Учебный курс

Безопасность сетей на базе Linux (Unix)

(лабораторные работы к курсу SecurL без ответов)

Автор: Лесковец В.В.

Версия: 2.0

г. Екатеринбург
2025

Оглавление

Глава 1. Введение.

1.1 Подготовка виртуалных машин.

1. Предполагается выполнение лабораторных работ на виртуальных машинах в среде VirtualBox или QEMU/KVM (libvirt).
2. Хостовая ОС может быть любой: Linux, Windows и пр.
3. Требования к хостовой машине:
    1. ОЗУ — от 16Гб.
    2. Не менее 6 ядер.
    3. Диск (SSD) — от 100Гб свободного места.
    4. Подготовленный шаблон виртуальных с установленной ОС Debian 12. Установлена по умолчанию. ОЗУ — 2Гб., 2 ядра, диск — 40Гб., каталог /home расположен на отдельном разделе, размером от 5Гб. Сеть назначенная для шаблона должна иметь выход в интернет и допускать взаимодействие ВМ между собой и с хостом.
4. Сделайте клон виртуальной машины с именем SRV1. В новой ВМ увеличьте количество памяти до 4Гб. В виртуальной машине должно быть создано два пользователя с именами sa и user. Пароль — lin123. Пользователь sa добавлен в группу sudo.
5. Запустите ВМ SRV1 и настройте имя гостевой машины на srv1. Не забудьте прописать новое имя в файле `/etc/hosts`.
6. Сделайте еще 2 клона виртуальной машины с именем CL1 и CL2.
7. Запустите ВМ CL1 и CL2 и настройте имя гостевой машины на cl1и cl2. Не забудьте прописать новые имена в файле `/etc/hosts`.

Глава 2. Обеспечение физической безопасности Linux-сервера.

2.1 Работа с ИБП.

Если имеется ИБП, то настройте управление им в вашей ОС. Данные о подключении к ИБП получите от преподавателя.

1. Установите пакеты nut и nut-client
2. Установите режим работы NUT в netclient
3. Настройте мониторинг ИБП
4. Перезапустите службу nut-monitor.service проверьте ее состояние.
5. Проверьте какие у ИБП: нагрузка, процент заряда, модель, общее состояние.

2.2 Настройка и управление загрузкой

1. Настройте пароль для изменения настроек в GRUB во время загрузки.

2. Опробуйте как работает пароль в GRUB.

3. Проведите процедуру сброса пароля.

2.3 Шифрование диска

На CL1:

1. Добавьте в виртуальную машину дисковый контроллер USB и подключите к нему диск.
2. Если пакет cryptsetup не установлен, то установите его.
3. Определите что вы будете шифровать, это целый USB диск, поэтому нужно определить его имя
4. Подготовка диска — заполнение диска случайными данными. Этот этап можно пропустить, но тогда данные будут уязвимыми.
5. Утилитой `cryptsetup` определите параметры шифрования.
6. Создайте виртуальное устройство для шифрованного диска
7. Создайте файловую систему
8. Смонтируйте файловую систему и создайте в ней файл с именем `essential_data.txt` и строкой «Важные данные» внутри файла.
9. Размонтируйте, закройте и отсоедините диск от ВМ.

На CL2

1. Подключите диск с шифрованными данными к CL2.
2. Если пакет cryptsetup не установлен, то установите его.
3. Определите ка называется шифрованный USB диск
4. Создайте виртуальное устройство для шифрованного диска
5. Смонтируйте файловую систему и прочтите в ней файл с именем `essential_data.txt`.

2.4 Управление внешними носителями.

1. Подключите к cl2 новый USB диск.
2. Создайте на нем файловую систему vfat и проверьте, что обычный пользователь может в графическом сеансе подключить этот диск и скопировать на него файл.

Здесь используется диск sdb, в вашей системе он может называться по другому.

3. Создайте группу пользователей usb-users и добавьте пользователя sa в эту группу.
4. Создайте правило UDEV, которое назначит группу usb-users на любой подключенный USB диск.
5. Перечитайте правила UDEV и проверьте как будет работать подключение USB носителя.
6. Отключите и вновь подключите USB диск. Проверьте что sa может с ним работать, а user нет.
7. Проверьте, что пользователи могут открывать оптические диски. Подключите к ВМ любой iso файл.
8. В файл `/etc/modprobe.d/blockcdroms.conf` добавьте строку с блокировкой модуля sr_mod.
9. Обновите все initrd файлы и перезагрузите машину.
10. Проверьте, что после перезагрузки оптические диски не открываются.

2.5 Отключение терминала VGA в процессе загрузки.

1. Выключите ВМ cl2 и добавьте в настройках ВМ COM порт №1, режим — TCP, путь/адрес — 54321, опцию подключения к существующему сокету — убрать. Запустите ВМ.
2. Подключитесь к порту 54321 на хосте по протоколу telnet.
3. Войдите на cl2 и активируйте консоль на первой последовательной линии.
4. Убедитесь что в telnet сессии отобразилось приглашение на вход в систему.
5. Настройте перевод вывода на первое последовательное соединение.
6. Обновите файл конфигурации GRUB.
7. Перезагрузите машину и проверьте, что теперь вывод процесса загрузки идет только на последовательную линию.

2.6 *Шифрование пользовательских данных (необязательное)

1. На CL1 проверьте, что установлен пакет cryptsetup.
2. Загрузите cl1 в однопользовательском режиме.
3. Сделайте архив пользовательских данных. Архив разместите в каталоге `/root`.
4. Настройте шифрование раздела, на котором находился каталог `/home`,
5. Опишите автоматическое подключение шифрованного раздела по паролю в `/etc/crypttab`.
6. Откройте шифрованный раздел.
7. Создайте файловую систему на открытом разделе.
8. Опишите подключение вновь созданной ФС в `/etc/fstab`.
9. Смонтируйте раздел и восстановите данные в /home.
10. Перезагрузите систему и проверьте что доступ к прежним данным пользователей восстановился.

Глава 3. Подключаемые модули аутентификации (PAM).

3.1 Настройка PAM

Задание выполняется на CL1.

1. Проверьте, что у вас установлен модуль pam_mkhomedir.so.

2. Настройте PAM на автоматическое создание домашних каталогов пользователей, используя модуль pam_mkhomedir.so.

Выбрать опцию «Create home directory on login».

3. Проверить в каком(их) файле произведена настройка.

4. Запустите команду `pam-auth-update` и проверьте, что опции для автоматической настройки модуля pam_umask нет.
5. Так же проверьте, что в файлах настройки PAM тоже нет упоминания модуля pam_umask.

6. Откройте справку по модулю и прочтите, как его настраивать.

7. В конце файла `/etc/pam.d/common-session` добавьте строку с подключением модуля.

8. Проверьте текущее значение umask пользователя user.

9. Измените описание учетной записи user, определив маску равную 0077.

10. Проверьте, что при новом входе пользователь получил значение umask, назначенное в свойствах учетной записи.

Глава 4. Аутентификация.

4.1 Учетные записи.

Задание выполняется на CL1.

1. Просмотрите файл /etc/shadow (с правами root). У всех ли пользователей содержимое второго поля выглядит приблизительно одинаково или же у некоторых пользователей имеются существенные отличия от записей для других пользователей?
2. Какие символы могут содержаться шифрованной строке пароля во втором поле файла /etc/shadow ?
3. Используя текстовые утилиты выведите таблицу, содержащую имена пользователей, их UID и GID, а также шифрованный пароль (необходимо иметь права root). Таблица должна содержать записи только для пользователей имеющих шифрованные пароли длиной более 10 символов.

4. Зарегистрируйте пользователя test1, для которого запрещен вход в сеанс, имеющего домашний каталог /var/spool/mail, и являющегося членом групп users и mail. Пользователь должен иметь UID=1100.

5. Создайте учетную запись для пользователя test2 с настройками по умолчанию, но без создания приватной группы. Проверьте создался ли домашний каталог пользователя, если да, то наполнен ли он файлами, и кому он принадлежит.

Домашний каталог в Debian автоматически не создается.

6. Измените имя пользователя test2 на test3.

7. Откройте сеанс для пользователя test3 через su или sudo. При входе должен быть создан домашний каталог. Затем закройте сеанс.

8. Какой каталог был создан для пользователя test3. Исправьте в настройках пользователя путь к домашнему каталогу.

9. Получите идентификаторы пользователя test3.

10. Удалите пользователя test3. И проверьте кому теперь принадлежат каталоги /home/test2 и /home/test3.

11. В файле `/etc/default/useradd` измените значение переменной `SHELL` на `/bin/bash`

12. В файле `/etc/login.defs` создайте переменную которая настраивает автоматическое создание домашних каталогов пользователей при их добавлении.

13. Зарегистрируйте пользователя test4 с настройками по умолчанию. Какая оболочка установлена для test4. Проверьте появился ли домашний каталог. Кому принадлежат каталоги вида test*.

14. Получите идентификатор пользователя test4 и сравните его с тем, что был у test3.

15. Установите пароль для test4 . Изучите содержимое соответствующей пользователю записи в файле `/etc/shadow`.

16. Установите дату устаревания учетной записи test4 на 31 декабря текущего года. Проверьте, что изменилось в `/etc/shadow`.

17. Удалите пароль пользователя и проверьте изменения в `/etc/shadow`.

18. Попробуйте войти пользователем test4. Пускает ли система без пароля?

19. Запретите вход с пустыми паролями.

20. Заблокируйте учетную запись test4.

4.2 Качество паролей

Задание выполняется на CL1.

1. Установите пакеты libpwquality-tools и libpam-pwquality.

2. Придумайте свой пароль и проверьте его на сложность.

3. Попробуйте сгенерировать несколько паролей автоматически и сравните их сложность со своими паролями.

4. Проверьте в каких файлах PAM используется модуль pam_pwquality.

5. Настройте политику в отношении паролей: минимальная длина — 8, повторение имени пользователя не более чем в 4 символах, минимальное количество классов — 3, максимум повторений одного символа — 2, только для локальных пользователей.

6. Установите пароль lin123 от имени суперпользователя пользователю test4.

7. Попробуйте изменить пароль пользователем test4 на tesQ1w2e3r4, test1234/ и Lin1234/

4.3 Блокировка учетных записей.

1. Включите модуль pam_faillock.

2. Настройте блокировку учетных записей на 30 мин при 5 неудачных попытках входа локального пользователя. Суперпользователь тоже должен блокироваться, но на 5 минут.

3. Установите программу John The Ripper и подберите пароли для пользователя user. Используйте имеющийся словарь из пакета john-data. Пароль lin123 добавьте в словарь после строки qwerty.

4. *(Дополнительное). Установите пакет hydra. Установите пакет vsftpd. Запустите службу ftp. Отключите блокировку учетных записей и подберите пароль для пользователя user.

4.4 Группы.

1. Создайте группу пользователей xusers с GID 1010.

2. Зарегистрируйте пользователя user в качестве участника группы xusers.

3. Используя утилиту `groupmod`, позволяющую изменять имена и GID групп. Измените имя группы на yusers.

4.5 Политики sudo.

1. Разрешите пользователю user выполнять команду passwd через утилиту sudo, для смены пароля любому пользователю кроме root.

4.6 Профили пользователей.

1. Измените значение umask на 027 для всех пользователей системы по умолчанию.

2. Установите в собственном профиле оболочки псевдоним ll для команды ls -l.

3. Каким образом сделать так, чтобы этот же псевдоним устанавливался и для всех вновь регистрируемых пользователей в системе, для которых оболочкой по умолчанию будет Bash?

4. В каком файле удобнее всего добавить к переменной окружения PATH путь к каталогу bin, находящемуся в домашнем каталоге обычного пользователя?

5. Добавить на рабочий стол для всех новых пользователей ярлык для запуска браузера Firefox.

4.7 Активность пользователей.

1. Определите, когда была последний раз загружена система.
2. С помощью опции `-a` команды `who` получите подробную информацию о пользователях и статусе системы.
3. С помощью команды who получите список пользователей, входивших в сеанс ранее.
4. Сравните предыдущий список со списком, выводимым командой `last`.
5. Получите отчет по входам в сеанс суперпользователя с помощью `lastlog`.
6. Кто входил в сеанс за последние пять дней?
7. Получите список активных сеансов.
8. Получите подробную информацию о статусе одного из сеансов. Какие процессы там запущены?
9. Заблокируйте и разблокируйте сеанс с графическим входом из другого терминала.
10. Попробуйте заблокировать сеанс в текстовом терминале.
11. Завершите сессию в графическом терминале. После закрытия сессии посмотрите какая сессия откралась на этом терминале.

Глава 5. Доступ к файлам.

5.1 Создание папки для общего доступа

Задание выполняется на srv1.

1. От имени суперпользователя создайте каталог `/home/project`.
2. Добавьте пользователей user1, user2 и user3.
3. Создайте группы RW_project и RO_project.
4. Добавьте пользователей user1 и user2 в RW_project, а пользователя user3 в RO_project.
5. Добавьте пользователя sa в группу adm.
6. Назначьте SGID на каталог `/home/project`, и права доступа 770.
7. Сделайте группу adm владельцем каталога `/home/project`.
8. Пользователем sa создайте в каталог `/home/project/d1` и файл `f1` в нем.
9. Проверьте права доступа на содержимое `/home/project`.
10. Создайте ACL для каталога `/home/project` так чтобы пользователи в группе RW_project имели права rw, а RO_project — r. Остальные пользователи никаких прав иметь не должны.
11. Проверьте распространяются ли права доступа каталога `/home/project` на `d1` и `f1`.
12. Перенесите ACL с каталога `/home/project` на все его текущее содержимое.
13. Пользователем user1 создайте в каталог `/home/project/d2` и файл `f2` в нем.
14. Получилось ли создать файлы? Если получилось, то какие права доступа получились у файлов и каталогов?
15. Установите ACL по умолчанию (default ACL) на каталог `/home/project` так, чтобы члены групп RW_project, RO_project и adm получали правильные права доступа на вновь создаваемые объекты.
16. Пользователем user1 создайте в каталог `/home/project/d3` и файл `f3` в нем.
17. Какие права доступа получились у новых файлов и каталогов?

18. Проверьте есть ли наследуемые ACL на каталоге `/home/project/d1`.

19. Перенесите ACL с каталога `/home/project` на все его текущее содержимое.

20. Проверьте, что теперь обычные файлы имеют права на исполнение. Исправьте это.

5.2 Специальные биты доступа.

1. Проверьте, какие биты прав доступа установлены на исполняемый файл команды passwd.

2. С помощью `ps` и `awk` получите список всех процессов в системе, для которых RUID не равен EUID.

3. На какой-либо виртуальной консоли запустите команду passwd от имени обычного пользователя. Выполните ту же команду, что и в предыдущем пункте. Имеется ли в требуемом списке процесс passwd?

4. Используя `find` запишите в файл `SUGID.txt` все имена файлов, на которые установлены биты SUID или SGID.

5. Найдите в `/home` все каталоги с установленными битами SGID или Sticky bit.

5.3 Дополнительные атрибуты файлов.

1. Создайте в домашнем каталоге подкаталог dir с файлами 1.txt, 2.txt, 3.txt

2. Установите атрибут a для 1.txt, i для 2.txt и c для 3.txt

3. Попробуйте выполнить с файлами следующие операции: добавить информацию в файлы, перезаписать содержимое, удалить файлы.

Глава 6. Модули безопасности Linux.

6.1 SELinux.

Задание выполняется на srv1.

1. Установите пакеты selinux-basics, selinux-policy-default, selinux-utils и auditd.
2. Выполнить команду `selinux-activate`, которая настроит GRUB, PAM и создаст файл `/.autorelabel`.
3. Перезагрузите ОС.
4. Проверьте установку командой `check-selinux-installation`.
5. Проверьте состояние SELinux. Если оно выключено, то включите его или переведите в режим enforcing.
6. Установите веб-сервер apache и проанализируйте как промаркированы файлы этой службы.
7. В файл `/var/www/html/index.html` запишите одну строку: Default Site. Убедитесь, что веб-сервер показывает стартовую страницу.
8. Создайте алиас для каталога `/home/myweb`, поместите в этот каталог файл `index.html` и проверьте доступна ли эта страница. На данном этапе страница не должна быть доступна.
9. Сделайте временную перемаркировку файлов для веб-сервера и проверьте доступ к странице алиаса.
10. Восстановите маркировку по умолчанию для `/home`. Проверьте доступность страницы.
11. Создайте постоянное правило маркировки примените эти правила к каталогу `/home/myweb`. Убедитесь, что правила маркировки отработали правильно и доступ к алиасу восстановился.
12. Разрешите сетевое подключение веб-сервера к базам данных.
13. Проанализируйте журнал аудита и примите решение по устранению отказов в доступе. Стоит ли их принять, проигнорировать или исправить политики или настройки политик. Если необходимо внесите нужные изменения.

6.2 *Создание модуля SELinux. Правила RBAC (необязательное).

1. Создайте собственный модуль для SELinux. (По примеру в учебнике).
2. Скомпилируйте и установите модуль.
3. Включите модуль.
4. Удалите свой модуль.
5. Создайте нового Unix пользователя и сопоставьте его с SELinux пользователем `staff_u`. Проверьте какие операции может выполнять данный пользователь.
6. Создайте SE пользователя `webadm_u`, связанного с ролью `webadm_u`. Затем Unix пользователя webadm, связанного с `webadm_u` и проверьте его привилегии.
7. Измените SELinux пользователя для учетной записи администратора на `user_u`. Проверьте действует ли изменение на работу от имени обычного и суперпользователя.

После выполнения лабораторных работ отключите SELinux!

```
$ sudo setenforce 0
$ sudo selinux-activate disable
$ sudo reboot
```

6.3 AppArmor

Выполняется на cl1.

1. Установите пакеты apparmor, apparmor-utils, apparmor-profiles, apparmor-profiles-extra.
2. Скопируйте программу `ping` в домашний каталог пользователя.
3. Проверьте, что копия `ping` работает. Если не работает, то назначьте linux capabilities cap_net_raw=ep на этот файл.
4. Создайте профиль AppArmor для копии программы `ping`.
5. Проверьте, что копия `ping` работает.
6. Переключите профиль в принудительный режим. Теперь `ping` должен перестать работать.
7. С помощью `aa-genprof` настройте профиль, чтобы он разрешал использование копии `ping`.

Глава 7. Мониторинг событий безопасности средствами ОС Linux.

7.1 Работа с журналами.

1. Проверьте установлен ли пакет rsyslog на машинах. Если нет, то установите его на всех ВМ. Далее почти все действия выполняются на srv1 на cl1 и cl2 настраивается только клиенты syslog.
2. Создайте в конфигурации демона rsyslog строку, которая заставит его записывать сообщения от источника auth с уровнем важности не ниже info в файл `/var/log/mylog` .
3. Добавьте в конце файла `/etc/rsyslog.conf` строку:

4. Определите, какой сигнал позволяет демону rsyslog перечитать файл конфигурации и продолжить работу с измененными настройками. Пошлите демону этот сигнал и проверьте, создался ли файл `/var/log/mylog` .

5. Проверьте, записываются ли в этот файл сообщения при входе в сеанс и выходе из него пользователей.
6. Создайте аналогичный журнал `/var/log/mylogpriv` для записи сообщений от источника authpriv . Проверьте его работоспособность. Записываются ли в него те же сообщения, что и в предыдущий журнал?

7. Настройте прием сообщений по протоколу UDP на srv1 и запись таких сообщений в отдельные журналы для каждого узла.
8. Удобней будет создать отдельный файл конфигурации, например `/etc/rsyslog.d/udp.conf` и в нем описать следующие строки:

9. На cl1 и cl2 настройте перенаправление событий на ваш srv1. И протестируйте работу службы.

10. Посмотрите журнал загрузки системы.
11. Попробуйте воспользоваться опцией -l видите ли вы разницу? Если нет, то как увидеть?

12. Настройте systemd вести постоянные журналы.

13. Создайте настройки ротации для журналов `/var/log/mylog` и `/var/log/mylogpriv`, созданных ранее. Файлы должны ротироваться ежедневно. Ротация первой копии должна осуществляться два раза. Ротируемые копии должны сжиматься утилитой gzip.
14. Создать новый файл `/etc/logrotate.d/mylog` со следующим содержимым:

15. Для файла `/var/log/mylog` установите в качестве дополнительного условия ротации достижение им размера 10 Кб.
16. Изменить файл `/etc/logrotate.d/mylog` следующим образом:

17. Создайте правила ротации журналов с сообщениями, поступающими из сети. Параметры ротации — ежедневно, 7 копий, со сжатием 2 копии, суффикс в виде даты.

18. Настройте автоматическую ротацию журнала `/var/log/messages`, посредством исходящих сообщений rsyslog. Для ротации используйте logrotate с отдельным конфигурационным файлом. Размер журнала для ротации 1MB.

19. Настройте блокировку учетной записи пользователя, который выполняет не разрешенные команды sudo.

20. Настройте rsyslog на запись IP адреса, с которого производится попытка входа по протоколу ssh пользователем root в файл `/var/log/badips.log`.

21. *Установите пакет logwatch и просмотрите отчет о функционировании вашего компьютера.
22. *Настройте получение статистики от web-серверас помощью webalizer.
23. *Установите пакет webalizer. И изучите файл конфигурации /etc/webalizer/webalizer.conf. Обратите внимание на опции конфигурации LogFile и OutputDir.

7.2 Аудит.

1. Проверьте запущен ли демон аудита.
2. Проверьте его настройки.
3. Создайте правило для отслеживания обращений к файлу `/etc/shadow` и `/etc/passwd`.
4. Перезапустите аудит и проверьте, что правила не сохранились
5. Опишите ваши правила в конфигурационном файле.
6. Проверьте регистрируются ли события когда вы добавляете нового пользователя или меняете пароль.

Глава 8. Защита сетевых взаимодействий.

8.1 Подготовка ВМ.

1. Выключите ВМ SRV1.
2. Добавьте к SRV1 второй адаптер, который подключен во внутреннюю сеть с именем netXX, где XX — номер, который вам назначил преподаватель. После включите ВМ.
3. Определите (по MAC) как называются сетевые интерфейсы внутри ВМ SRV1.
4. Удалите все соединения кроме lo в NetworkManager и настройте интерфейсы так, чтобы внешний интерфейс получал адрес от DHCP, а на внутреннем был назначен статический адрес 10.1.1.1/24.

8.2 Фильтрация пакетов

1. Проверьте текущие правила фильтрации
2. Создайте таблицу для фильтрации ip пакетов.
3. Добавьте в таблицу базовую цепочку с именем input для входящего трафика.
4. Добавьте в таблицу регуляную цепочку с именем SSH-IN.
5. Разрешите в цепочке input любые пакеты, которые относятся к установленным соединениям.
6. Разрешите любой входящий трафик на интерфейсе lo в цепочке input, который идет с адресов сети 127.0.0.0/8. И запретите любой другой трафик.
7. Настройте прыжок из цепочки input в SSH-IN, когда приходит пакет на порт 22.
8. Разрешите входящий трафик для сервера SSH с адресов сетей 127.0.0.0/8 и 10.1.1.0/24. Остальные пакеты должны быть запрещены.
9. Можете ли вы теперь открыть какую-нибудь веб страницу в интернете? И почему?
10. Создайте файл с именем `nft.rules` записав в него строку flush ruleset.
11. Допишите в это же файл текущие правила.
12. Сделайте копию файла `nft.rules` и в копии за комментируйте строку с разрешением установленных соединений и измените политику цепочки input на drop. Потом примените правила. Можете ли вы открыть какой-либо сайт в браузере?
13. В исходном файле `nft.rules` добавьте счетчики к правилам в цепочке SSH-IN. Примените эти правила.
14. На SRV1 попробуйте подключиться по ssh к адресам 127.0.0.1 и 10.1.1.1. Оба ли подключения удались?
15. Добавьте еще одно правило, которое разрешает подключаться с адреса 10.1.1.1 на интерфейс lo.

16. Проверьте состояние счетчиков.

17. CL1 и CL2 подключите в ту же сеть в VirtualBox, что и второй адаптер SRV1. Настройте адреса соответственно 10.1.1.11/24 и 10.1.1.12/24. Шлюз по умолчанию 10.1.1.1. DNS сервер такой же как указан в файле `/etc/resolv.conf` на srv1.
18. Подключитесь с cl1 или cl2 на srv1 (10.1.1.1) по SSH. Проверьте, что счетчики начали увеличиваться согласно количеству попыток подключения.

19. Проверьте что ни cl1 ни cl2 не могут выйти в интернет.

8.3 NAT.

1. Очистите все правила на srv1.
2. Включите пересылку пакетов на srv1.
3. Добавьте таблицу с именем NAT.
4. В таблицу NAT цепочку типа nat, хуком postrouting и именем s-nat.
5. В цепочку s-nat добавьте правило для маскарадинга всех пакетов из сети 10.1.1.0/24 и исходящих с внешнего интерфейса.
6. Проверьте, что cl1 и cl2 могут выходить в интернет.
7. Опубликуйте службу SSH на cl1 и cl2 с портами соответственно 22011 и 22012 на srv1.
8. Сохраните текущие правила фильтрации в файл `/etc/mynftd.rules`.
9. Создайте скрипт, который будет управлять правилами фильтрации с именем `/usr/local/sbin/mynftd`, сделайте файл исполняемым.
10. Создайте службу systemd, которая будет запускать `/usr/local/sbin/mynftd` во время старта ОС.

8.4 *Firewalld (необязательное).

1. Остановите сервис mynftd. И запретите его запуск.
2. Если сервис firewalld еще не установлен, то установите и запустите его.
3. Посмотрите какие имеются зоны. Какие интерфейсы в этих зонах и какие службы могут сейчас работать.
4. Переопределите внутренний интерфейс в зону work. Какие теперь службы разрешены?
5. Переведите внешний интерфейс в зону external.
6. Дайте разрешение для всех служб и портов, которые вам необходимы.
7. Настройте NAT маскарадинг. Проверьте, что cl1 и cl2 могут выходить в интернет.
8. Остановите и запретите запуск службы firewalld.
9. Вновь включите и запустите службу mynftd. Проверьте, что клиенты могут выходить в интернет.

8.5 Прокси сервер squid.

1. Остановите службу mynftd. Проверьте, что cl1 и cl2 не могут выходить в интернет.
2. Установите прокси сервер squid на srv1.
3. Сохраните исходный файл конфигурации squid и создайте новый удалив все строки с комментариями и повторяющиеся строки.
4. Создайте ACL для адресов источника с именем mynet и адресом 10.1.1.0/24 и предоставьте доступ к интернету для этого списка. Удалите ACL localnet.
5. Настройте клиентов для работы с прокси сервером.
6. Определите URL ACL с регулярным выражением google. Запретите доступ к страницам подпадающим под действие созданного ACL
7. Установите максимальный размер запроса клиента равным 10кб.
8. Установите ограничение скорости получения информации для файлов с расширением zip на величину 100кбит/с.
9. Настройте базовую аутентификацию на вашем сервере.

]

10. Отключите аутентификацию, запрет google и пулы задержки.
11. Запустите службу mynftd. Проверьте, что cl1 и cl2 могут выходить в интернет.

8.6 SSH.

1. Проверьте установлена ли и запущена служба SSH.

2. Проверьте работоспособность команд `ssh` и `scp`.

3. Создайте пару ключей RSA и поместите публичный ключ на желаемый сервер. Оставьте парольную фразу пустой - в таком случае при успешном обмене ключами вводить пароль для доступа к удаленному узлу не буде требоваться (но сам ключ будет не защищен).

4. Защитите созданный ключ паролем.

5. Проверьте, что теперь при каждом входе на сервер у вас будут спрашивать пароль для разблокирования ключа.
6. Войдите в систему в графический сеанс и запустите эмулятор терминала. Добавьте частный ключ в связку ключей ssh агента. Пароль будет запрошен только один раз в момент добавления ключа.

7. Войдите в систему не используя графического сеанса и проверьте, что агент в этом случае недоступен.

8. Настройте запуск ssh агента:

9. Запретите вход пользователю root с помощью пароля.

10. Измените порт 22 на порт 33322.

11. Настройте клиентскую машину так, чтобы она по молчанию подключалась к серверу по порту 33322.

12. *Установите пакет fail2ban и настройте блокировку адресов, которые пытаются подобрать пароль пользователей по ssh.

Глава 9. Инфраструктура открытых ключей на основе openssl.

9.1 Создание CA.

1. В качестве корневого CA будет использоваться srv1.
2. Создайте сертификат корневого CA.

3. Добавьте сертификат вашего CA в список доверенных

9.2 Использование сертификатов.

1. Запросите сертификаты для srv1 с именами srv1, srv1.class.itcloud и для IP адреса 10.1.1.1.

2. Создайте сертификаты для cl1 и cl2. Альтернативные имена cl1 и cl2 и IP адреса 10.1.1.11 и 10.1.1.12.
3. Настройте защищенное с помощью stunnel соединение между cl1 и cl2 с использованием ранее полученных сертификатов. Cl1 — сервер.

4. Настройте работу веб сервера apache на srv1 для работы с ранее полученными сертификатами.

Глава 10. Безопасность уровня приложений.

10.1 Контейнеры Docker.

Задание выполняется на cl1.

1. Установите инструменты для работы с контейнерами Docker.

2. Добавьте пользователя sa в группу docker, чтобы разрешить ему управлять контейнерами.

3. Найдем образ с веб-сервером (Nginx или Apache).

4. Запустите это приложение и проверьте работу веб-сервера.

5. Настройте запуск контейнера так, чтобы он показывал содержимое каталога `~/web8080`. Контейнер должен удаляться после остановки.

6. Сделайте еще один контейнер, который запускает веб сервер на порту 8888 и работает с каталогом `~/web8888`.

10.2 Контейнеры LXD.

Задание выполняется на cl2.

1. Установите пакеты для работы LXD.
2. Произведите первоначальную настройку.
3. Проверьте источники, с которых вы можете получить образы.
4. Добавьте еще один удаленный репозиторий.

Для сравнения:

5. Запустите контейнер с ОС Debian 12 и именем deb12-container.
6. Войдите в контейнер и создайте в нем файл.
7. Выключите контейнер и найдите файл, который вы создали внутри контейнера.
8. Вновь запустите контейнер и проверьте содержимое файла.
9. Установите на контейнер deb12-container ограничения: 1Гб памяти и 1 ядро.
10. Проверьте конфигурацию контейнера.
11. Перезагрузите cl2 и проверьте запустится ли контейнер во время старта хостовой ОС.
12. Установите параметр boot.autostart в значение true.

Глава 11. Поддержание системы в актуальном состоянии.

11.1 Установка обновлений.

1. Обновите локальный кэш репозиториев. Посмотрите сколько пакетов может быть обновлено.

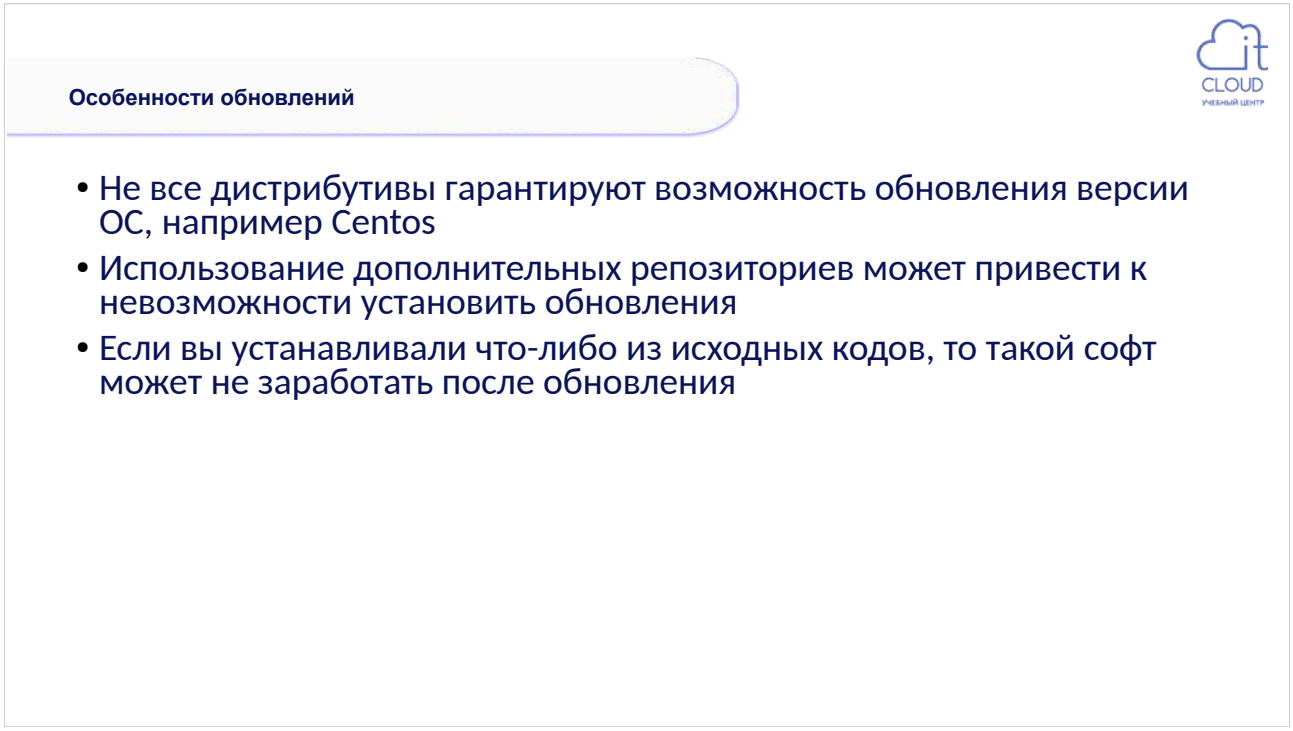
2. Получите список пакетов, которые можно обновить.

3. Проверьте имеются ли обновления для ядра.

4. Установите обновления без удаления пакетов.

5. Закончите установку обновление с удалением пакетов.

6. Если обновлялось ядро, то перезагрузите систему.



В работе с обновлениями могут возникнуть трудности. Которые надо заранее учитывать перед запуском обновления.

Не всегда гарантирована возможность обновить версию ОС. Например Centos не гарантирует, что вы сможете выполнить обновление версии с 6 на 7 или, что после обновления у вас не возникнут трудности. В других ОС процесс обновления версии хорошо отработан и почти всегда проходит без осложнений. Но надо помнить, что изменение версии это всегда повышенный риск того, что у вас что-нибудь после обновления не заработает.

Если вы используете нестандартные репозитории, то нет гарантии что обновления не вызовут проблем. Майнтайнеры этих репозиториев не всегда могут отследить изменения в дистрбутивах, для которых они публикуют свои пакеты.

Еще одна потенциальная проблема это софт, который был установлен из исходных кодов. Обновления могут нарушить нормальное функционирование таких программ.

Для предупреждения таких проблем необходимо тестировать обновления на непроизводственных системах. Необходимо разрабатывать план установки обновления, а так же план аварийного восстановления на случай, если обновление будет неудачным.

Глава 12. Контроль целостности.

12.1 Rkhunter.

1. Установите rkhunter.
2. Проверьте систему на наличие руткитов.

12.2 Samhain.

Задание выполнять на cl1.

1. Установите samhain.
2. Создайте baseline.
3. Внесите изменения в файл `passwd` (добавьте нового пользователя) и проверьте систему.

12.3 AIDE.

Задание выполнять на cl2.

1. Установите aide.
2. Создайте и активируйте базу.
3. Внесите изменения в файл `hosts` и проверьте систему.

Глава 13. Контроль защищенности Linux – систем.

13.1 Scap-workbench.

1. Установите scap-workbench.
2. Установите scap-security-guide .
3. Проведите сканирование системы.

13.2 oscap.

1. Установите пакеты openscap-scanner, openscap-utils и bzip2.
2. Скачайте документ с описанием рекомендованных настроек системы, в формате OVAL (Open Vulnerability and Assessment Language).

3. Запустите проверку:

4. Проверьте результат сканирования.