола TLS.

5. В каких файлах обычно находятся настройки работы Dovecot? За что отвечает каждый из файлов?
   - /etc/dovecot/dovecot.conf - конфигурационный файл
   - /etc/dovecot/conf.d/10-auth.conf – файл аутентификации
   - /etc/dovecot/conf.d/auth-system.conf.ext - файл аутентификации для системных пользователей
   - /etc/dovecot/conf.d/10-mail.conf – способ хранения сообщений
6. В чём назначение Postfix?

Postfix — агент передачи почты. Он обрабатывает почту для указанных в настройках доменов.

7. Какие методы аутентификации пользователей можно использовать в Dovecot и в чём их отличие?

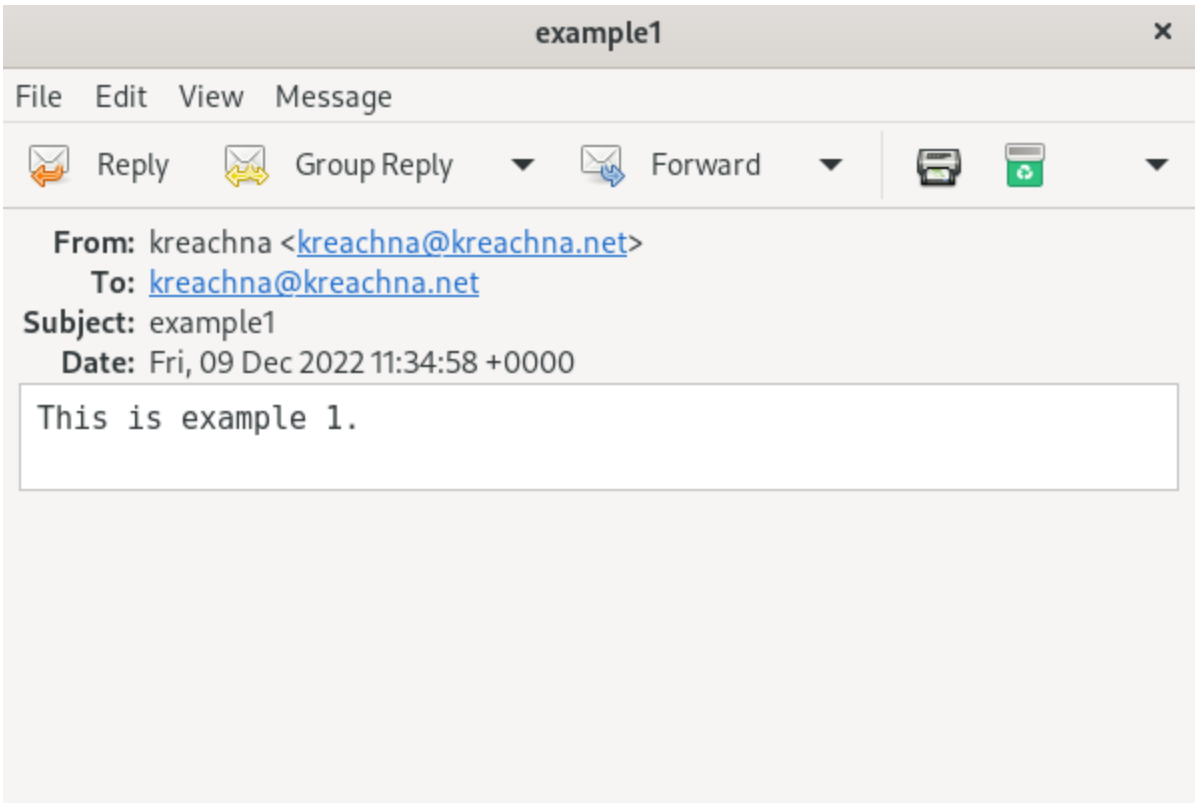
CRAM-MD5 — Защищает пароль при передаче от подслушивания.

SCRAM-SHA-1, SCRAM-SHA-256 — Механизм проверки подлинности ответа на вызов (SCRAM) Механизмы SAS и GSS-API.

APOP — проверка подлинности, специфичная для POP3.

ANONYMOUS — поддержка анонимного входа в систему

8. Приведите пример заголовка письма с пояснениями его полей.



9. Приведите примеры использования команд для работы с почтовыми протоколами через терминал (например через telnet).
   - подключилась с помощью протокола Telnet к почтовому серверу по протоколу POP3 (через порт 110), ввела свой логин для подключения и пароль
   - с помощью команды list получила список писем
   - с помощью команды retr 1 получила первое письмо из списка
   - с помощью команды dele 2 удалила второе письмо из списка
   - с помощью команды quit завершила сеанс работы с telnet

10. Приведите примеры с пояснениями по работе с doveadm.

doveadm mailbox list -u user — просмотр почты пользователя

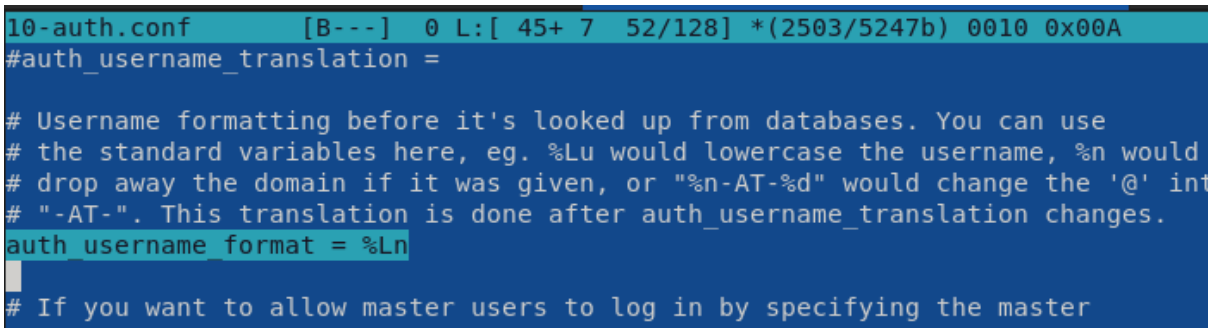
```
[root@server.kreachna.net ~]# doveadm mailbox list -u kreachna
INBOX
```

Лаб10

1. Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.

Auth_username_format = %Ln

В файле /etc/dovecot/conf.d/10-auth.conf в ходе лабораторной работы мы задавали формат имени пользователя для аутентификации в форме логина без указания домена. За это отвечает добавление «n». Для того, чтобы задать формат в форме логина с указанием домена, нужно не указывать данную опцию.



2. Какие функции выполняет почтовый Relay-сервер?

   Это сервер-посредник, принимающий электронную почту у отправителей и доставляющий ее получателям. Обеспечивает приём сообщения, временное хранение пересылку сообщения узлу-получателю.

3. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?

   Чрезмерное расходование трафика третьими лицами, массовые вредоносные рассылки, организации атак на отказ в обслуживании на другие почтовые системы, неиспользуемые службы и открытые порты, утечки информации.

Лаб11

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

   /etc/ssh/sshd_config: PermitRootlogin no

   /etc/ssh/sshd_config: AllowUsers alice

2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

   Добавить новый порт в в файле конфигурации, исправить метки безопасности и открыть порт в настройках межсетевого экрана. Организация через разные порты дает гарантию возможности открыть сеансы ssh даже при ошибки конфигурации.

3. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?

   fN

4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?

   ssh -fNL 5555:localhost:80 server2.example.com

5. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?

   semanage port -a -t ssh_port_t -p tcp 2022

6. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?

   firewall-cmd --add-port=2022/tcp

   firewall-cmd --add-port=2022/tcp --permanent

Лаб12

1. Почему важна точная синхронизация времени для служб баз данных?

   Если дата и время будут указаны неверно в базе данных может возникнуть конфликт записей.

2. Почему служба проверки подлинности Kerberos сильно зависит от правильной синхронизации времени?

   Когда KDC получает AS_REQ сообщение — он проверяет, что клиент, от которого пришёл запрос, существует, и его метка времени близка к локальному времени KDC (обычно ± 5 минут). Данная проверка производится не для защиты от повторов (сообщение посылается открытым текстом), а для проверки соответствия времени. Если хотя бы одна из проверок не проходит — клиенту отправляется сообщение об ошибке, и он не аутентифицируется.

3. Какая служба используется по умолчанию для синхронизации времени на RHEL 7?

   1. ручной с помощью утилиты ntpdate
   2. автоматический при помощи сервиса ntp

4. Какова страта по умолчанию для локальных часов?

   8

5. Какой порт брандмауэра должен быть открыт, если вы настраиваете свой сервер как одноранговый узел NTP?

123

6. Какую строку вам нужно включить в конфигурационный файл chrony, если вы хотите быть сервером времени, даже если внешние серверы NTP недоступны?

   allow 192.168.0.0/16

```
chrony.conf        [----] 20 L:[ 22+25  47/ 52] *(1276/1391b) 0102
# the system clock.
#minsources 2

# Allow NTP client access from local network.
#allow 192.168.0.0/16
allow 192.168.0.0/16
```

7. Какую страту имеет хост, если нет текущей синхронизации времени NTP?

   0

8. Какую команду вы бы использовали на сервере с chrony, чтобы узнать, с какими серверами он синхронизируется?

   chronyc sources

9. Как вы можете получить подробную статистику текущих настроек времени для процесса chrony вашего сервера?

   chronyc tracking

```
[root@server.kreachna.net ~]# chronyc tracking
Reference ID    : C2BEA801 (ntp.ix.ru)
Stratum         : 2
Ref time (UTC)  : Sat Dec 17 09:54:08 2022
System time     : 0.000111979 seconds fast of NTP time
Last offset     : +0.000165861 seconds
RMS offset      : 0.000316950 seconds
Frequency       : 508.069 ppm fast
Residual freq   : +0.042 ppm
Skew            : 4.129 ppm
Root delay      : 0.007412221 seconds
Root dispersion : 0.001556168 seconds
Update interval : 64.4 seconds
Leap status     : Normal
```

Лаб13

1. Как называется файл конфигурации, содержащий общие ресурсы NFS?

   /etc/fstab

2. Какие порты должны быть открыты в брандмауэре, чтобы обеспечить полный доступ к серверу NFS?

NFS использует порт 2049. NFSv3 и NFSv2 используют службу portmapper на TCP или UDP-порту 111.

3. Какую опцию следует использовать в /etc/fstab, чтобы убедиться, что общие ресурсы NFS могут быть установлены автоматически при перезагрузке?
   server.user.net:/srv/nfs /mnt/nfs nfs _netdev 0 0

Лаб14

1. Какова минимальная конфигурация для smb.conf для создания общего ресурса, который предоставляет доступ к каталогу /data?
   [data]
   comment = data resource
   path = /data
2. Как настроить общий ресурс, который даёт доступ на запись всем пользователям, имеющим права на запись в файловой системе Linux?
   writable = yes (read only=no)
3. Как ограничить доступ на запись к ресурсу только членам определённой группы?
   read list = @group
4. Какой переключатель SELinux нужно использовать, чтобы позволить пользователям получать доступ к домашним каталогам на сервере через SMB?
   На примере общего ресурса /srv/sambashare:
   semanage fcontext -a -t samba_share_t "/srv/sambashare(/.*)?"
   restorecon -vR /srv/sambashare
5. Как ограничить доступ к определённому ресурсу только узлам из сети 192.168.10.0/24?
   hosts deny = 192.168.10.0/24
6. Какую команду можно использовать, чтобы отобразить список всех пользователей Samba на сервере?
   pdbedit -L
7. Что нужно сделать пользователю для доступа к ресурсу, который настроен как многопользовательский ресурс?
   Подключиться к серверу с помощью smbclient: smbclient -L //server.
8. Как установить общий ресурс Samba в качестве многопользовательской учётной записи, где пользователь alice используется как минимальная учётная запись пользователя?

guest ok = yes

guest account = alice

9. Как можно запретить пользователям просматривать учётные данные монтирования Samba в файле /etc/fstab?

   veto files = /etc/fstab

10. Какая команда позволяет перечислить все экспортируемые ресурсы Samba, доступные на определённом сервере?

    smbtree

Лаб15

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?

   imjournal

2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?

   imuxsock

3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?

   $OmitLocalLogging on – данная строка отключает прием логов через модуль imuxsock.

4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?

   Все настройки rsyslog находятся в файле /etc/rsyslog.conf.

5. Каким параметром управляется пересылка сообщений из journald в rsyslog?

   Journald отправляет сообщения в rsyslog по умолчанию. Об этом заботятся две части конфигурации. Во-первых, файл /etc/systemd/journald.conf содержит строку ForwardToSyslog, которая по умолчанию имеет значение yes. Вовторых rsyslog.conf содержит модуль imjournal, необходимый для получения сообщений из journald.

6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

   imfile - модуль ввода текстовых файлов

7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?

   ommysql

8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?
   $ModLoad imtcp и $InputTCPServerRun 514
9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?
   firewall-cmd --add-port=514/tcp
   firewall-cmd --add-port=514/tcp --permanent

Лаб16

1. Поясните принцип работы Fail2ban.

Fail2ban считывает логи (например, /var/log/apache2/error.log) и блокирует IP-адреса, активность которых является подозрительной(например, большое количество попыток войти с неправильно введенным паролем, выполнение опасных или бессмысленных действий и т.д.). В случае обнаружения подобных действий программа обновляет правила брандмауэра для блокировки такого IPадреса на определенный промежуток времени.

2. Настройки какого файла более приоритетны: jail.conf или jail.local?

После установки в каталоге /etc/fail2ban будет такая структура конфигурационных файлов

- /etc/fail2ban/jail.conf
- /etc/fail2ban/jail.d/*.conf
- /etc/fail2ban/jail.local
- /etc/fail2ban/jail.d/*.local

Конфигурационные файлы считываются сверху вниз. Последний считанный файл имеет высший приоритет. В данном случае при существовании фалов с расширением local будут более приоритетны.

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Если вы хотите настроить оповещение о срабатывании блокировки Fail2ban по электронной почте, это тоже настраивается в разделе [DEFAULT]. Только необходимо чтобы на вашей машине был настроен почтовый сервер и он мог отправлять письма на внешний адрес. Иначе все письма будут доставлены к локальной учетной записи Linux.

- destemail - этот параметр задает адрес электронной почты, на который вы хотите

получать сообщения. Значение по умолчанию root@localhost;

- mta - определяет почтовый агент, который будет использоваться для доставки почты. Если у вас настроен Sendmail, оставьте значение по умолчанию. Если же письма нужно доставлять на локальную машину поменяйте значение на mail.
- Также для локальной почты нужно заменить строчку action_mw на action_mwl

4. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.

В данном файле, если мы откроем часть «HTTP servers», мы встретим описание нескольких правил. Они имеют следующий синтаксис: [название правила], port — порт целевого сервиса, logpath — расположение лог-файла, в котором фильтр будет искать подозрительную активность на основе описанных критериев, bantime — время бана в секундах, по истечении которого IP–адрес удаляется из списка заблокированных, maxretry — количество подозрительных совпадений, после которых применяется правило. Здесь присутствуют несколько секций, например, [apache-auth] - определяет неудачные попытки ввода пароля, [apache-badbots] - определяет ботов, которые ищут email адреса, [apache-noscript] - блокирует доступ к определенным скриптам, [apache-overflows] - предотвращает попытки переполнения Apache, [apache-nohome] - блокирует неудачные попытки поиска домашней директории. Но они не активированы, чтобы это исправить, нужно в каждую секцию добавить параметр enabled = true.

5. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе.

В данном файле, если мы откроем часть «MAIL servers», мы встретим описание нескольких правил. Они имеют следующий синтаксис: [название правила], port — порт целевого сервиса, logpath — расположение лог-файла, в котором фильтр будет искать подозрительную активность на основе описанных критериев, maxretry — количество подозрительных совпадений, после которых применяется правило.

6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?

Действие определяется в переменной action в зависимости от предпочтений администратора. Все правила реагирования на действия злоумышленника описаны в файле /etc/fail2ban/action.d. Соответственно, в качестве значения параметра action не может быть указана информация, которой нет в файле /etc/fail2ban/action.d

7. Как получить список действующих правил Fail2ban?

fail2ban-client status

8. Как получить статистику заблокированных Fail2ban адресов?

fail2ban-client status <имя клетки>

9. Как разблокировать IP-адрес?

fail2ban-client set <имя клетки> unbanip <ip-адрес>