

Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №1
по курсу «СиМОИБ»
на тему: «Средства безопасности ОС UNIX/Linux»

Выполнил студент
группы 421702:

Бруцкий Д.С.

Проверил:

Захаров В.В.

МИНСК

2016

Задачи:

1. Создать группу пользователей.
2. Добавить новых пользователей.
3. Выполнить аудит ОС Ubuntu 16.04 KDE edition.

Выполнение

1. Создание группы пользователей

Для создания группы пользователей party используется команда `groupadd`

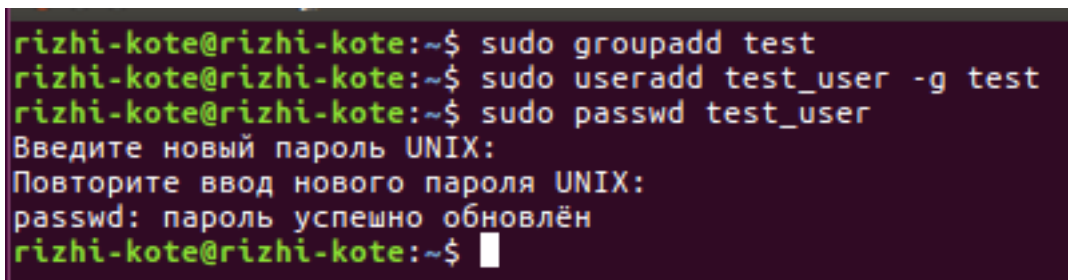
2. *Добавление новых пользователей*

Добавим двух новых пользователей.

`sudo useradd test_user -g test`

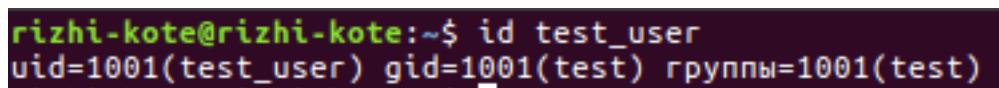
Добавление пользователя осуществляется при помощи команды `useradd`. Ключ `-g` означает, что для создаваемого пользователя группа `test` будет считаться первичной. По совету из руководства пароль пользователя устанавливается посредством утилиты `passwd`. По умолчанию пароль не задается, но учетная пользователя будет заблокирована до установки пароля.

Для просмотра информации о пользователях используется команда `id <имя пользователя>`. Результаты выполнения данной команды для



```
rizhi-kote@rizhi-kote:~$ sudo groupadd test
rizhi-kote@rizhi-kote:~$ sudo useradd test_user -g test
rizhi-kote@rizhi-kote:~$ sudo passwd test_user
Введите новый пароль UNIX:
Повторите ввод нового пароля UNIX:
passwd: пароль успешно обновлён
rizhi-kote@rizhi-kote:~$
```

Рисунок 1 – Добавление пользователя



```
rizhi-kote@rizhi-kote:~$ id test_user
uid=1001(test_user) gid=1001(test) группы=1001(test)
```

Рисунок 3 – Свойства созданного пользователя

3. Аудит

3.1. Установите систему Unix, к которой имеется административный доступ и на которой можно вносить изменения, не затрагивая рабочие приложения.

3.2. Найдите файлы загрузки и определите, какие приложения запускаются при загрузке системы. Выявите приложения, которые являются необходимыми для системы, и отключите все остальные.

Место расположение файлов загрузки: `/etc/rc2.d`

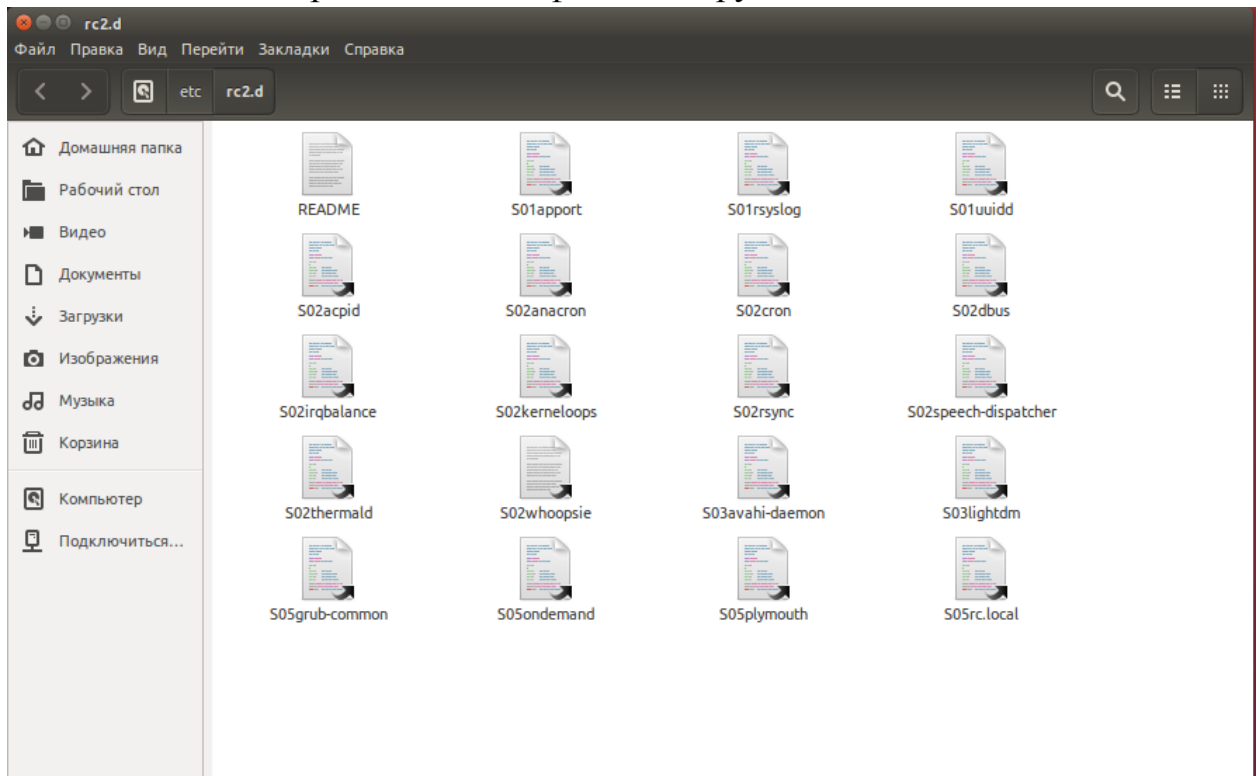


Рисунок 3 – Файлы загрузки

Отключённые службы: bluetooth,
cups – сервер печати,
cups-browsed – поиск принтеров
saned – сервер принтеров

3.3. Просмотрите файл `inetd.conf` и определите, какие службы включены. Определите службы, необходимые для системы, и отключите все остальные. Не забудьте выполнить команду `kill -HUP` для процесса `inetd`, чтобы перезапустить его с использованием новой конфигурации.

В ОС Ubuntu 16.04 файл inetd.conf считается устаревшим. Его аналогом является xinetd.

```
rizhi-kote@rizhi-kote:/$ cat /etc/xinetd.conf
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    # Please note that you need a log_type line to be able to use log_on_success
    # and log_on_failure. The default is the following :
    # log_type = SYSLOG daemon info
}

includedir /etc/xinetd.d
```

Рисунок 4 – Файл конфигурации xinetd.conf

В данном файле не прописаны ни какие службы.

3.4. Определите, используется ли в системе NFS. Внесите соответствующие изменения в файл dfstab.

В исследуемой ОС Ubuntu 16.04 не используется NFS. Это было проверенно с помощью следующей команды: df -T

```
rizhi-kote@rizhi-kote:/$ df -T
Файл.система  Тип      1К-блоков  Использовано  Доступно  Использовано%  Смонтирова
но в
udev          devtmpfs 488852      0             488852      0% /dev
tmpfs         tmpfs    101628      5016          96612       5% /run
/dev/sda1     ext4     7092728    4114696       2594700     62% /
tmpfs         tmpfs    508136      300           507836      1% /dev/shm
tmpfs         tmpfs    5120        4             5116        1% /run/lock
tmpfs         tmpfs    508136      0             508136      0% /sys/fs/cg
roup
tmpfs         tmpfs    101628      88            101540      1% /run/user/
1000
```

Рисунок 6 – Определение типа файловой системы

3.5. Если система использует telnet или FTP, загрузите TCP Wrappers и установите программу в системе. Настройте TCP Wrappers на разрешение доступа только к telnet и FTP, согласно требованиям системы.

При вводе команды «telnet» в терминал, можно узнать, установлен ли telnet. Если такого пакета не установлено, то выводится соответствующее сообщение. В исследуемой ОС telnet не используется.

```
rizhi-kote@rizhi-kote:/$ telnet
bash: /usr/bin/telnet: Нет такого файла или каталога
rizhi-kote@rizhi-kote:/$
```

- 3.6. Найдите файл приветственного сообщения. Определите, используется ли корректное приветственное сообщение. Если это не так, разместите в системе корректное приветственное сообщение.

Чтобы настроить приветственное сообщение до логирования необходимо изменить файлы `/etc/issue` и `/etc/issue.net`, введя в них соответствующий текст. Что настроить приветственное сообщение после логирования необходимо изменить файлы `00-header` в `/etc/update-motd.d`.

- 3.7. Выясните, настроены ли в системе требуемые ограничения на пароли согласно политике безопасности организации. Если это не так, внесите соответствующие настройки.

В файле `passwd` в `/etc/pam.d` введем ограничения на максимальное количество символов, минимальное количество пароля, время жизни пароля.

`PASS_MAX_DAYS 45` (Максимальное число дней, в течение которых пароль может использоваться)

`PASS_MIN_DAYS 1` (Минимальное число дней между сменой паролей)

`PASS_MIN_LEN 8` (минимальная длина пароля)

`PASS_MAX_LEN 10` (за сколько дней до истечения срока действия пароля появляется предупреждение)

- 3.8. Определите, настроен ли в системе должным образом параметр `umask` по умолчанию. Если это не так, настройте `umask` соответствующим образом.

Параметр `umask` по умолчанию не настроен.

В файле `/etc/profile` прописываем `umask 027` для настройки параметра `umask` (по умолчанию) для всех пользователей. Владельцу файла разрешаем чтение, запись и выполнение - 0. Группе разрешаем только чтение - 2. Остальным запрещаем все - 7.

Для того, чтобы настроить параметр для конкретного пользователя, необходимо изменять файл `/etc/passwd`.

r = read permissions

w = write permissions

x = execute permissions

3.9. Определите требования для входа через корневую учетную запись. Если администраторам требуется осуществлять вход сначала с использованием их собственного идентификатора (ID), настройте соответствующим образом конфигурацию системы.

Разработчики Ubuntu и всех его форков блокируют административную корневую учетную запись (root) по умолчанию во всех установках Ubuntu. Это не означает, что учетная запись root удалена или к ней нет доступа. Ей просто присвоен пароль, который не совпадает ни с одним возможным зашифрованным значением, соответственно, ее невозможно использовать для входа напрямую. Однако можно использовать в режиме рекавери.

Вместо этого поощряется применение пользователями инструмента с именем `sudo` для переноса административных обязанностей. Sudo позволяет авторизованным пользователям временно повышать их привилегии, используя их собственный пароль вместо знания пароля, присвоенного суперпользователю.

3.10. Проверьте систему на наличие неиспользуемых учетных записей. Все подобные учетные записи должны быть заблокированы.

Для каждой неиспользуемой учетной записи следует изменить их записи в файле `/etc/shadow`, чтобы предотвратить успешный вход в систему с их помощью. Для учетных записей, вход посредством которых запрещен, поле пароля должно

содержать какие-либо данные с символом "*". Символ "*" не соответствует ни одному реальному паролю и, таким образом, не может быть угадан или взломан. Посредством размещения в этом поле соответствующих символов, таких как "LK", можно явным образом сообщать о том, что данная учетная запись заблокирована.

В исследуемой ОС все неиспользуемые учетные записи, кроме 3-х, заблокированы по умолчанию (в поле пароля указан символ *). Неиспользуемых учётных записей не обнаружено.

- 3.11. Установите в системе соответствующие обновления.
sudo apt-get update – обновить информацию о репозиториях
sudo apt-get upgrade – установить и скачать обновления

- 3.12. Проверьте систему на некорректные пользовательские идентификаторы. В особенности следует искать учетные записи с UID, значение которого равно 0.

В файле passwd хранятся сведения о каждом пользователе (пароль, id, id группы ...). Отыщем всех пользователей с подозрительным id, после чего удалим их используя команду в терминале userdel username.

Результат: было найдено 3 пользователя, идентификаторы которых были меньше 100.

- 3.13. Убедитесь в том, что в системе ведется журнал подозрительной активности, и что файл syslog.conf настроен соответствующим образом.

Файл syslog.conf отсутствует. Аналогом программы ведения журналов syslog является rsyslog. Rsyslog настраивается через файл /etc/rsyslog.conf. Rsyslog настроен корректно.

- 3.14. Произведите в системе поиск скрытых файлов. Если будут найдены необычные скрытые файлы, исследуйте их, чтобы убедиться, что в систему никто не проник.

Все имена скрытых файлов в системе начинаются с «.». В терминале запустим поиск всех файлов имя которых начинается с «.»

```
find / -name «.*»
```

Результат: обнаружено огромное количество скрытых файлов

- 3.15. Произведите поиск файлов SUID и SGID. Если будут обнаружены такие файлы, расположенные в каталогах пользователей, исследуйте их, чтобы убедиться, что в систему никто не проник.

```
find / -type f -perm -02000 -ls
```

```
find / -type f -perm -04000 -ls
```

Результат: SUID и SGID не были обнаружены в пользовательских каталогах

- 3.16. Произведите поиск файлов, общедоступных для записи. Если будут найдены такие файлы, либо устраните проблему посредством изменения разрешений (сначала выясните, для чего эти файлы используются), либо обратитесь к ним внимание владельца.

Команда: «find . -perm -222 -print»

- 3.17. Проверьте сетевые интерфейсы на наличие любых неправильных настроек.

Для настройки автоматического подключения необходимо отредактировать файл конфигурации `etc/network/interfaces`.

По умолчанию установлены следующие значения

```
rizhi-kote@rizhi-kote:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
```

- 3.18. Проверьте систему на предмет прослушиваемых (активных) портов. Если обнаружится какое-либо несоответствие, найдите процесс, использующий порт, и определите, должен ли данный процесс работать в системе.

Команда: `sudo netstat -nlpA inet`

```
rizhi-kote@rizhi-kote:~$ sudo netstat -nlpA inet
Активные соединения с интернетом (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp      0      0 127.0.1.1:53 0.0.0.0:* LISTEN 1887/dnsmasq
tcp      0      0 127.0.1.1:631 0.0.0.0:* LISTEN 1708/cupsd
udp      0      0 0.0.0.0:60925 0.0.0.0:* 1989/avahi-daemon:
udp      0      0 127.0.1.1:53 0.0.0.0:* 1887/dnsmasq
udp      0      0 0.0.0.0:68 0.0.0.0:* 1871/dhclient
udp      0      0 0.0.0.0:5353 0.0.0.0:* 1989/avahi-daemon:
```

Рисунок 11 – Активные порты

- 3.19. Проверьте таблицу процессов в системе и определите, выполняются ли какие-либо несоответствующие процессы.

Воспользуемся командой в терминале «ps --All»

F	S	UID	PID	PPID	C	PRI	NI	ADDR	SZ	WCHAN	TTY	TIME	CMD
4	S	0	1	0	0	80	0	-	46377	-	?	00:00:01	systemd
1	S	0	2	0	0	80	0	-	0	-	?	00:00:00	kthreadd
1	S	0	3	2	0	80	0	-	0	-	?	00:00:00	ksoftirqd/0
1	S	0	5	2	0	60	-20	-	0	-	?	00:00:00	kworker/0:0H
1	S	0	7	2	0	80	0	-	0	-	?	00:00:00	rcu_sched
1	S	0	8	2	0	80	0	-	0	-	?	00:00:00	rcu_bh
1	S	0	9	2	0	-40	-	-	0	-	?	00:00:00	migration/0
5	S	0	10	2	0	-40	-	-	0	-	?	00:00:00	watchdog/0
5	S	0	11	2	0	80	0	-	0	-	?	00:00:00	kdevtmpfs
1	S	0	12	2	0	60	-20	-	0	-	?	00:00:00	netns
1	S	0	13	2	0	60	-20	-	0	-	?	00:00:00	perf
1	S	0	14	2	0	80	0	-	0	-	?	00:00:00	khungtaskd
1	S	0	15	2	0	60	-20	-	0	-	?	00:00:00	writeback
1	S	0	16	2	0	85	5	-	0	-	?	00:00:00	ksmd
1	S	0	17	2	0	99	19	-	0	-	?	00:00:00	khugepaged
1	S	0	18	2	0	60	-20	-	0	-	?	00:00:00	crypto
1	S	0	19	2	0	60	-20	-	0	-	?	00:00:00	kintegrityd
1	S	0	20	2	0	60	-20	-	0	-	?	00:00:00	bioset
1	S	0	21	2	0	60	-20	-	0	-	?	00:00:00	kblockd
1	S	0	22	2	0	60	-20	-	0	-	?	00:00:00	ata_sff
1	S	0	23	2	0	60	-20	-	0	-	?	00:00:00	md
1	S	0	24	2	0	60	-20	-	0	-	?	00:00:00	devfreq_wq

Рисунок 12 – Таблица процессов

Выводы:

После установки OS Ubuntu 16.04 в ней, как правило, присутствует ряд уязвимостей. Большую часть из них можно устранить посредством обновления или внесения изменений в конфигурационные файлы. В рамках данной лабораторной был проведён аудит ОС Ubuntu 16.04.

Найденные уязвимости:

1. в файлах загрузки присутствовали редко используемые службы, которые были отключены.
2. настройки паролей не соответствуют стандартам безопасности.
3. неправильно настроен параметр umask по умолчанию.

Для обеспечения лучшей безопасности необходимо настроить все параметры согласно стандартам безопасности. Так же можно использовать по для настройки и управления аудитом (ClearBoot, audit). Аудит в Linux – мощнейшее средство слежения за системой, но оно требует от пользователя глубокого знания ОС.