МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

РТУ МИРЭА

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Практическая работа № 3

«Установка и настройка операционной системы Linux. Методы обеспечения безопасности ОС»

по дисциплине «Безопасность операционных систем»

Москва

2023

1.1. Подготовка учебного стенда. Установка ОС Linux на виртуальную машину

Порядок выполнения работы:

1. Установка Virtual Box

Скачайте дистрибутив для своей операционной системы и установите Oracle Virtual Box актуальной версии.

https://www.virtualbox.org/wiki/Downloads

2. Установка виртуального образа Linux

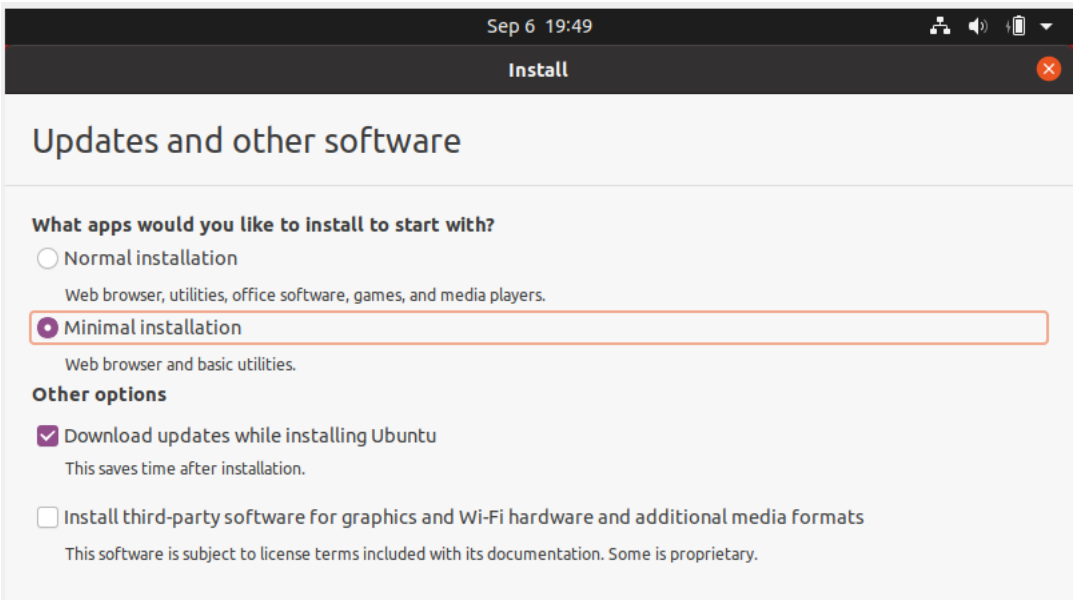
Для выполнения работы нам подойдет любой дистрибутив Linux. Наиболее популярные можно скачать по ссылкам.

CentOS7: http://mirror.yandex.ru/centos/7.9.2009/isos/x86_64/CentOS-7-x86_64-DVD-2009.iso

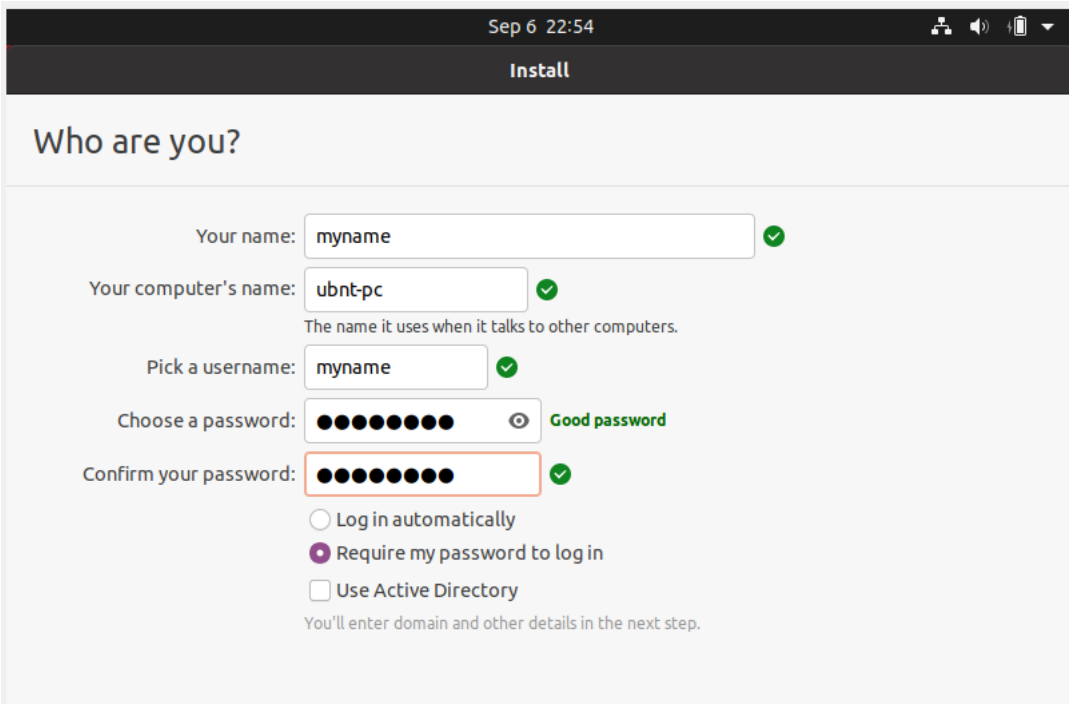
Ubuntu 20.04 LTS: https://releases.ubuntu.com/focal/ubuntu-20.04.6-desktop-amd64.iso

Для создания виртуальной машины выберите скачанный образ в VirtualBox, настройте необходимые параметры: **установите галочку пропустить автоматическую установку**, имя создаваемой машины, объем оперативной памяти (мин. 2Гб), объем жесткого диска (мин 25Гб) и запустите установку.

Далее выбираем параметры установки, рекомендуется указать минимальный набор устанавливаемого ПО



Далее продолжаем по-умолчанию до указания информации о пользователе ОС



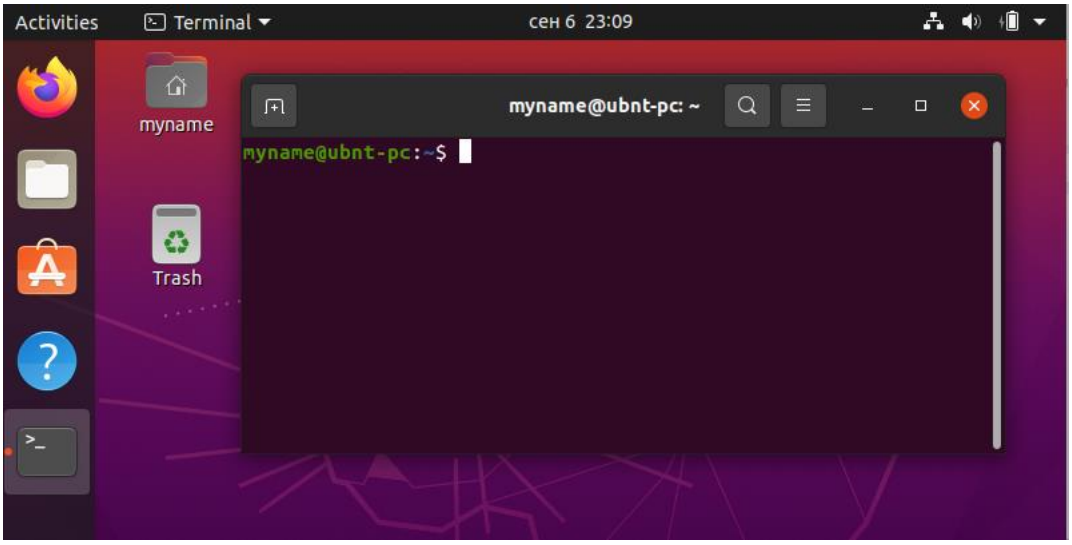
Заполняем (*добиваясь поощрения при установке пароля, влияет на балл*) и продолжаем установку. После установки необходимо выполнить перезагрузку ВМ.

Отчёт:

- Задайте сложный пароль пользователю при установке ОС (screenshot).

1.2. Управление пользователями и обновление ОС

Запустите терминал управления ОС: *ctrl+alt+t*



В ОС Linux администратором является пользователь root, который создается автоматически и по соображениям безопасности под ним нельзя авторизоваться и его использование ограниченно. Вся работа ведется под обычным непривилегированным пользователем, а для выполнения действий, требующих прав администратора ОС, используется утилита sudo.

Познакомьтесь с утилитой sudo вызвав краткое описание утилиты, выполнив в терминале команду *sudo –h*

или прочитав справочную информацию по ней, с помощью команды *man sudo*

Эти же команды можно использовать для изучения других утилит.

Для поддержания безопасности ОС необходимо регулярно производить обновление системы и установленного ПО, с помощью команд

apt update - обновление репозиториев

apt upgrade - обновление пакетов

Утилита apt используется не только для обновлений, но и для установки ПО, давайте установим набор утилит для виртуализации выполнив команду:

apt install open-vm-tools

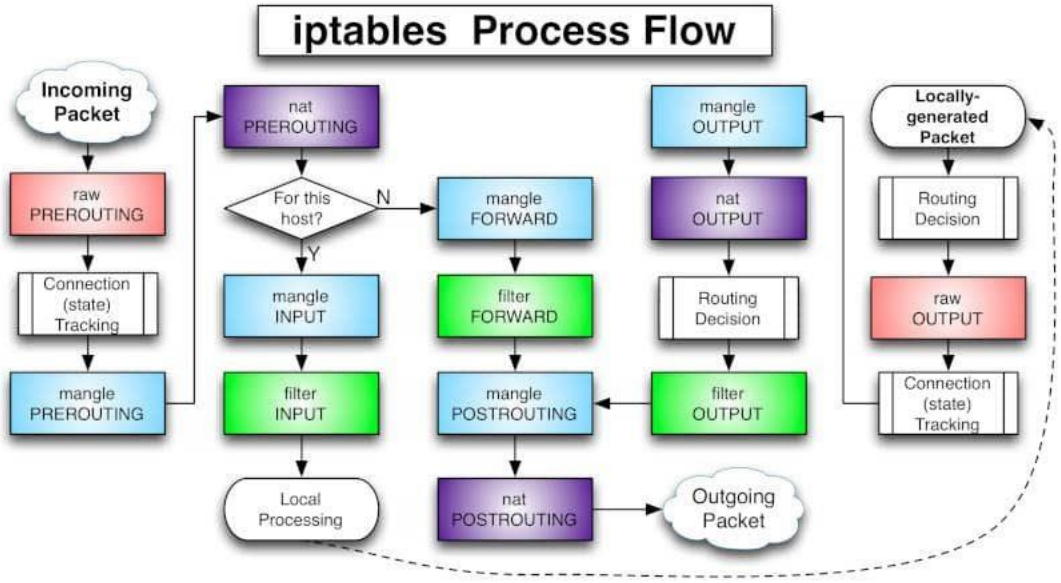
Отчёт:

- Задайте сложный пароль пользователю при установке ОС (screenshot).
- описание утилиты sudo;
- описание утилиты apt;
- с помощью утилиты useradd добавьте нового пользователя user-baso-0*-21-fio* и авторизуйтесь под ним (скриншот)

1.3. Знакомство с локальным межсетевым экраном

Важным аспектом обеспечения безопасности любой системы является межсетевой экран. Управление межсетевым экраном в Linux выполняется утилитой iptables. IPTables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux, начиная с версии 2.4. Для использования утилиты iptables требуются привилегии суперпользователя (root). Ознакомьтесь с параметрами утилиты самостоятельно.

На рисунке представлен принцип работы iptables



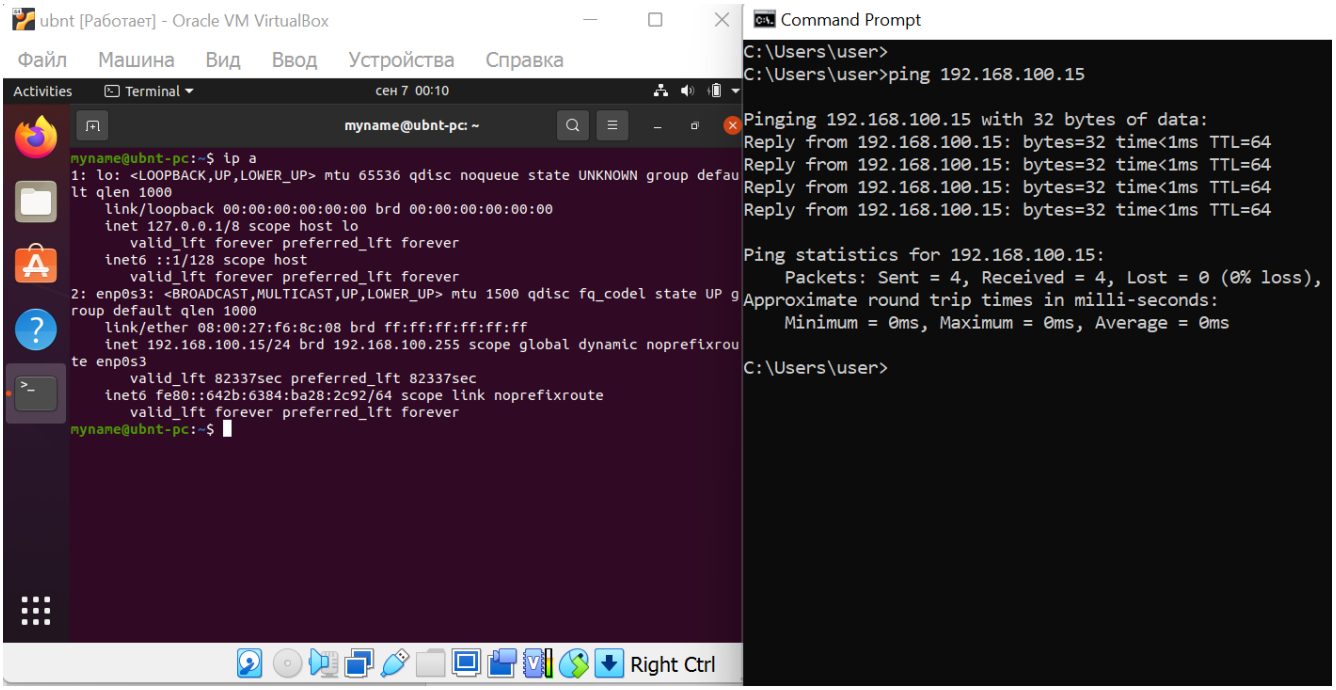
Посмотрим уже имеющиеся правила iptables командой:

iptables -L -n –v или *iptables –vnL*

Прежде чем изменять правила, рекомендуется сохранить их, например, командой

iptables-save > iptables.txt

Давайте добавим правило запрещающее входящий трафик по протоколу icmp. Проверим что он разрешен, «пропинговав» нашу ВМ с хоста

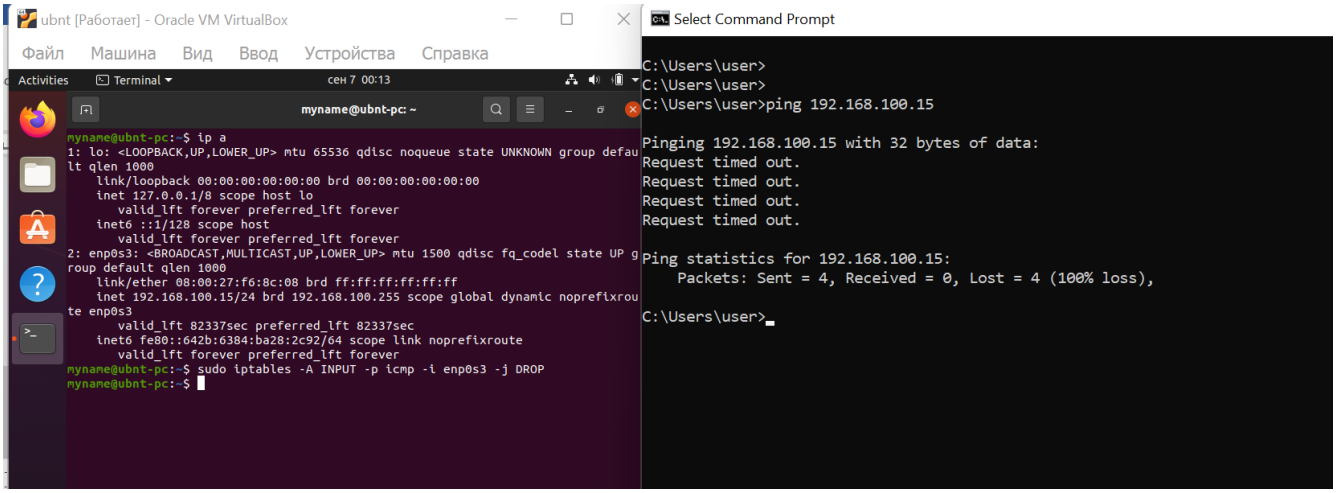


Добавим правило на запрет входящего трафика протокола icmp:

iptables -A INPUT -p icmp -i enp0s3 -j DROP

Добавить правило можно с помощью текстового редактора, например, *nano* добавив правило в файл полученный при выполнении команды *iptables-save*. Далее необходимо применить правила из файла командой *iptables-restore*.

Проверим правило, пропинговав нашу ВМ с хоста



Отчёт:

- описание утилиты *iptables* (цепочки, действия, возможности);
- результат команды *iptables -L -n –v* (скриншот);
- восстановите правила межсетевого экрана по-умолчанию (скриншот).

1.4. Журналирование в Linux

Журналы системы — это важнейший компонент безопасности ОС. Они содержат информацию о том, кто и когда пытался войти в систему, а также о результатах этих попыток. Операционная система или приложение должны в обязательном порядке рассказывать о своей жизни: регистрировать входы в систему, сбои, ошибки и другие значительные события.

По умолчанию события журналируются в каталог /var/log/. В нем имеется множество различных *.log файлов содержащих события от различных источников в текстовом виде. Просмотрите этот каталог командой

ls, для отображения в виде списка используйте параметр *–l*

Файлы /var/log/syslog или /var/log/messages — глобальный системный журнал. В нем мы можем найти события, произошедшие с момента запуска системы от различных компонентов ОС — ядра, служб, устройств и т. д.

Журнал событий var/log/kern.log — содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок, произошедших при работе пользовательских модулей, встроенных в ядро.

События от оборудования и драйверов устройств находятся в файле /var/log/dmesg. В этом файле фиксируются ошибки работы драйверов и оборудования.

События установки системы можно найти в файле /var/log/anaconda.log, а в файле /var/log/boot.log находятся логи загрузки системы.

Журнал демона crond /var/log/cron — содержит результаты выполнения различных событий планировщика задач cron.

Журналы /var/log/auth.log или /var/log/secure — наиболее интересны для безопасников, так как они содержат информацию об авторизации пользователей, то есть попытки не/успешных входов в систему и методов аутентификации.

Еще один журнал событий, который представляет особый интерес для специалистов по информационной безопасности это /var/log/audit — лог демона auditd.

Рассмотрим несколько утилит работающих с журналами авторизации пользователей

last – получение данных о последних входах в систему

lastlog – просмотра журналов последней успешной аутентификации пользователей

lastb – получение данных о неудачных попытках входа в систему

w – получение данных о текущих сессиях

Рассмотрим утилиту управления журналированием *journalctl*. Сначала ознакомимся с конфигурационным файлом, он расположен в */etc/systemd/journald.conf*. Внесем некоторые изменения для настройки ротации логов:

Для начала нужно проверить наличие директории */var/log/journal*, если она отсутствует, то ее необходимо создать.

Storage=persistent включаем постоянное хранение логов;

SystemMaxUse=1G максимальный объем который логи могут занимать на диске;

SystemKeepFree= объем свободного места, которое должно остаться на диске после сохранения логов;

SystemMaxFileSize=50M объем файла лога, по достижении которого он будет удален с диска.

Теперь можно искать необходимую информацию:

journalctl --list-boot

journalctl --since "2023-09-28 14:00:00"

journalctl --since "2023-09-28 14:00:00" –until "2023-09-28 14:05:00"

journalctl –u gdm

journalctl /usr/bin/bash

journalctl | grep user-baso-0-21-fio**

journalctl -f

Подробнее с возможностями утилиты можно ознакомиться в справке *man journalctl*.

В system также предусмотрены специальные компоненты для организации централизованного хранения логов с удаленных хостов.

Отчёт:

- опишите разницу между утилитами last и lastlog;
- продемонстрируйте логи о подключениях пользователя user-baso-0*-21-fio* (скриншот)
- выведите на экран консоли файл настроек journalctl (скриншот)

1.4. Резервное копирование в Linux

Резервное копирование на Linux системах всегда важно для предотвращения потери данных. Поэтому ознакомление с различными инструментами резервного копирования очень важно, особенно для системных администраторов, которые работают с большими объемами важных данных.

Всегда полезно сохранять резервные копии данных, это можно делать вручную или настроить автоматическое выполнение. Многие средства резервного копирования имеют разные функции, которые позволяют пользователям настраивать тип резервного копирования, время резервного копирования, протоколирование операций резервного копирования и др.

Рассмотрим несколько методов резервного копирования в Linux.

Tar

tar утилита для создания и редактирования архивов в ОС Linux. Воспользуемся ей для выполнения процедуры создания резервной копии ОС:

1. перемещаемся в корневой раздел cd /
2. переходим к копированию системы. Здесь важно исключить разделы /proc /lost+found /sys, как и сам архив /backup.tgz: *tar cvpzf backup.tgz –exclude=/proc –exclude=/lost+found –exclude=/backup.tgz –exclude=/mnt –exclude=/sys –exclude=/web /*
3. Посмотрим на созданный архив: *ls –l /*

Для восстановления выполняем загрузку с диска Live CD Linux и распаковываем наш архив в корень /.

Rsync

Это средство резервного копирования командной строки, популярное среди пользователей Linux, особенно системных администраторов. Оно обладает богатыми возможностями, включая инкрементное резервное копирование, обновление всего дерева каталогов и файловой системы, как локальных, так и удаленных резервных копий, сохранение прав доступа к файлам, ссылок и многое другое.

Также имеет графический пользовательский интерфейс Grsync, но главное преимущество Rsync заключается в том, что резервные копии могут быть автоматизированы с использованием сценариев и заданий в **cron**.

cron это планировщик задач в Linux системах.

Пример резервного копирования директории /tmp с помощью rsync:

rsync –a /tmp/ /home/user/tmp_backup

добавим исключение директории из резервной копии

rsync –a –exclude=snap-private-tmp /tmp/ /home/user/tmp_backup_exclude

Сравните результаты.

Подробнее с возможностями утилиты можно ознакомиться в справке *man rsync*.

Отчёт:

- Создайте резервную копию файла passwd в директории root, с помощью утилиты rsync (screenshot).
- Создайте резервную копию директории /var/log/ в корневой директории, с помощью утилиты tar (screenshot).
- Создайте с помощью утилиты rsync резервную копию ОС, такую же как в примере с утилитой tar. Сравните их (screenshot).
- Автоматизируйте создание резервной копии ОС с помощью утилиты rsync через планировщик задач на запуск каждый день в 22 часа (screenshot).