Занятие 63: практическое

ИНСТРУКЦИОННАЯ КАРТА № 27

на выполнение практического занятия по МДК.03.02
" Безопасность функционирования информационных систем "
для студентов специальности 09.02.02 Компьютерные сети

Тема: Аудит системы Unix/Linux.

Цель работы: Изучить технические средства диагностики уровня защищенности операционных систем
Норма времени: 2 ак. часа
Оснащение рабочего места: ПК, инструкционные карты, конспект.
Информационное обеспечение:
Аудит системных событий в Linux. – https://habr.com/ru/company/selectel/blog/267833/
Лучшие инструменты аудита безопасности Linux. – https://spy-soft.net/linux-hardening-tools/
Аудит в системе Unix Linux. – https://intellect.icu/audit-v-sisteme-unix-linux-5766?ysclid=ldm0g12lxq109616
Компетенции, умения и навыки, которыми должны овладеть обучающиеся: ОК9, ПК.3.1
После выполненных работ студент должен **знать:** принципы работы сканеров безопасности; **уметь:** использовать сканеры безопасности для поиска уязвимостей.

Теоретические сведения 1
Понятие аудита системы 1
Основные инструменты аудита 2
Программы сторонних разработчиков 2
Ход работы 3
Задание 1. Установка пакета auditd 3
Задание 2. Работа с правилами аудита 3
Содержание отчета о занятии 3

Теоретические сведения

Понятие аудита системы

Сканеры безопасности позволяют проверить уровень защищенности большого количества хостов. Однако они ориентированы только на известные уязвимости. Аудит позволяет отследить системные события и своевременно предупредить об отклонениях в работе системы.

> Аудит – это подсистема, позволяющая получить подробную информацию обо всех системных событиях. Она не обеспечивает никакой дополнительной защиты, но предоставляет подробную информацию о нарушениях безопасности, на основании которой можно принять конкретные меры.

Примеры критичных с точки зрения безопасности системных событий:
- ❑ запуск и завершение работы системы;
- ❑ чтение, запись и изменение прав доступа к файлам;
- ❑ инициация сетевых соединений или изменение сетевых настроек;
- ❑ попытки неудачной авторизации в системе;
- ❑ изменение информации о пользователях и группах;
- ❑ запуск и остановка приложений;
- ❑ выполнение системных вызовов.

Ни одно из названных событий не может произойти без использования системных вызовов ядра. Чтобы их отслеживать, достаточно просто перехватывать соответствующие системные вызовы. Именно это и делает подсистема аудита.

В англоязычной литературе понятие аудита принято называть Hardening Linux. Hardening обозначает процесс обеспечения безопасности системы (программы) за счет снижения ее уязвимости и, как правило, с использованием **исключительно штатных утилит или механизмов защиты**.

> Демон **auditd** доступен в любом современном Linux-дистрибутиве и может быть установлен с помощью стандартного менеджера пакетов.

Установка «штатного» аудита производится командой: **`sudo apt-get install auditd`**

> В большинстве операционных систем семейства Unix используется централизованная система регистрации системных сообщений **Syslog**.

Данная система позволяет администратору вести полный контроль за сообщениями как самой системы и системных процессов, так и прикладных процессов. Она обладает очень большой гибкостью и позволяет сортировать сообщения как по источникам, так и по степени важности и направлять их в различные пункты назначения: в журнальные файлы, на терминалы пользователей и даже на другие машины в сети. Таким образом, администратор может организовать централизованную процедуру регистрации системных сообщений во всей сети.

> Система **Syslog** состоит из трех компонентов:
> - демона **syslogd**, который осуществляет регистрацию событий;

- библиотечных функций **openlog(),syslog(),closelog()**, которые передают сообщения демону **syslogd**;
- команды **logger**, которая принимает сообщения от интерпретатора команд.

Основные инструменты аудита

В состав пакета **auditd** входят демон **auditd** и несколько вспомогательных утилит:

- **auditctl** — утилита для управления демоном auditd; позволяет получать информацию о текущем состоянии подсистемы аудита, а также добавлять и удалять правила;
- **autrace** — утилита для аудита событий, порождаемых процессами (работает по тому же принципу, что и strace);
- **ausearch** — утилита для поиска событий в журнальных файлах;
- **aureport** — утилита для генерации отчётов о работе системы аудита.

Получив вызов от приложения в пространстве пользователя, подсистема аудита пропускает его через один из следующих фильтров: user, task или exit. После этого вызов пропускается через фильтр exclude, который исходя из правил аудита передаёт его демону auditd для дальнейшей обработки.

Добавление и удаление правил выполняется утилитой auditctl.

Для работы с правилами используется **auditctl** с опциями:

- **-l** — показать все правила;
- **-a** — создать новое;
- **-d** — удалить правило;
- **-D** — удалить все правила из списка.

Чтобы создать новое правило, нужно выполнить команду вида:

```
$ auditctl -a <список>, <действие> -S <имя системного вызова> -F <фильтры>
```

Сначала после опции **-a** указывается список, в который нужно добавить правило.

Всего существует 5 списков правил:

task — события, связанные с созданием новых процессов;
entry — события, которые имеют место при входе в системный вызов;
exit — события, которые имеют место при выходе из системного вызова;
user — события, использующие параметры пользовательского пространства;
exclude — используется для исключения событий.

Примеры правил:
требуется вести аудит обращений к файлам из каталога **/etc**

```
$ auditctl -a exit,always -S open -F path =/etc/
```

отслеживать системные вызовы open () от пользователя с UID 1001

```
$ auditctl -a exit,always -S open -F loginuid=1001
```

отслеживать доступ к файлам паролей и групп и попытки их изменения:

```
$ auditctl -w /etc/group -p wa
$ auditctl -w /etc/passwd -p wa
```

Правила можно не только задавать через командную строку, но и прописывать в файле **/etc/audit/audit.rules**.

Программы сторонних разработчиков

Наряду с инструментами аудита, являющимися частью системы, существуют специальные программы аудита.

Наиболее популярными программами аудита Linux от сторонних разработчиков являются:

- **Lynis** — auditing system hardening testing
- **Lunar** — a UNIX security auditing tool
- **Nix Auditor** — a CIS Audit made easier
- **Loki** — Simple IOC and Incident Response Scanner
- **Linux Security Auditing Tool (LSAT)**

Ход работы

Задание 1. Установка пакета auditd

Выполнить установку пакета (только первая группа).

Задание 2. Работа с правилами аудита

1. Выполнить примеры команд работы с правилами, приведенные выше. **Показать результат преподавателю**.
2. Выполнить удаление всех правил.

Содержание отчета о занятии

1. Аудит - это…
2. В любом дистрибутиве Linux доступен пакет …
3. В операционной системе Unix имеется пакет …
4. В состав пакета auditd входят утилиты: …
5. Опции утилиты auditctl: …
6. Основные списки правил: …
7. Наиболее популярными программами аудита Linux от сторонних разработчиков являются: …

Инструкционную карту составил преподаватель Дубик Н.А.