МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__» _____2016 г.

ЛАБОРАТОРНАЯ РАБОТА № 6
«Наблюдение и аудит в ОС Linux»

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных систем», «Администрирование вычислительных сетей» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01.

Курск 2016

УДК 004
Составители: В.В. Гефнер, И.В. Калуцкий

Рецензент
Кандидат технических наук, доцент кафедры
защиты информации и систем связи *А.Г. Спеваков*

Наблюдение и аудит в ОС Linux: методические указания к выполнению лабораторных и практических работ по дисциплинам: «Администрирование вычислительных систем», «Администрирование вычислительных сетей» / Юго-Зап. гос. ун-т; сост.: В.В. Гефнер, И.В. Калуцкий, Курск, 2016. 9 с.: ил. нет, Библиогр.: с. 9

Содержат сведения по вопросам наблюдения и аудита в ОС GNU/Linux.

Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Комплексная защита объектов информатизации», «Информационная безопасность», «Информационная безопасность автоматизированных систем».

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных систем», «Администрирование вычислительных сетей» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01.дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать . 31.05.16 Формат 60x84 1/16.
Усл. печ. л. 0,5. Уч. –изд.л. 0,4. Тираж 30 экз. Заказ 586 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

Цель работы

Цель лабораторной работы – ознакомление и получение практических навыков наблюдения и аудита в ОС GNU/Linux.

Порядок выполнения работы

1. Изучить теоретическую часть.
2. Выполнить задания, поставленные в данном методическом указании.
3. Сделать вывод по проделанной работе.

Содержание отчёта

1. Титульный лист.
2. Задание на лабораторную работу.
3. Ход выполнения лабораторной работы со скриншотами.
4. Вывод по лабораторной работе.

Выполнение работы

1. Зарегистрируйтесь в системе в консольном режиме с правами **root**. Намеренно сделайте несколько ошибок при вводе пароля, чтобы «отметиться» в журналах аудита.

2. С помощью команды **md5sum** вычислите и запишите контрольную сумму для одного из файлов в каталоге **/home/user1/qu1**. С помощью команды **echo** добавьте один символ в этот файл:

echo a >>/home/user1/qu1/jan

Вновь вычислите контрольную сумму файла и сравните два результата.

3. С помощью команды **md5sum** вычислите и запишите в файл контрольную сумму всех файлов в каталоге **/bin**.

4. С помощью команды **find** найдите в корневом каталоге файлы:

- имеющие атрибуты **SUID (find / -perm +4000);**
- имеющие атрибуты **SGID (find / -perm +2000);** файлы, которые разрешено модифицировать всем: **find / -type f -perm +2** ;
- файлы, не имеющие владельца **(find / -nouser**);
- файлы и каталоги, имеющие UID незарегистрированных в системе пользователей.

Объясните, какой интерес могут представлять для администратора указанные категории файлов?

5. Путем просмотра процессов убедитесь в том, что системный сервис **syslogd** запущен. В целях контроля его действий найдите в журналах аудита записи о попытках своего входа в систему (это может быть файл **secure** или **auth** в каталоге **/var/log**).

6. С помощью команды **grep** найдите уязвимые учетные записи в файле паролей:

- имеющие числовые идентификаторы суперпользователя и его группы: **UID**=0 и **GID**=0;
- имеющие право на вход в систему без ввода пароля (отсутствующее второе поле в виде **::**).

Если у вас есть проблемы с вводом команды и установкой соответствующих фильтров, вы можете просто внимательно просмотреть содержимое файла паролей **/etc/passwd**.

7. С помощью команды **id user_name** посмотрите список основной и дополнительных групп пользователей. Найдите дополнительные группы **floppy**, **cdrom** и **plugdev**, дающие право использовать сменные машинные носители **/etc/cdrom**, **/etc/fd0** и т.д. для бесконтрольного блочного копирования данных.

Задание 1

Просматривая файл истории командной строки одного из пользователей, администратор обнаружил следующий фрагмент (см. ниже). Требуется исследовать приведенную последовательность

команд, выявить намерения пользователя и установить, удалось ли ему нарушить установленную по умолчанию политику безопасности. Наиболее важные команды сопроводите своими комментариями.

```
su su su su root whereis su pwd cp /din/su cp /bin/su cp --help cp --help |
more cp /bin/su /home/petrov ls -l /bin ls -l /bin | more chmod 777 /bin/su
ls -l /bin
cp /bin/chmod /home/petrov chmod 777 /bin/su
/home/petrov/chmod 777 /bin/su ls -l /bin | more ls -l
/home/petrov/chmod 4777 chmod ls -l
/home/petrov/chmod 777 /bin/su ls -l chown root chmod fdformat --help
fdformat /dev/fd0 mke2fs /dev/fd0 cat /etc/fstab man mount ls /mnt
mount -t ext2 /dev/fd0 /mnt/floppy ls -l /mnt/floppy cd /mnt/floppy echo
#! /bin/bash > ls echo chmod 777 /bin/su >> ls cat ls
chmod 777 ls umount /dev/fd0 cd umount /dev/fdo mount -t ext2
/dev/fd0 /bin ls -l /
mount -t ext2 /dev/fd0 /mnt/floppy
/mnt/floppy/ls
```

Задание 2

Проанализируйте содержимое файла **/etc/passwd** и сделайте выводы в отношении потенциальных угроз безопасности. Проставьте в необходимых местах свои комментарии.

```
abcd:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/bin/bash
```

games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody::0:99:Nobody:/:/bin/bash
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin nscd:x:28:28:NSCD
Daemon:/:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
root:x:501:501::/home/ivanov:/bin/vi
gromov:x:502:1::/home/gromov:/bin/bash
user1:x:503:504::/home/user1:/bin/bash
user2:!!:504:505::/home/user2:/bin/bash

Задание 3

Почти в каждой книге по безопасности операционных систем UNIX/Linux отмечается опасность запуска пользователями специально подготовленных файлов (исполняемых или командных) с установленным атрибутом **SUID**. Указывается на необходимость установки в файле **/etc/fstab** запрета на запуск файлов со сменных машинных носителей (noexec), а тем более – с установленным атрибутом SUID (nosuid). Предлагается проверить реальность такой угрозы. Дискету или носитель USBFlash с «опасным» сценарием подготовьте с правами администратора, отредактируйте файл **/etc/fstab**, а затем проверьте наличие угрозы с консоли пользователя. На машинном носителе с помощью утилиты **mke2fs** должна быть установлена файловая система **ext2fs**, в противном случае не удастся

скопировать на нее файл с нужными атрибутами. По результатам выполнения задания сделайте выводы.

Задание 4

Предлагается выяснить, существует ли надежный способ исключить возможность копирования пользователем конфиденциальной информации с жесткого магнитного диска на сменный машинный носитель. При этом учтите, что запрет на монтирование дисков не исключает возможности блочного копирования компьютерной информации.

Задание 5

У вас возникли подозрения, что в ваше отсутствие злоумышленники получили физический доступ к компьютеру на вашем рабочем месте. На единственном жестком диске компьютера установлена операционная система Linux с офисными приложениями и конфиденциальной информацией. В составе компьютера имеются устройства чтения и записи на ГМД и CDR(W), а также интерфейсы USB. Системный блок компьютера был опечатан, и печати остались неповрежденными. Можно ли установить факт и характер несанкционированного доступа в операционной среде компьютера? Если да, то каким образом?

Библиографический список

1. Техническая электронная документация по операционной системе Linux.

2. Береснев А.Л. Администрирование GNU/Linux с нуля./А.Л. Береснев –СПб.: БВХ-Петербург, 2010 – 576 с.

3. Блум, Ричард, Бреснахэн, Кристина. Командная строка Linux и сценарии оболочки. Библия пользователя/ Ричард Блум, Кристина Бреснахэн -М. : ООО “И.Д. Вильямс”, 2012. — 784 с.

4. В.В. Бакланов Защитные механизмы операционной системы Linux: учебное пособие / В.В. Бакланов. под ред. Н.А. Гайдамакина. Екатеринбург: УрФУ, 2011. 354 с.